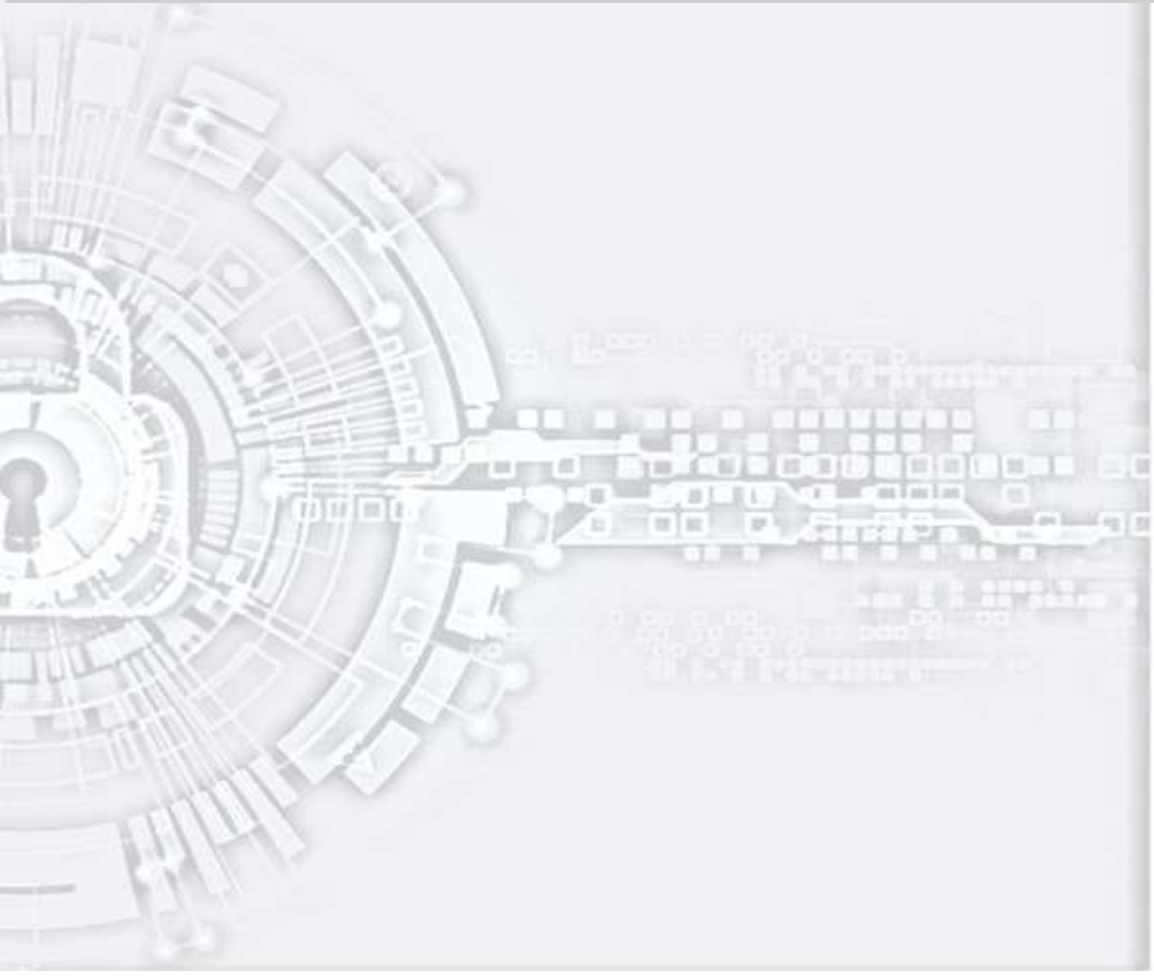
Universidad Nacional Autónoma de México

Facultad de Ingeniería

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES FACULTAD DE INGENIERÍA



AGOSTO 2022

ÍNDICE

Presentación

La Facultad de Ingeniería (FI) es la primera escuela de ingeniería del continente americano, que ha consolidado a lo largo de 230 años su papel protagónico en la formación profesional de excelencia.

Cuenta con 15 programas de licenciatura, incluyendo el más reciente Ingeniería Aeroespacial aprobado en 2019, diseñados para dar respuesta a las necesidades tecnológicas y de infraestructura que el país requiere para construir una sociedad más humana y justa; cabe destacar que 13 de ellos cumplen con los lineamientos del Consejo de Acreditación de la Ingeniería, CACEI, lo cual garantiza el excelente nivel académico de sus egresados. Asimismo 12 carreras obtuvieron en 2021 el sello EUR-ACE otorgado por la Red Europea para la Acreditación de Educación en Ingeniería, lo que las coloca a la altura de las mejores del mundo. En el posgrado, se ofrecen programas de maestría y doctorado, con ocho áreas de conocimiento inscritos en el programa de calidad del Conacyt, y el Programa Único de Especializaciones en Ingeniería, con 13 campos disciplinarios. De esta manera, la FI atiende a una población de cerca de 14,000 estudiantes de licenciatura y 2000 de posgrado.

En la entidad se cuenta con aulas y laboratorios que están a cargo de especialistas que con su experiencia y juventud transmiten a los futuros profesionistas los conocimientos de vanguardia en todos los campos de la ingeniería. La formación académica se refuerza mediante la vinculación que se realiza con los sectores productivos, público y privado, que se concreta en convenios y colaboraciones con instituciones gubernamentales y prestigiadas empresas

Sus académicas y académicos desde los tres campus, Ciudad Universitaria, Morelos y Querétaro publican artículos arbitrados e indizados, así como informes técnicos; realizan investigación que genera patentes y desarrollan software, con la valiosa colaboración de las y los estudiantes. Asimismo, a través de la Incubadora de Empresas y el Programa Innova UNAM los estudiantes desarrollan servicios y productos innovadores que resuelven necesidades específicas de la sociedad.

A través de la División de Educación Continua y a Distancia se imparten cursos y diplomados con certificación internacional para una actualización de excelencia acorde al avance de la tecnología.

Además de la enseñanza e investigación, se realiza con esmero la tercera función sustantiva de la UNAM: la extensión de la cultura, y en este contexto honrosamente resguarda dos recintos históricos: el Real Seminario de Minería y el Palacio de Minería, cuna de la ingeniería americana. En el majestuoso palacio se lleva a cabo una tradición cultural de la Ciudad de México: la Feria Internacional del Libro del Palacio de Minería para fomentar la lectura, ya que reúne a casas editoriales nacionales y extranjeras contando con un vasto programa cultural.

La música es un valor de identidad cultural de los ingenieros. Por ello, la Orquesta Sinfónica de Minería, con el apoyo de distinguidos egresados de la FI, realiza año con año su Temporada de verano en la Sala Nezahualcóyotl con programas que incluyen a los más célebres compositores de todas las épocas y países.

En la Facultad de Ingeniería la difusión del quehacer académico es fundamental. Así, se publican la revista arbitrada e indizada Ingeniería, Investigación y Tecnología, la Gaceta digital y se cuenta con el portal de Comunicación, redes sociales y los programas de radio Ingeniería en marcha y la Feria de los libros transmitidos por Radio UNAM.

La Facultad de Ingeniería es una institución con tradiciones, valores e identidad propia, porque enaltece su pasado, trabaja en el presente y tiene su mirada puesta en el futuro enarbolando su misión: la formación integral de profesionales en ingeniería capaces de transformar sustentable y responsablemente la naturaleza en beneficio del progreso y desarrollo de México.

Introducción

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de la esta área universitaria con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Su propósito es identificar los sistemas de tratamiento de datos personales que posee esta área universitaria, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

Este modelo pretende brindar a las áreas universitarias homogeneidad en la redacción, organización y contenido para que elaboren su propio documento de seguridad en el que se describan las tres medidas de seguridad para la protección de los datos personales.

El marco jurídico del documento de seguridad se regula por el capítulo II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada el 26 de enero de 2017, que establece un conjunto mínimo de medidas de seguridad que cada dependencia o entidad universitaria deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, según el tipo de soportes —físicos, electrónicos o ambos— en los que residen dichos datos y dependiendo del nivel de protección que tales datos requieran.

Específicamente los artículos 31, 32 y 33 de la Ley General, del 55 al 72 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018, así como del 20 al 31 de los Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México, publicados en la Gaceta UNAM el 25 de febrero de 2019.

El cimiento del formato de documento de seguridad es la aplicación de un enfoque basado en los riesgos de los activos universitarios, específicamente los datos personales y los soportes que los resguardan. Además, el formato considera el tamaño y estructura de la institución, objetivos, clasificación de la información, requerimientos de seguridad y procesos que se precisan en razón de los activos que posee esta Máxima Casa de Estudios, lo cual se encuentran contemplado en el estándar internacional en materia de seguridad de la información ISO/IEC 27002:2013 "*Tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información".*

SECRETARÍA GENERAL

SECRETARÍA GENERAL DE LA FACULTAD DE INGENIERÍA

La Secretaría General (SG) coordina y apoya la debida ejecución de las actividades de carácter académico de la Facultad de Ingeniería, además de promover la participación coordinada y sistemática del cargo directivo de la entidad en la planeación y administración de la institución. Asimismo, es la encargada de elaborar, implementar y dar seguimiento a los planes y programas de trabajo necesarios para la buena marcha de la Facultad.

La SG coordina el trabajo conjunto de:

- Coordinación de Procesos e Información del Consejo Técnico (CPICT)
- Coordinación del Programa de Superación del Personal Académico (CPSPA)
- Coordinación del Sistema de Bibliotecas (CB)
- Departamento de Información y Estadística (DIES)
- Departamento de Personal Académico y Movilidad Estudiantil (DPAME)
- Unidad de Apoyo Editorial (UDAE)
- Unidad de servicios de Cómputo Académico (UNICA)

ÍNDICE

Coordinación de Procesos e Información del Consejo Técnico (CPICT)

La Coordinación de Procesos e Información del Consejo Técnico depende directamente del Secretario General de la Facultad y su objetivo es apoyar al secretariado del Consejo Técnico en todos los asuntos emanados de la actividad del pleno del Consejo Técnico y de sus comisiones temporales y permanentes; en general, apoyar a los consejeros en su labor como tales.

Esta Coordinación es la encargada de instrumentar y administrar los sistemas de información que sustentan el trabajo del pleno. Asimismo, la Coordinación tiene el resguardo documental de las actas de las sesiones y demás documentos relacionados con la actividad del Consejo Técnico.

Sistema de Licencias y Comisiones (SILICOM)

El SISTEMA DE LICENCIAS Y COMISIONES permite a los académicos de la Facultad solicitar a su Consejo Técnico, de manera eficiente, licencias y comisiones conforme a lo establecido en los artículos del 95 al 100 del Estatuto del Personal Académico. Asimismo, agiliza y sistematiza la entrega de informes y permite hacer un seguimiento del trámite respectivo.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-01-CPICT-01
Nombre del sistema *	Sistema de Licencias y Comisiones (SILICOM)
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, correo electrónico, teléfono particular, teléfono de oficina, teléfono móvil, RFC, CURP, número de trabajador.
Responsable*:	Facultad de Ingeniería
Nombre*:	Víctor Hugo Tovar Pérez
Cargo*:	Coordinador de la CPICT
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema y el rol que tendrán. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema que impactan en el tratamiento de datos personales. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas. - Validar los procesos y reglas de negocio con las que opera el sistema.
	Encargados:
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	Christian Mitchel Elizalde Rivera
Cargo*:	Técnico Académico
Funciones*:	Administrar el sistema, esta actividad involucra la actualización de los datos personales de los académicos provistos por otras instancias de la UNAM
Obligaciones*:	Procurar el correcto despliegue de información únicamente a los usuarios involucrados en las diferentes etapas del proceso

(Nombre del Usuario 2*)	Raúl Ricardo Hernández Serrano
Cargo*:	Ayudante de profesor
Funciones*:	Monitorear las bitácoras del sistema para determinar posibles afectaciones, ataques y errores del sistema
Obligaciones*:	Solventar las vulnerabilidades en cuanto al acceso de usuarios
(Nombre del Usuario 3*)	Jefes de División de la Facultad de Ingeniería
Cargo*:	Jefe de División
Funciones*:	Revisar solicitudes recibidas de los académicos adscritos a su División
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 4*)	Miembros de la Comisión de Asuntos Académico Administrativos del Consejo Técnico de la Facultad de Ingeniería
Cargo*:	Consejero Técnico
Funciones*:	Revisar solicitudes recibidas de los académicos y emitir una recomendación al pleno del Consejo Técnico.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos Personales.
(Nombre del Usuario 5*)	Personal de apoyo de la CPICT
Cargo*:	Encargados del área de Normatividad académica
Funciones*:	Poner a disposición de la Comisión de Asuntos Académico Administrativos las solicitudes recibidas de los académicos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos Personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-01-CPICT-01
Nombre del sistema*	Sistema de Licencias y Comisiones (SILICOM)
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos y archivos digitales proporcionados por los usuarios.
Características del lugar donde se resguardan los soportes:*	Servidor productivo ubicado en la oficina de la Coordinación de Procesos e Información del Consejo Técnico.

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 9 a 11.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-01-CPICT-01
Nombre del sistema *	Sistema de Licencias y Comisiones (SILICOM)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema no realiza tratamiento de datos personales con soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**
   - **a)** Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

     Se registra el inicio de sesión exitoso en el sistema con fecha, hora, identidad, rol y dirección IP.
   - **b)** Para soportes físicos: Número o clave del expediente utilizado, y

     No se utilizan soportes físicos.
   - **c)** Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

     Solo se registra el inicio de sesión exitoso.
2. Si las bitácoras están en soporte físico o en soporte electrónico;

   Bitácoras en soporte electrónico.
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;

   Archivos *.log dentro del sistema. Se almacenan por 4 años.
4. La manera en que asegura la integridad de las bitácoras, y

   El acceso a las bitácoras está restringido al administrador del servidor.

5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y

      El área universitaria. Se analizan bajo demanda para corroborar temporalidad de algún incidente.
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

      Editor de texto y hoja de cálculo.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento o registro de incidentes.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

   Para las personas que acceden a sus instalaciones:

   a) ¿Cómo las identifica?
   No se cuenta con mecanismos de identificación
   b) ¿Cómo las autentifica?
   No se cuenta con mecanismos de autenticación.
   c) ¿Cómo les autoriza el acceso?
   No se cuenta con mecanismos de control de acceso.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

   Para las personas que acceden a dichos espacios interiores:

   1. ¿Cómo las identifica?
      Mediante la credencial de trabajador vigente.
   2. ¿Cómo las autentifica?
      Mediante la credencial de trabajador cuyo nombre coincide con los colaboradores publicados en portal.
   3. ¿Cómo les autoriza el acceso?
      Cuentan con llaves para el acceso al espacio donde se encuentra el servidor.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La información del personal académico y funcionariado se actualiza con base en la Nómina de la Facultad de Ingeniera, y los catálogos del Sistema de Información de Personal proporcionados por la Dirección General de Personal (DGP). Esta actualización comprende:

- Corrección de datos como: RFC, CURP, primer apellido, segundo apellido, y nombres.
- Inhabilitación de usuarios al no detectar su vigencia en nómina.
- Registro de personal de nueva contratación.

La frecuencia de actualización es quincenal. Estos datos son verificados previamente por la DGP.

Adicionalmente, el personal académico puede registrar, actualizar o borrar sus datos de: correo electrónico, teléfono de oficina y teléfono móvil. La modificación de esta información puede realizarse en cualquier momento en tanto la persona interesada esté vigente en la Nómina de la Facultad de Ingeniería.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):
- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
  Sí
- **b)** ¿Es discrecional (matriz de control de acceso)?
  Sí
- **c)** ¿Está basado en roles (perfiles) o grupos?
  Sí
- **d)** ¿Está basado en reglas?
  Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  Sí
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  Sí
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Solo se cifra la contraseña al ser almacenada.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
  Sí
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Solo se cifra la contraseña al ser almacenada.

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles?
  El administrador del sistema.
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
  El Coordinador de la CPICT.
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?
  No

5. Acceso remoto al sistema de tratamiento de datos personales:
- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
  No
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
  Sí
- **c)** ¿Cómo se evita el acceso remoto no autorizado?
  Lista blanca de usuarios con acceso mediante SSH. Autenticación a través de infraestructura de

llave pública.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos __X__, diferenciales ___ o incrementales __X__;
   b) De forma automática __X__ o Manual __X__,
   c) Periodicidad con que los realiza: __diario y semana
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
   Discos duros externos y servidor de respaldo.
3. Cómo y dónde archiva esos medios, y
   Discos duros externos: se encuentran bajo resguardo del Coordinador de la CPICT.
   Servidor de respaldo: instalaciones de la CPICT.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   El área universitaria.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   Se cuenta con un servidor de respaldo que se sincroniza de forma automática una vez al día. Este servidor cambiaría a productivo en cuanto surja una contingencia.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No se han realizado pruebas de eficiencia. Se estima que el procedimiento para dar continuidad de la operación tarde menos de 3 horas en horarios y días hábiles.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);
   b) Si el sitio es propio o subcontratado con un tercero;
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.
   No se cuenta con un sitio redundante.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-01-CPICT-01	
Nombre del sistema *	Sistema de Licencias y Comisiones (SILICOM)	
Recurso*	**Descripción***	**Control***
Auditoría de seguridad	Se utilizan herramientas de penetración para detectar	El responsable es el administrador del servidor.

	puertos abiertos y recursos sin control de acceso.	Las herramientas cuentan con licencia de software libre.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-01-CPICT-01	
Nombre del sistema *	Sistema de Licencias y Comisiones (SILICOM)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Pruebas de vulnerabilidad	Se realizaron pruebas de penetración al servidor que hospeda al sistema como parte de una Auditoría de Seguridad para la integración a la infraestructura de FEU de otro sistema.	a) Raúl Ricardo Hernández Serrano b) Septiembre de 2021

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-01-CPICT-01	
Nombre del sistema *	Sistema de Licencias y Comisiones (SILICOM)	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Pruebas de vulnerabilidad	La cantidad de incidentes de seguridad con impacto bajo	a) Raúl Ricardo Hernández Serrano b) Septiembre de 2021

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General	
Identificador único*	SG-01-CPICT-01

Nombre del sistema *	Sistema de Licencias y Comisiones (SILICOM)	
Medida de seguridad*	**Acciones***	**Responsable***
Seguridad SSL	a) Implementar protocolo SSL en el servidor que alberga el sistema. b) Mantener vigente el certificado SSL y verificar s correcto funcionamiento.	a) Raúl Ricardo Hernández Serrano b) Periodicidad trimestral
Corrección de errores en sistema	a) Habilitar bitácoras individuales por sistema dentro del servidor b) Atención a la notificación de errores por parte de usuarios y detectados en las bitácoras.	a) Raúl Ricardo Hernández Serrano b) Bajo demanda

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-01-CPICT-01		
Nombre del sistema *	Sistema de Licencias y Comisiones (SILICOM)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Los responsables de seguridad de datos personales no han recibido capacitación.			

8.2. Programa de difusión de la protección a los datos personales

Secretaría General	
Identificador único*	SG-01-CPICT-01
Nombre del sistema *	Sistema de Licencias y Comisiones (SILICOM)

Actividad*	Descripción*	Duración*	Cobertura*
No se cuenta con un programa de difusión de la protección de datos personales.			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-01-CPICT-01		
Nombre del sistema *	Sistema de Licencias y Comisiones (SILICOM)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Incorporación de nuevas características	Actualización de los parámetros de funcionamiento del sistema acorde al semestre en cuestión	2 semanas, periodicidad: semestral	Ajuste para la captura de nuevas solicitudes.
Actualización de tablas de datos	Actualización de académicos y funcionarios respecto a la nómina que libera cada quincena la DGP	1 hora, periodicidad: quincenal	Se registran nuevos usuarios para que puedan acceder al sistema y se inactivan usuarios que no están vigentes en nómina.

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-01-CPICT-01		
Nombre del sistema *	Sistema de Licencias y Comisiones (SILICOM)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Limpieza de equipo	Limpieza de polvo y residuos en componentes internos y conectores del equipo con sopladora de aire y brocha	2 horas cada 6 meses	Reestablecer la capacidad de enfriamiento del equipo

Inspección visual de componentes electrónicos	Verificar que capacitores y placas electrónicas no presenten signos de desgaste o fin de vida útil	2 horas cada 6 meses	
Reemplazo de pasta térmica	Remover material de intercambio térmico reseco y aplicar nuevo	2 horas cada año	Reestablecer la capacidad de enfriamiento del equipo

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-01-CPICT-01	
Nombre del sistema *	Sistema de Licencias y Comisiones (SILICOM)	
Proceso*	**Descripción***	**Responsable***
Respaldo semanal en disco duro externo	1. Respaldar base de datos completa 2. Respaldar código fuente y recursos del sistema	Responsable: Christian Mitchel Elizalde Rivera Tiempo máximo de ejecución en días: 1
Respaldo diario automatizado en servidor de respaldo	1. Respaldar base de datos completa 2. Respaldar código fuente y recursos del sistema	Responsable: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 1

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General		
Identificador único*	SG-01-CPICT-01	
Nombre del sistema *	Sistema de Licencias y Comisiones (SILICOM)	
Proceso*	**Descripción***	**Responsable***
Borrado seguro de aplicativo y recursos	- Identificación de directorios que	Nombre del responsable del proceso:

	contienen al aplicativo y recursos - Ejecución de comandos para borrado seguro en sistema de archivos del dispositivo de almacenamiento	Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 3
Disposición final de dispositivos de almacenamiento internos y externos	- Extracción del dispositivo de almacenamiento del gabinete. - Desmantelamiento de componentes internos que almacenan información como chips de memoria y discos. - Lijado de superficies de discos y destrucción de chips de memoria.	Nombre del responsable del proceso: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 3

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)

Permite la captura, por parte de Profesores de Carrera y Técnicos Académicos, de su programa e informe semestral, así como la revisión por parte de las divisiones y la Comisión de Evaluación.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-02-CPICT-02
Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, correo electrónico, teléfono particular, teléfono de oficina, teléfono móvil, RFC, CURP, número de trabajador.
Responsable*:	Facultad de Ingeniería
Nombre*:	Víctor Hugo Tovar Pérez
Cargo*:	Coordinador de la CPICT
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema y el rol que tendrán. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema que impactan en el tratamiento de datos personales. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas. - Validar los procesos y reglas de negocio con las que opera el sistema.
	Encargados:
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	Christian Mitchel Elizalde Rivera
Cargo*:	Técnico Académico
Funciones*:	Administrar el sistema, esta actividad involucra la actualización de los datos personales de los académicos provistos por otras instancias de la UNAM
Obligaciones*:	Procurar el correcto despliegue de información únicamente a los usuarios involucrados en las diferentes etapas del proceso
(Nombre del Usuario 2*)	Raúl Ricardo Hernández Serrano
Cargo*:	Ayudante de profesor
Funciones*:	Monitorear las bitácoras del sistema para determinar

	posibles afectaciones, ataques y errores del sistema
Obligaciones*:	Solventar las vulnerabilidades en cuanto al acceso de usuarios
(Nombre del Usuario 3*)	Jefes de División de la Facultad de Ingeniería
Cargo*:	Jefe de División
Funciones*:	Revisar programas e informes recibidos de los académicos adscritos a su División
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 4*)	Jefes de Departamento de las Divisiones de la Facultad de Ingeniería
Cargo*:	Jefe de Departamento
Funciones*:	Revisar programas e informes recibidos de los académicos adscritos a su División
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 5*)	Miembros de la Comisión de Evaluación del Consejo Técnico de la Facultad de Ingeniería
Cargo*:	Consejero Técnico
Funciones*:	Revisar programas e informes recibidos de los académicos y emitir una recomendación al pleno del Consejo Técnico.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos Personales.
(Nombre del Usuario 6*)	Personal de apoyo de la CPICT
Cargo*:	Encargados del área de Normatividad académica
Funciones*:	Poner a disposición de la Comisión de Evaluación las solicitudes recibidas de los académicos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos Personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-02-CPICT-02
Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos y archivos digitales proporcionados por los usuarios.
Características del lugar donde se resguardan los soportes: *	Servidor productivo ubicado en la oficina de la Coordinación de Procesos e Información del Consejo Técnico.

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 21 a 23.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-02-CPICT-02
Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema no realiza tratamiento de datos personales con soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
Se registra el inicio de sesión exitoso en el sistema con fecha, hora, identidad, rol y dirección IP.

b) Para soportes físicos: Número o clave del expediente utilizado, y
No se utilizan soportes físicos.

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
Solo se registra el inicio de sesión exitoso.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
Bitácoras en soporte electrónico.
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
Archivos *.log dentro del sistema. Se almacenan por 4 años.
4. La manera en que asegura la integridad de las bitácoras, y
El acceso a las bitácoras está restringido al administrador del servidor.
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y

   El área universitaria. Se analizan bajo demanda para corroborar temporalidad de algún incidente.

   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

   Editor de texto y hoja de cálculo.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento o registro de incidentes.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación

b) ¿Cómo las autentifica?
No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Mediante la credencial de trabajador vigente.
2. ¿Cómo las autentifica?
   Mediante la credencial de trabajador cuyo nombre coincide con los colaboradores publicados en portal.
3. ¿Cómo les autoriza el acceso?
   Cuentan con llaves para el acceso al espacio donde se encuentra el servidor.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La información del personal académico y funcionariado se actualiza con base en la Nómina de la Facultad de Ingeniera, y los catálogos del Sistema de Información de Personal proporcionados por la Dirección General de Personal (DGP). Esta actualización comprende:

- Corrección de datos como: RFC, CURP, primer apellido, segundo apellido, y nombres.
- Inhabilitación de usuarios al no detectar su vigencia en nómina.
- Registro de personal de nueva contratación.

La frecuencia de actualización es quincenal. Estos datos son verificados previamente por la DGP.

Adicionalmente, el personal académico puede registrar, actualizar o borrar sus datos de: correo electrónico, teléfono de oficina y teléfono móvil. La modificación de esta información puede realizarse en cualquier momento en tanto la persona interesada esté vigente en la Nómina de la Facultad de Ingeniería.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):
- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
  Sí
- **b)** ¿Es discrecional (matriz de control de acceso)?
  Sí
- **c)** ¿Está basado en roles (perfiles) o grupos?
  Sí
- **d)** ¿Está basado en reglas?
  Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  Sí
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  Sí
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Solo se cifra la contraseña al ser almacenada.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo se cifra la contraseña al ser almacenada.

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
El administrador del sistema.
b) ¿Quién autoriza la creación de nuevos perfiles?
El Coordinador de la CPICT.
c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí
c) ¿Cómo se evita el acceso remoto no autorizado?
Lista blanca de usuarios con acceso mediante SSH. Autenticación a través de infraestructura de llave pública.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
a) Completos __X__, diferenciales ___ o incrementales __X__;
b) De forma automática __X__ o Manual __X__,
c) Periodicidad con que los realiza: __diario y semana
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
Discos duros externos y servidor de respaldo.
3. Cómo y dónde archiva esos medios, y
Discos duros externos: se encuentran bajo resguardo del Coordinador de la CPICT.
Servidor de respaldo: instalaciones de la CPICT.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
El área universitaria.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
Se cuenta con un servidor de respaldo que se sincroniza de forma automática una vez al día. Este servidor cambiaría a productivo en cuanto surja una contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
No se han realizado pruebas de eficiencia. Se estima que el procedimiento para dar continuidad de la operación tarde menos de 3 horas en horarios y días hábiles.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o subcontratado con un tercero;

c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.
No se cuenta con un sitio redundante.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-02-CPICT-02	
Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)	
Recurso*	**Descripción***	**Control***
Auditoría de seguridad	Se utilizan herramientas de penetración para detectar puertos abiertos y recursos sin control de acceso.	El responsable es el administrador del servidor. Las herramientas cuentan con licencia de software libre.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-02-CPICT-02	
Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Pruebas de vulnerabilidad	Se realizaron pruebas de penetración al servidor que hospeda al sistema como parte de una Auditoría de Seguridad para la integración a la infraestructura de FEU de otro sistema.	a) Raúl Ricardo Hernández Serrano b) Septiembre de 2021

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General	
Identificador único*	SG-02-CPICT-02

Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Pruebas de vulnerabilidad	La cantidad de incidentes de seguridad con impacto bajo	a) Raúl Ricardo Hernández Serrano b) Septiembre de 2021

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-02-CPICT-02	
Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)	
Medida de seguridad*	**Acciones***	**Responsable***
Seguridad SSL	a) Implementar protocolo SSL en el servidor que alberga el sistema. b) Mantener vigente el certificado SSL y verificar s correcto funcionamiento.	a) Raúl Ricardo Hernández Serrano b) Periodicidad trimestral
Corrección de errores en sistema	a) Habilitar bitácoras individuales por sistema dentro del servidor b) Atención a la notificación de errores por parte de usuarios y detectados en las bitácoras.	a) Raúl Ricardo Hernández Serrano b) Bajo demanda

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General	
Identificador único*	SG-02-CPICT-02

Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Los responsables de seguridad de datos personales no han recibido capacitación.			

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-02-CPICT-02		
Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-02-CPICT-02		
Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Incorporación de nuevas características	Actualización de los parámetros de funcionamiento del sistema acorde al semestre en cuestión	2 semanas, periodicidad: semestral	Ajuste para la captura de nuevas solicitudes.

Actualización de tablas de datos	Actualización de académicos y funcionarios respecto a la nómina que libera cada quincena la DGP	1 hora, periodicidad: quincenal	Se registran nuevos usuarios para que puedan acceder al sistema y se inactivan usuarios que no están vigentes en nómina.

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-02-CPICT-02		
Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Limpieza de equipo	Limpieza de polvo y residuos en componentes internos y conectores del equipo con sopladora de aire y brocha	2 horas cada 6 meses	Reestablecer la capacidad de enfriamiento del equipo
Inspección visual de componentes electrónicos	Verificar que capacitores y placas electrónicas no presenten signos de desgaste o fin de vida útil	2 horas cada 6 meses	
Reemplazo de pasta térmica	Remover material de intercambio térmico reseco y aplicar nuevo	2 horas cada año	Reestablecer la capacidad de enfriamiento del equipo

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General	
Identificador único*	SG-02-CPICT-02

Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)	
Proceso*	**Descripción***	**Responsable***
Respaldo semanal en disco duro externo	1. Respaldar base de datos completa 2. Respaldar código fuente y recursos del sistema	Responsable: Christian Mitchel Elizalde Rivera Tiempo máximo de ejecución en días: 1
Respaldo diario automatizado en servidor de respaldo	1. Respaldar base de datos completa 2. Respaldar código fuente y recursos del sistema	Responsable: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 1

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General		
Identificador único*	SG-02-CPICT-02	
Nombre del sistema *	Sistema de Programas e Informes de la Facultad de Ingeniería (PROINFI)	
Proceso*	**Descripción***	**Responsable***
Borrado seguro de aplicativo y recursos	- Identificación de directorios que contienen al aplicativo y recursos - Ejecución de comandos para borrado seguro en sistema de archivos del dispositivo de almacenamiento	Nombre del responsable del proceso: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 3
Disposición final de dispositivos de almacenamiento internos y externos	- Extracción del dispositivo de almacenamiento del gabinete. - Desmantelamiento de componentes internos que almacenan información como chips de memoria y discos.	Nombre del responsable del proceso: Raúl Ricardo Hernández Serrano

	- Lijado de superficies de discos y destrucción de chips de memoria.	Tiempo máximo de ejecución en días: 3

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

Módulo de Informes de profesores de asignatura

Permite la captura, por parte del personal de asignatura (Profesores de Asignatura), de su informe semestral, así como la gestión por parte de la Comisión de Evaluación para recomendar al pleno la sanción respectiva.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-03-CPICT-03
Nombre del sistema *	Módulo de Informes de profesores de asignatura
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, correo electrónico, teléfono particular, teléfono de oficina, teléfono móvil, RFC, CURP, número de trabajador.
Responsable*:	Facultad de Ingeniería
Nombre*:	Víctor Hugo Tovar Pérez
Cargo*:	Coordinador de la CPICT
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema y el rol que tendrán. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema que impactan en el tratamiento de datos personales. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas. - Validar los procesos y reglas de negocio con las que opera el sistema.
	Encargados:
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	Christian Mitchel Elizalde Rivera
Cargo*:	Técnico Académico
Funciones*:	Administrar el sistema, esta actividad involucra la actualización de los datos personales de los académicos provistos por otras instancias de la UNAM
Obligaciones*:	Procurar el correcto despliegue de información únicamente a los usuarios involucrados en las diferentes etapas del proceso
(Nombre del Usuario 2*)	Raúl Ricardo Hernández Serrano
Cargo*:	Ayudante de profesor
Funciones*:	Monitorear las bitácoras del sistema para determinar

	posibles afectaciones, ataques y errores del sistema
Obligaciones*:	Solventar las vulnerabilidades en cuanto al acceso de usuarios
(Nombre del Usuario 3*)	Miembros de la Comisión de Evaluación del Consejo Técnico de la Facultad de Ingeniería
Cargo*:	Consejero Técnico
Funciones*:	Revisar programas e informes recibidos de los académicos y emitir una recomendación al pleno del Consejo Técnico.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos Personales.
(Nombre del Usuario 4*)	Personal de apoyo de la CPICT
Cargo*:	Encargados del área de Normatividad académica
Funciones*:	Poner a disposición de la Comisión de Evaluación las solicitudes recibidas de los académicos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos Personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-03-CPICT-03
Nombre del sistema *	Módulo de Informes de profesores de asignatura
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos y archivos digitales proporcionados por los usuarios.
Características del lugar donde se resguardan los soportes: *	Servidor productivo ubicado en la oficina de la Coordinación de Procesos e Información del Consejo Técnico.

3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-03-CPICT-03
Nombre del sistema *	Módulo de Informes de profesores de asignatura
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema no realiza tratamiento de datos personales con soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
Se registra el inicio de sesión exitoso en el sistema con fecha, hora, identidad, rol y dirección IP.

b) Para soportes físicos: Número o clave del expediente utilizado, y
No se utilizan soportes físicos.

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
Solo se registra el inicio de sesión exitoso.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
Bitácoras en soporte electrónico.

3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
Archivos *.log dentro del sistema. Se almacenan por 4 años.

4. La manera en que asegura la integridad de las bitácoras, y

El acceso a las bitácoras está restringido al administrador del servidor.

5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y

   El área universitaria. Se analizan bajo demanda para corroborar temporalidad de algún incidente.

   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

   Editor de texto y hoja de cálculo.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento o registro de incidentes.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación

b) ¿Cómo las autentifica?
No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
Mediante la credencial de trabajador vigente.
2. ¿Cómo las autentifica?
Mediante la credencial de trabajador cuyo nombre coincide con los colaboradores publicados en portal.
3. ¿Cómo les autoriza el acceso?
Cuentan con llaves para el acceso al espacio donde se encuentra el servidor.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La información del personal académico y funcionariado se actualiza con base en la Nómina de la Facultad de Ingeniera, y los catálogos del Sistema de Información de Personal proporcionados por la Dirección General de Personal (DGP). Esta actualización comprende:

- Corrección de datos como: RFC, CURP, primer apellido, segundo apellido, y nombres.
- Inhabilitación de usuarios al no detectar su vigencia en nómina.
- Registro de personal de nueva contratación.

La frecuencia de actualización es quincenal. Estos datos son verificados previamente por la DGP.

Adicionalmente, el personal académico puede registrar, actualizar o borrar sus datos de: correo electrónico, teléfono de oficina y teléfono móvil. La modificación de esta información puede realizarse en cualquier momento en tanto la persona interesada esté vigente en la Nómina de la Facultad de Ingeniería.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
Sí
b) ¿Es discrecional (matriz de control de acceso)?
Sí
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo se cifra la contraseña al ser almacenada.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo se cifra la contraseña al ser almacenada.

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
El administrador del sistema.
b) ¿Quién autoriza la creación de nuevos perfiles?
El Coordinador de la CPICT.
c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí
c) ¿Cómo se evita el acceso remoto no autorizado?

Lista blanca de usuarios con acceso mediante SSH. Autenticación a través de infraestructura de llave pública.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   - **d)** Completos __X__, diferenciales ___ o incrementales __X__;
   - **e)** De forma automática __X__ o Manual __X__,
   - **f)** Periodicidad con que los realiza: __diario y semana
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Discos duros externos y servidor de respaldo.
3. Cómo y dónde archiva esos medios, y
   Discos duros externos: se encuentran bajo resguardo del Coordinador de la CPICT.
   Servidor de respaldo: instalaciones de la CPICT.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   El área universitaria.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   Se cuenta con un servidor de respaldo que se sincroniza de forma automática una vez al día. Este servidor cambiaría a productivo en cuanto surja una contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No se han realizado pruebas de eficiencia. Se estima que el procedimiento para dar continuidad de la operación tarde menos de 3 horas en horarios y días hábiles.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   - **a)** El tipo de sitio (caliente, tibio o frío);
   - **b)** Si el sitio es propio o subcontratado con un tercero;
   - **c)** Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   - **d)** Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

   No se cuenta con un sitio redundante.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-03-CPICT-03	
Nombre del sistema *	Módulo de Informes de profesores de asignatura	
Recurso*	**Descripción***	**Control***
Auditoría de seguridad	Se utilizan herramientas de penetración para detectar	El responsable es el administrador del servidor.

	puertos abiertos y recursos sin control de acceso.	Las herramientas cuentan con licencia de software libre.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-03-CPICT-03	
Nombre del sistema *	Módulo de Informes de profesores de asignatura	
Medida de seguridad*	**Procedimiento***	**Responsable***
Pruebas de vulnerabilidad	Se realizaron pruebas de penetración al servidor que hospeda al sistema como parte de una Auditoría de Seguridad para la integración a la infraestructura de FEU de otro sistema.	a) Raúl Ricardo Hernández Serrano b) Septiembre de 2021

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-03-CPICT-03	
Nombre del sistema *	Módulo de Informes de profesores de asignatura	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Pruebas de vulnerabilidad	La cantidad de incidentes de seguridad con impacto bajo	a) Raúl Ricardo Hernández Serrano b) Septiembre de 2021

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General	
Identificador único*	SG-03-CPICT-03
Nombre del sistema *	Módulo de Informes de profesores de asignatura

Medida de seguridad*	Acciones*	Responsable*
Seguridad SSL	a) Implementar protocolo SSL en el servidor que alberga el sistema. b) Mantener vigente el certificado SSL y verificar s correcto funcionamiento.	a) Raúl Ricardo Hernández Serrano b) Periodicidad trimestral
Corrección de errores en sistema	a) Habilitar bitácoras individuales por sistema dentro del servidor b) Atención a la notificación de errores por parte de usuarios y detectados en las bitácoras.	a) Raúl Ricardo Hernández Serrano b) Bajo demanda

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-03-CPICT-03		
Nombre del sistema *	Módulo de Informes de profesores de asignatura		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Los responsables de seguridad de datos personales no han recibido capacitación.			

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-03-CPICT-03		
Nombre del sistema *	Módulo de Informes de profesores de asignatura		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-03-CPICT-03		
Nombre del sistema *	Módulo de Informes de profesores de asignatura		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Incorporación de nuevas características	Actualización de los parámetros de funcionamiento del sistema acorde al semestre en cuestión	2 semanas, periodicidad: semestral	Ajuste para la captura de nuevas solicitudes.
Actualización de tablas de datos	Actualización de académicos y funcionarios respecto a la nómina que libera cada quincena la DGP	1 hora, periodicidad: quincenal	Se registran nuevos usuarios para que puedan acceder al sistema y se inactivan usuarios que no están vigentes en nómina.

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-03-CPICT-03		
Nombre del sistema *	Módulo de Informes de profesores de asignatura		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Limpieza de equipo	Limpieza de polvo y residuos en componentes internos y conectores del equipo con sopladora de aire y brocha	2 horas cada 6 meses	Reestablecer la capacidad de enfriamiento del equipo

Inspección visual de componentes electrónicos	Verificar que capacitores y placas electrónicas no presenten signos de desgaste o fin de vida útil	2 horas cada 6 meses	
Reemplazo de pasta térmica	Remover material de intercambio térmico reseco y aplicar nuevo	2 horas cada año	Reestablecer la capacidad de enfriamiento del equipo

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-03-CPICT-03	
Nombre del sistema *	Módulo de Informes de profesores de asignatura	
Proceso*	**Descripción***	**Responsable***
Respaldo semanal en disco duro externo	1. Respaldar base de datos completa 2. Respaldar código fuente y recursos del sistema	Responsable: Christian Mitchel Elizalde Rivera Tiempo máximo de ejecución en días: 1
Respaldo diario automatizado en servidor de respaldo	1. Respaldar base de datos completa 2. Respaldar código fuente y recursos del sistema	Responsable: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 1

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General		
Identificador único*	SG-03-CPICT-03	
Nombre del sistema *	Módulo de Informes de profesores de asignatura	
Proceso*	**Descripción***	**Responsable***

Borrado seguro de aplicativo y recursos	- Identificación de directorios que contienen al aplicativo y recursos - Ejecución de comandos para borrado seguro en sistema de archivos del dispositivo de almacenamiento	Nombre del responsable del proceso: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 3
Disposición final de dispositivos de almacenamiento internos y externos	- Extracción del dispositivo de almacenamiento del gabinete. - Desmantelamiento de componentes internos que almacenan información como chips de memoria y discos. - Lijado de superficies de discos y destrucción de chips de memoria.	Nombre del responsable del proceso: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 3

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)

Permite la captura, por parte de las secretarías de las divisiones de la Facultad de Ingeniería, de las cargas académicas semestrales.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-04-CPICT-04
Nombre del sistema *	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, correo electrónico, teléfono particular, teléfono de oficina, teléfono móvil, RFC, CURP, número de trabajador.
Responsable*:	Facultad de Ingeniería
Nombre*:	Víctor Hugo Tovar Pérez
Cargo*:	Coordinador de la CPICT
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema y el rol que tendrán. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema que impactan en el tratamiento de datos personales. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas. - Validar los procesos y reglas de negocio con las que opera el sistema.
	Encargados:
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	Christian Mitchel Elizalde Rivera
Cargo*:	Técnico Académico
Funciones*:	Administrar el sistema, esta actividad involucra la actualización de los datos personales de los académicos provistos por otras instancias de la UNAM
Obligaciones*:	Procurar el correcto despliegue de información únicamente a los usuarios involucrados en las diferentes etapas del proceso
(Nombre del Usuario 2*)	Raúl Ricardo Hernández Serrano
Cargo*:	Ayudante de profesor
Funciones*:	Monitorear las bitácoras del sistema para determinar

	posibles afectaciones, ataques y errores del sistema
Obligaciones*:	Solventar las vulnerabilidades en cuanto al acceso de usuarios
(Nombre del Usuario 3*)	Secretarios académicos de las Divisiones de la Facultad de Ingeniería
Cargo*:	Secretario Académico de División
Funciones*:	Realizar la carga académica del personal adscrito a la División. Realizar correcciones a la carga académica al finalizar el semestre. Capturar la entrega oportuna de actas del profesorado respecto a la carga registrada.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 4*)	Personal de apoyo de la CPICT
Cargo*:	Encargados del área de Normatividad académica y Estímulos
Funciones*:	Poner a disposición de la Comisión de Evaluación las solicitudes recibidas de los académicos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos Personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-04-CPICT-04
(Nombre del sistema A1*)	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos y archivos digitales proporcionados por los usuarios.
Características del lugar donde se resguardan los soportes: *	Servidor productivo ubicado en la oficina de la Coordinación de Procesos e Información del Consejo Técnico.

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 46 a 48.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-04-CPICT-04
Nombre del sistema *	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema no realiza tratamiento de datos personales con soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

Se registra el inicio de sesión exitoso en el sistema con fecha, hora, identidad, rol y dirección IP.

b) Para soportes físicos: Número o clave del expediente utilizado, y

No se utilizan soportes físicos.

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

Solo se registra el inicio de sesión exitoso.

2. **Si las bitácoras están en soporte físico o en soporte electrónico;**
   Bitácoras en soporte electrónico.
3. **Lugar dónde almacena las bitácoras y por cuánto tiempo;**
   Archivos *.log dentro del sistema. Se almacenan por 4 años.
4. **La manera en que asegura la integridad de las bitácoras, y**
   El acceso a las bitácoras está restringido al administrador del servidor.
5. **Respecto del análisis de las bitácoras:**
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   El área universitaria. Se analizan bajo demanda para corroborar temporalidad de algún incidente.
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
   Editor de texto y hoja de cálculo.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento o registro de incidentes.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

   Para las personas que acceden a sus instalaciones:

   a) ¿Cómo las identifica?
   No se cuenta con mecanismos de identificación
   b) ¿Cómo las autentifica?
   No se cuenta con mecanismos de autenticación.
   c) ¿Cómo les autoriza el acceso?
   No se cuenta con mecanismos de control de acceso.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

   Para las personas que acceden a dichos espacios interiores:

   1. ¿Cómo las identifica?
      Mediante la credencial de trabajador vigente.
   2. ¿Cómo las autentifica?
      Mediante la credencial de trabajador cuyo nombre coincide con los colaboradores publicados en portal.
   3. ¿Cómo les autoriza el acceso?
      Cuentan con llaves para el acceso al espacio donde se encuentra el servidor.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La información del personal académico y funcionariado se actualiza con base en la Nómina de la Facultad de Ingeniera, y los catálogos del Sistema de Información de Personal proporcionados por la Dirección General de Personal (DGP). Esta actualización comprende:

- Corrección de datos como: RFC, CURP, primer apellido, segundo apellido, y nombres.
- Inhabilitación de usuarios al no detectar su vigencia en nómina.
- Registro de personal de nueva contratación.

La frecuencia de actualización es quincenal. Estos datos son verificados previamente por la DGP.

Adicionalmente, el personal académico puede registrar, actualizar o borrar sus datos de: correo electrónico, teléfono de oficina y teléfono móvil. La modificación de esta información puede realizarse en cualquier momento en tanto la persona interesada esté vigente en la Nómina de la Facultad de Ingeniería.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
Sí
b) ¿Es discrecional (matriz de control de acceso)?
Sí
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo se cifra la contraseña al ser almacenada.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo se cifra la contraseña al ser almacenada.

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
El administrador del sistema.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Coordinador de la CPICT.

c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí

c) ¿Cómo se evita el acceso remoto no autorizado?
Lista blanca de usuarios con acceso mediante SSH. Autenticación a través de infraestructura de llave pública.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos __X__, diferenciales ___ o incrementales __X__;

b) De forma automática __X__ o Manual __X__,

c) Periodicidad con que los realiza: __diario y semana

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
Discos duros externos y servidor de respaldo.

3. Cómo y dónde archiva esos medios, y
Discos duros externos: se encuentran bajo resguardo del Coordinador de la CPICT.
Servidor de respaldo: instalaciones de la CPICT.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
El área universitaria.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
Se cuenta con un servidor de respaldo que se sincroniza de forma automática una vez al día. Este servidor cambiaría a productivo en cuanto surja una contingencia.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
No se han realizado pruebas de eficiencia. Se estima que el procedimiento para dar continuidad de la operación tarde menos de 3 horas en horarios y días hábiles.

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) El tipo de sitio (caliente, tibio o frío);

b) Si el sitio es propio o subcontratado con un tercero;

c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y

d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

No se cuenta con un sitio redundante

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-04-CPICT-04	
Nombre del sistema *	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)	
Recurso*	**Descripción***	**Control***
Auditoría de seguridad	Se utilizan herramientas de penetración para detectar puertos abiertos y recursos sin control de acceso.	El responsable es el administrador del servidor. Las herramientas cuentan con licencia de software libre.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-04-CPICT-04	
Nombre del sistema *	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Pruebas de vulnerabilidad	Se realizaron pruebas de penetración al servidor que hospeda al sistema como parte de una Auditoría de Seguridad para la integración a la infraestructura de FEU de otro sistema.	a) Raúl Ricardo Hernández Serrano b) Septiembre de 2021

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General	
Identificador único*	SG-04-CPICT-04
Nombre del sistema *	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)

Medida de seguridad*	Resultado de evaluación*	Responsable*
Pruebas de vulnerabilidad	La cantidad de incidentes de seguridad con impacto bajo	a) Raúl Ricardo Hernández Serrano b) Septiembre de 2021

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-04-CPICT-04	
Nombre del sistema *	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)	
Medida de seguridad*	**Acciones***	**Responsable***
Seguridad SSL	a) Implementar protocolo SSL en el servidor que alberga el sistema. b) Mantener vigente el certificado SSL y verificar s correcto funcionamiento.	a) Raúl Ricardo Hernández Serrano b) Periodicidad trimestral
Corrección de errores en sistema	a) Habilitar bitácoras individuales por sistema dentro del servidor b) Atención a la notificación de errores por parte de usuarios y detectados en las bitácoras.	a) Raúl Ricardo Hernández Serrano b) Bajo demanda

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General	
Identificador único*	SG-04-CPICT-04
Nombre del sistema *	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)

Actividad*	Descripción*	Duración*	Cobertura*
Los responsables de seguridad de datos personales no han recibido capacitación.			

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-04-CPICT-04		
Nombre del sistema *	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-04-CPICT-04		
Nombre del sistema *	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Incorporación de nuevas características	Actualización de los parámetros de funcionamiento del sistema acorde al semestre en cuestión	2 semanas, periodicidad: semestral	Ajuste para la captura de nuevas solicitudes.
Actualización de tablas de datos	Actualización de académicos y funcionarios respecto a la nómina que libera	1 hora, periodicidad: quincenal	Se registran nuevos usuarios para que puedan acceder al sistema y se inactivan

	cada quincena la DGP		usuarios que no están vigentes en nómina.

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-04-CPICT-04		
Nombre del sistema *	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Limpieza de equipo	Limpieza de polvo y residuos en componentes internos y conectores del equipo con sopladora de aire y brocha	2 horas cada 6 meses	Reestablecer la capacidad de enfriamiento del equipo
Inspección visual de componentes electrónicos	Verificar que capacitores y placas electrónicas no presenten signos de desgaste o fin de vida útil	2 horas cada 6 meses	
Reemplazo de pasta térmica	Remover material de intercambio térmico reseco y aplicar nuevo	2 horas cada año	Reestablecer la capacidad de enfriamiento del equipo

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-04-CPICT-04	
Nombre del sistema *	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)	
Proceso*	**Descripción***	**Responsable***
Respaldo semanal en disco duro externo	1. Respaldar base de datos completa	Responsable: Christian Mitchel Elizalde Rivera

	2. Respaldar código fuente y recursos del sistema	Tiempo máximo de ejecución en días: 1
Respaldo diario automatizado en servidor de respaldo	1. Respaldar base de datos completa 2. Respaldar código fuente y recursos del sistema	Responsable: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 1

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General		
Identificador único*	SG-04-CPICT-04	
Nombre del sistema *	Sistema de Carga Académica de la Facultad de Ingeniería (CAFI)	
Proceso*	**Descripción***	**Responsable***
Borrado seguro de aplicativo y recursos	- Identificación de directorios que contienen al aplicativo y recursos - Ejecución de comandos para borrado seguro en sistema de archivos del dispositivo de almacenamiento	Nombre del responsable del proceso: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 3
Disposición final de dispositivos de almacenamiento internos y externos	- Extracción del dispositivo de almacenamiento del gabinete. - Desmantelamiento de componentes internos que almacenan información como chips de memoria y discos. - Lijado de superficies de discos y destrucción de chips de memoria.	Nombre del responsable del proceso: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 3

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

Módulo de concursos de oposición

Permite la gestión de los concursos de oposición cerrados. El módulo es para uso exclusivo de jefes de división y miembros de las Comisiones Dictaminadoras de la Facultad de Ingeniería.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-05-CPICT-05
Nombre del sistema *	Módulo de concursos de oposición
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, correo electrónico, teléfono particular, teléfono de oficina, teléfono móvil, RFC, CURP, número de trabajador.
Responsable*:	Facultad de Ingeniería
Nombre*:	Víctor Hugo Tovar Pérez
Cargo*:	Coordinador de la CPICT
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema y el rol que tendrán. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema que impactan en el tratamiento de datos personales. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas. - Validar los procesos y reglas de negocio con las que opera el sistema.
	Encargados:
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	Christian Mitchel Elizalde Rivera
Cargo*:	Técnico Académico
Funciones*:	Administrar el sistema, esta actividad involucra la actualización de los datos personales de los académicos provistos por otras instancias de la UNAM
Obligaciones*:	Procurar el correcto despliegue de información únicamente a los usuarios involucrados en las diferentes etapas del proceso
(Nombre del Usuario 2*)	Raúl Ricardo Hernández Serrano
Cargo*:	Ayudante de profesor

Funciones*:	Monitorear las bitácoras del sistema para determinar posibles afectaciones, ataques y errores del sistema
Obligaciones*:	Solventar las vulnerabilidades en cuanto al acceso de usuarios
(Nombre del Usuario 3*)	Jefes de División de la Facultad de Ingeniería
Cargo*:	Jefe de División
Funciones*:	Revisar las solicitudes y descargar los formatos de opinión institucional de los académicos adscritos a su División
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 4*)	Comisiones Dictaminadoras de la Facultad de Ingeniería
Cargo*:	Miembro de Comisión Dictaminadora
Funciones*:	Revisar las solicitudes y descargar los formatos de evaluación de Concurso de Oposición Cerrado que han solicitado los académicos de la Facultad de Ingeniería
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 5*)	Personal de apoyo de la CPICT
Cargo*:	Encargados del área de Normatividad académica
Funciones*:	Poner a disposición de la Comisión de Evaluación las solicitudes recibidas de los académicos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos Personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-05-CPICT-05
(Nombre del sistema A1*)	Módulo de concursos de oposición
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos y archivos digitales proporcionados por los usuarios.
Características del lugar donde se resguardan los soportes: *	Servidor productivo ubicado en la oficina de la Coordinación de Procesos e Información del Consejo Técnico.

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 58 a 60.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-05-CPICT-05
Nombre del sistema *	Módulo de concursos de oposición
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema no realiza tratamiento de datos personales con soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**
   - **a)** Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

     Se registra el inicio de sesión exitoso en el sistema con fecha, hora, identidad, rol y dirección IP.

   - **b)** Para soportes físicos: Número o clave del expediente utilizado, y

     No se utilizan soportes físicos.

   - **c)** Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

     Solo se registra el inicio de sesión exitoso.
2. **Si las bitácoras están en soporte físico o en soporte electrónico;**
   Bitácoras en soporte electrónico.
3. **Lugar dónde almacena las bitácoras y por cuánto tiempo;**
   Archivos *.log dentro del sistema. Se almacenan por 4 años.
4. **La manera en que asegura la integridad de las bitácoras, y**
   El acceso a las bitácoras está restringido al administrador del servidor.
5. **Respecto del análisis de las bitácoras:**
   - **a)** Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero)

y cada cuándo las analiza, y

El área universitaria. Se analizan bajo demanda para corroborar temporalidad de algún incidente.

b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

Editor de texto y hoja de cálculo.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento o registro de incidentes.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

   Para las personas que acceden a sus instalaciones:

   a) ¿Cómo las identifica?
   No se cuenta con mecanismos de identificación

   b) ¿Cómo las autentifica?
   No se cuenta con mecanismos de autenticación.

   c) ¿Cómo les autoriza el acceso?
   No se cuenta con mecanismos de control de acceso.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

   Para las personas que acceden a dichos espacios interiores:

   1. ¿Cómo las identifica?
      Mediante la credencial de trabajador vigente.
   2. ¿Cómo las autentifica?
      Mediante la credencial de trabajador cuyo nombre coincide con los colaboradores publicados en portal.
   3. ¿Cómo les autoriza el acceso?
      Cuentan con llaves para el acceso al espacio donde se encuentra el servidor.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La información del personal académico y funcionariado se actualiza con base en la Nómina de la Facultad de Ingeniera, y los catálogos del Sistema de Información de Personal proporcionados por la Dirección General de Personal (DGP). Esta actualización comprende:

- Corrección de datos como: RFC, CURP, primer apellido, segundo apellido, y nombres.
- Inhabilitación de usuarios al no detectar su vigencia en nómina.
- Registro de personal de nueva contratación.

La frecuencia de actualización es quincenal. Estos datos son verificados previamente por la DGP.

Adicionalmente, el personal académico puede registrar, actualizar o borrar sus datos de: correo electrónico, teléfono de oficina y teléfono móvil. La modificación de esta información puede realizarse en cualquier momento en tanto la persona interesada esté vigente en la Nómina de la Facultad de Ingeniería.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
Sí
b) ¿Es discrecional (matriz de control de acceso)?
Sí
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo se cifra la contraseña al ser almacenada.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo se cifra la contraseña al ser almacenada.

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
El administrador del sistema.
b) ¿Quién autoriza la creación de nuevos perfiles?
El Coordinador de la CPICT.
c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí
c) ¿Cómo se evita el acceso remoto no autorizado?
Lista blanca de usuarios con acceso mediante SSH. Autenticación a través de infraestructura de llave pública.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos __X__, diferenciales ___ o incrementales __X__;
   b) De forma automática __X__ o Manual __X__,
   c) Periodicidad con que los realiza: __diario y semana
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
   Discos duros externos y servidor de respaldo.
3. Cómo y dónde archiva esos medios, y
   Discos duros externos: se encuentran bajo resguardo del Coordinador de la CPICT.
   Servidor de respaldo: instalaciones de la CPICT.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   El área universitaria.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   Se cuenta con un servidor de respaldo que se sincroniza de forma automática una vez al día. Este servidor cambiaría a productivo en cuanto surja una contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No se han realizado pruebas de eficiencia. Se estima que el procedimiento para dar continuidad de la operación tarde menos de 3 horas en horarios y días hábiles.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);
   b) Si el sitio es propio o subcontratado con un tercero;
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.
   No se cuenta con un sitio redundante.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-05-CPICT-05	
Nombre del sistema *	Módulo de concursos de oposición	
Recurso*	**Descripción***	**Control***
Auditoría de seguridad	Se utilizan herramientas de penetración para detectar puertos abiertos y recursos sin control de acceso.	El responsable es el administrador del servidor.

		Las herramientas cuentan con licencia de software libre.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-05-CPICT-05	
Nombre del sistema *	Módulo de concursos de oposición	
Medida de seguridad*	**Procedimiento***	**Responsable***
Pruebas de vulnerabilidad	Se realizaron pruebas de penetración al servidor que hospeda al sistema como parte de una Auditoría de Seguridad para la integración a la infraestructura de FEU de otro sistema.	a) Raúl Ricardo Hernández Serrano b) Septiembre de 2021

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-05-CPICT-05	
Nombre del sistema *	Módulo de concursos de oposición	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Pruebas de vulnerabilidad	La cantidad de incidentes de seguridad con impacto bajo	a) Raúl Ricardo Hernández Serrano b) Septiembre de 2021

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General	
Identificador único*	SG-05-CPICT-05
Nombre del sistema *	Módulo de concursos de oposición

Medida de seguridad*	Acciones*	Responsable*
Seguridad SSL	a) Implementar protocolo SSL en el servidor que alberga el sistema. b) Mantener vigente el certificado SSL y verificar s correcto funcionamiento.	a) Raúl Ricardo Hernández Serrano b) Periodicidad trimestral
Corrección de errores en sistema	a) Habilitar bitácoras individuales por sistema dentro del servidor b) Atención a la notificación de errores por parte de usuarios y detectados en las bitácoras.	a) Raúl Ricardo Hernández Serrano b) Bajo demanda

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-05-CPICT-05		
Nombre del sistema *	Módulo de concursos de oposición		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Los responsables de seguridad de datos personales no han recibido capacitación.			

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-05-CPICT-05		
Nombre del sistema *	Módulo de concursos de oposición		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión			

de la protección de datos personales.			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-05-CPICT-05		
Nombre del sistema *	Módulo de concursos de oposición		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Incorporación de nuevas características	Actualización de los parámetros de funcionamiento del sistema acorde al semestre en cuestión	2 semanas, periodicidad: semestral	Ajuste para la captura de nuevas solicitudes.
Actualización de tablas de datos	Actualización de académicos y funcionarios respecto a la nómina que libera cada quincena la DGP	1 hora, periodicidad: quincenal	Se registran nuevos usuarios para que puedan acceder al sistema y se inactivan usuarios que no están vigentes en nómina.

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-05-CPICT-05		
Nombre del sistema *	Módulo de concursos de oposición		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Limpieza de equipo	Limpieza de polvo y residuos en componentes internos y conectores del equipo con	2 horas cada 6 meses	Reestablecer la capacidad de enfriamiento del equipo

	sopladora de aire y brocha		
Inspección visual de componentes electrónicos	Verificar que capacitores y placas electrónicas no presenten signos de desgaste o fin de vida útil	2 horas cada 6 meses	
Reemplazo de pasta térmica	Remover material de intercambio térmico reseco y aplicar nuevo	2 horas cada año	Reestablecer la capacidad de enfriamiento del equipo

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-05-CPICT-05	
Nombre del sistema *	Módulo de concursos de oposición	
Proceso*	**Descripción***	**Responsable***
Respaldo semanal en disco duro externo	1. Respaldar base de datos completa 2. Respaldar código fuente y recursos del sistema	Responsable: Christian Mitchel Elizalde Rivera Tiempo máximo de ejecución en días: 1
Respaldo diario automatizado en servidor de respaldo	1. Respaldar base de datos completa 2. Respaldar código fuente y recursos del sistema	Responsable: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 1

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General	
Identificador único*	SG-05-CPICT-05
Nombre del sistema *	Módulo de concursos de oposición

Proceso*	Descripción*	Responsable*
Borrado seguro de aplicativo y recursos	- Identificación de directorios que contienen al aplicativo y recursos - Ejecución de comandos para borrado seguro en sistema de archivos del dispositivo de almacenamiento	Nombre del responsable del proceso: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 3
Disposición final de dispositivos de almacenamiento internos y externos	- Extracción del dispositivo de almacenamiento del gabinete. - Desmantelamiento de componentes internos que almacenan información como chips de memoria y discos. - Lijado de superficies de discos y destrucción de chips de memoria.	Nombre del responsable del proceso: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 3

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)

Permite la inscripción de aspirantes a los Concursos de Oposición Abiertos de la Facultad de Ingeniería publicados en Gaceta UNAM. Además, es utilizado por las Comisiones Dictaminadora en los procesos de aceptación de aspirantes y evaluación de los participantes.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-06-CPICT-06
Nombre del sistema *	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, correo electrónico, teléfono particular, teléfono de oficina, teléfono móvil, RFC, CURP, número de trabajador.
Responsable*:	Facultad de Ingeniería
Nombre*:	Víctor Hugo Tovar Pérez
Cargo*:	Coordinador de la CPICT
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema y el rol que tendrán. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema que impactan en el tratamiento de datos personales. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas. - Validar los procesos y reglas de negocio con las que opera el sistema.
	Encargados:
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	Raúl Ricardo Hernández Serrano
Cargo*:	Ayudante de profesor
Funciones*:	- Administrar el sistema, esta actividad involucra la actualización de los datos personales de los académicos provistos por otras instancias de la UNAM. - Monitorear las bitácoras del sistema para determinar posibles afectaciones, ataques y errores del sistema.
Obligaciones*:	- Procurar el correcto despliegue de información únicamente a los usuarios involucrados en las diferentes etapas del

	proceso. - Solventar las vulnerabilidades en cuanto al acceso de usuarios.
(Nombre del Usuario 2*)	Comisiones Dictaminadoras de la Facultad de Ingeniería
Cargo*:	Miembro de Comisión Dictaminadora
Funciones*:	Revisar las solicitudes y descargar los formatos de evaluación de Concurso de Oposición Cerrado que han solicitado los académicos de la Facultad de Ingeniería
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 3*)	Personal de apoyo de la CPICT
Cargo*:	Encargados del área de Normatividad académica
Funciones*:	Poner a disposición de la Comisión de Evaluación las solicitudes recibidas de los académicos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos Personales.

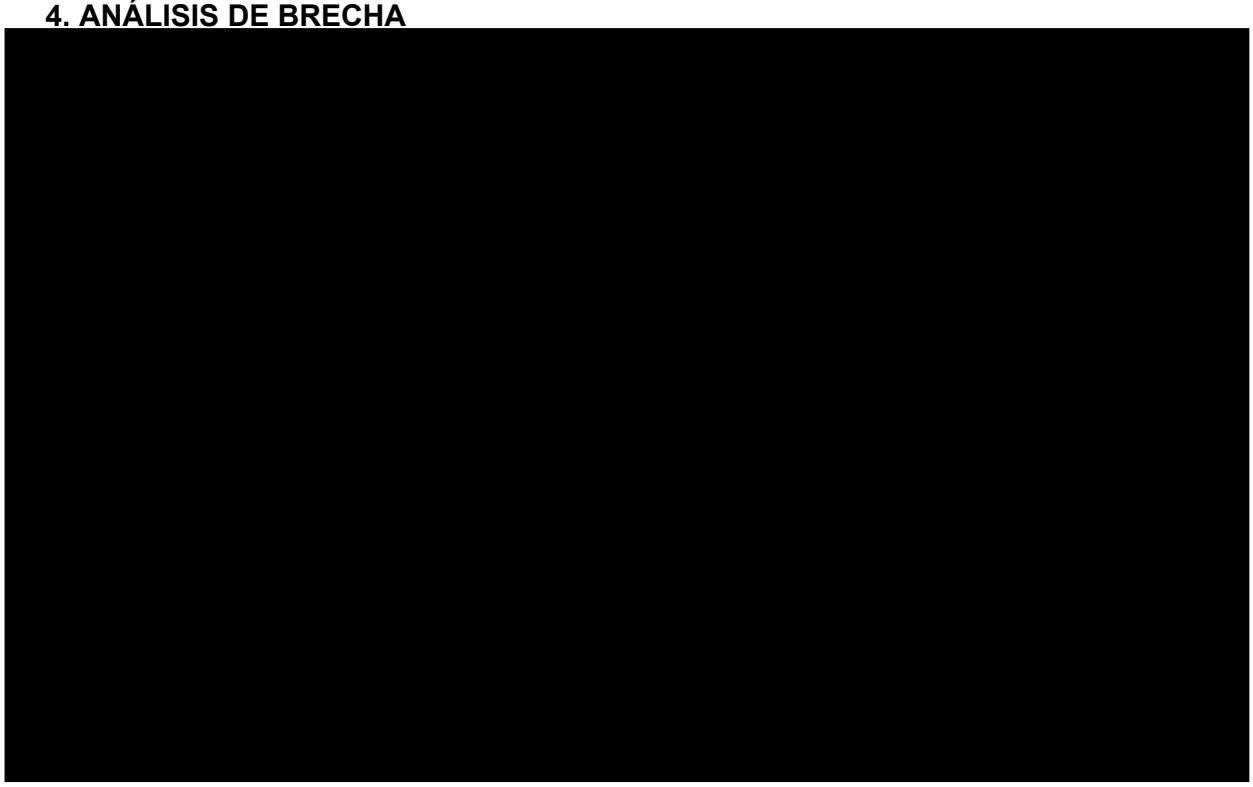
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-06-CPICT-06
(Nombre del sistema A1*)	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos y archivos digitales proporcionados por los usuarios.
Características del lugar donde se resguardan los soportes: *	Servidor productivo ubicado en la oficina de la Coordinación de Procesos e Información del Consejo Técnico.

3. ANÁLISIS DE RIESGOS

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 70 a 72.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA



5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-06-CPICT-06
Nombre del sistema *	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema no realiza tratamiento de datos personales con soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

Se registra el inicio de sesión exitoso en el sistema con fecha, hora, identidad, rol y dirección IP.

b) Para soportes físicos: Número o clave del expediente utilizado, y

No se utilizan soportes físicos.

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

Solo se registra el inicio de sesión exitoso.

2. **Si las bitácoras están en soporte físico o en soporte electrónico;**
   Bitácoras en soporte electrónico.
3. **Lugar dónde almacena las bitácoras y por cuánto tiempo;**
   Archivos *.log dentro del sistema. Se almacenan por 4 años.
4. **La manera en que asegura la integridad de las bitácoras, y**
   El acceso a las bitácoras está restringido al administrador del servidor.
5. **Respecto del análisis de las bitácoras:**
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y

   El área universitaria. Se analizan bajo demanda para corroborar temporalidad de algún incidente.

   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

   Editor de texto y hoja de cálculo.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento o registro de incidentes.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

   Para las personas que acceden a sus instalaciones:

   a) ¿Cómo las identifica?
   No se cuenta con mecanismos de identificación

   b) ¿Cómo las autentifica?
   No se cuenta con mecanismos de autenticación.

   c) ¿Cómo les autoriza el acceso?
   No se cuenta con mecanismos de control de acceso.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

   Para las personas que acceden a dichos espacios interiores:

   1. ¿Cómo las identifica?
      Mediante la credencial de trabajador vigente.
   2. ¿Cómo las autentifica?
      Mediante la credencial de trabajador cuyo nombre coincide con los colaboradores publicados en portal.
   3. ¿Cómo les autoriza el acceso?
      Cuentan con llaves para el acceso al espacio donde se encuentra el servidor.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La información del personal académico y funcionariado se actualiza con base en la Nómina de la Facultad de Ingeniera, y los catálogos del Sistema de Información de Personal proporcionados por la Dirección General de Personal (DGP). Esta actualización comprende:

- Corrección de datos como: RFC, CURP, primer apellido, segundo apellido, y nombres.
- Inhabilitación de usuarios al no detectar su vigencia en nómina.
- Registro de personal de nueva contratación.

La frecuencia de actualización es quincenal. Estos datos son verificados previamente por la DGP.

Adicionalmente, el personal académico puede registrar, actualizar o borrar sus datos de: correo electrónico, teléfono de oficina y teléfono móvil. La modificación de esta información puede realizarse en cualquier momento en tanto la persona interesada esté vigente en la Nómina de la Facultad de Ingeniería.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
Sí
b) ¿Es discrecional (matriz de control de acceso)?
Sí
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo se cifra la contraseña al ser almacenada.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo se cifra la contraseña al ser almacenada.

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
El administrador del sistema.
b) ¿Quién autoriza la creación de nuevos perfiles?
El Coordinador de la CPICT.
c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?

No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?

Sí

c) ¿Cómo se evita el acceso remoto no autorizado?

Lista blanca de usuarios con acceso mediante SSH. Autenticación a través de infraestructura de llave pública.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos __X__, diferenciales ___ o incrementales __X__;

b) De forma automática __X__ o Manual __X__,

c) Periodicidad con que los realiza: __diario y semana

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:

Discos duros externos y servidor de respaldo.

3. Cómo y dónde archiva esos medios, y

Discos duros externos: se encuentran bajo resguardo del Coordinador de la CPICT.

Servidor de respaldo: instalaciones de la CPICT.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

El área universitaria.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

Se cuenta con un servidor de respaldo que se sincroniza de forma automática una vez al día. Este servidor cambiaría a productivo en cuanto surja una contingencia.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

No se han realizado pruebas de eficiencia. Se estima que el procedimiento para dar continuidad de la operación tarde menos de 3 horas en horarios y días hábiles.

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) El tipo de sitio (caliente, tibio o frío);

b) Si el sitio es propio o subcontratado con un tercero;

c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y

d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

No se cuenta con un sitio redundante.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-06-CPICT-06	
Nombre del sistema *	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)	
Recurso*	**Descripción***	**Control***
Auditoría de seguridad	Se utilizan herramientas de penetración para detectar puertos abiertos y recursos sin control de acceso.	El responsable es el administrador del servidor. Las herramientas cuentan con licencia de software libre.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-06-CPICT-06	
Nombre del sistema *	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Pruebas de vulnerabilidad	Se realizaron pruebas de penetración al servidor que hospeda al sistema como parte de una Auditoría de Seguridad para la integración a la infraestructura de FEU de otro sistema.	a) Raúl Ricardo Hernández Serrano b) Septiembre de 2021

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-06-CPICT-06	
Nombre del sistema *	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***

Pruebas de vulnerabilidad	La cantidad de incidentes de seguridad con impacto bajo	a) Raúl Ricardo Hernández Serrano b) Septiembre de 2021

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-06-CPICT-06	
Nombre del sistema *	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)	
Medida de seguridad*	**Acciones***	**Responsable***
Seguridad SSL	a) Implementar protocolo SSL en el servidor que alberga el sistema. b) Mantener vigente el certificado SSL y verificar su correcto funcionamiento.	a) Raúl Ricardo Hernández Serrano b) Periodicidad trimestral
Corrección de errores en sistema	a) Habilitar bitácoras individuales por sistema dentro del servidor b) Atención a la notificación de errores por parte de usuarios y detectados en las bitácoras.	a) Raúl Ricardo Hernández Serrano b) Bajo demanda

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-06-CPICT-06		
Nombre del sistema *	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Los responsables de seguridad de datos personales no han recibido capacitación.			

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-06-CPICT-06		
Nombre del sistema *	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-06-CPICT-06		
Nombre del sistema *	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Incorporación de nuevas características	Actualización de los parámetros de funcionamiento del sistema acorde al semestre en cuestión	2 semanas, periodicidad: semestral	Ajuste para la captura de nuevas solicitudes.
Actualización de tablas de datos	Actualización de académicos y funcionarios respecto a la nómina que libera	1 hora, periodicidad: quincenal	Se registran nuevos usuarios para que puedan acceder al sistema y se inactivan usuarios que no están vigentes en nómina.

	cada quincena la DGP		

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-06-CPICT-06		
Nombre del sistema *	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Limpieza de equipo	Limpieza de polvo y residuos en componentes internos y conectores del equipo con sopladora de aire y brocha	2 horas cada 6 meses	Reestablecer la capacidad de enfriamiento del equipo
Inspección visual de componentes electrónicos	Verificar que capacitores y placas electrónicas no presenten signos de desgaste o fin de vida útil	2 horas cada 6 meses	
Reemplazo de pasta térmica	Remover material de intercambio térmico reseco y aplicar nuevo	2 horas cada año	Reestablecer la capacidad de enfriamiento del equipo

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-06-CPICT-06	
Nombre del sistema *	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)	
Proceso*	**Descripción***	**Responsable***
Respaldo semanal en disco duro externo	1. Respaldar base de datos completa	Responsable: Christian Mitchel Elizalde Rivera

	2. Respaldar código fuente y recursos del sistema	Tiempo máximo de ejecución en días: 1
Respaldo diario automatizado en servidor de respaldo	1. Respaldar base de datos completa 2. Respaldar código fuente y recursos del sistema	Responsable: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 1

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General		
Identificador único*	SG-06-CPICT-06	
Nombre del sistema *	Sistema Electrónico para Concursos de Oposición Abiertos (SECOA)	
Proceso*	**Descripción***	**Responsable***
Borrado seguro de aplicativo y recursos	- Identificación de directorios que contienen al aplicativo y recursos - Ejecución de comandos para borrado seguro en sistema de archivos del dispositivo de almacenamiento	Nombre del responsable del proceso: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 3
Disposición final de dispositivos de almacenamiento internos y externos	- Extracción del dispositivo de almacenamiento del gabinete. - Desmantelamiento de componentes internos que almacenan información como chips de memoria y discos. - Lijado de superficies de discos y destrucción de chips de memoria.	Nombre del responsable del proceso: Raúl Ricardo Hernández Serrano Tiempo máximo de ejecución en días: 3

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

ÍNDICE

Coordinación del Sistema de Bibliotecas (CSB)

La Coordinación del Sistema de Bibliotecas (CSB) de la Facultad de Ingeniería (FI), creada en el año 2000 y actualmente adscrita a la Secretaría General de la FI, está conformada por cinco bibliotecas de las cuales tres se encuentran en el campus de Ciudad Universitaria: Biblioteca Mtro. Enrique Rivero Borrell, ubicada en el Conjunto Sur o Anexo de Ingeniería, para el área de ciencias básicas, Biblioteca Ing. Antonio Dovalí Jaime, en el Conjunto Norte, para el área de estudios profesionales, y Biblioteca Dr. Enzo Levi, para el área de posgrado y especialidad; las bibliotecas que están fuera del campus y que físicamente se localizan en el Palacio de Minería son la Biblioteca Ing. Antonio M. Anza, que resguarda el Acervo Histórico, y el Centro de Información y Documentación Ing. Bruno Mascanzoni, para apoyo de los cursos que imparte la División de Educación Continua y a Distancia del plantel.

Cada biblioteca cuenta con un edificio ex profeso con mobiliario, salas de lectura, espacio para acervos y cubículos de estudio (solo en las bibliotecas Mtro. Enrique Rivero Borrell y Dr. Enzo Levi), además de un taller de conservación y restauración en la biblioteca histórica ubicada en el Palacio de Minería. Se cuenta con infraestructura tecnológica para conexión a RedUNAM y redes inalámbricas, además del apoyo de personal administrativo, académico y de confianza.

LA CSB administra el sistema bibliotecario de la FI con la finalidad de proveer recursos bibliohemerográficos y servicios bibliotecarios y de información con calidad, agilidad y oportunidad que habiliten a la comunidad de ingeniería para el desarrollo de sus actividades, sean la docencia, la investigación o la difusión de la cultura nacional e internacional.

El Sistema de Bibliotecas de la FI pertenece al Sistema Bibliotecario de la UNAM, administrado y regulado por la Dirección General de Bibliotecas y Servicios Digitales de Información. Internamente, se cuenta con un reglamento y una Comisión de Bibliotecas.

Repositorio digital institucional REPOFI

El sistema que administra la CSB es el repositorio digital institucional, que tiene como objetivo recolectar, preservar y compartir materiales emanados de la comunidad de la FI, organizados en comunidades, subcomunidades y, en algunos casos, colecciones.

Comunidades:

- Acervo Histórico del Palacio de Minería
- Apuntes Facultad de Ingeniería
- División de Educación Continua y a Distancia
- Ediciones Facultad de ingeniería
- Publicaciones Académicas
- Taller de Publicación
- Trabajos escritos para titulación

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-07-CSB-01
Nombre del sistema *	Repositorio digital institucional REPOFI
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre completo del autor o autores del trabajo, nombre completo de directores/asesores de trabajo de titulación, correo electrónico (personal o institucional), número de cuenta, carrera o división de adscripción, teléfono.
Responsable*:	Coordinación del Sistema de Bibliotecas de la Facultad de Ingeniería
Nombre*:	Esp. María de Guadalupe Flor Díaz de León Fernández de Castro
Cargo*:	Coordinadora del Sistema de Bibliotecas Facultad de Ingeniería
Funciones*:	Recibir las respectivas solicitudes sobre la creación de comunidades y su aprobación. Valorar los contenidos de estas comunidades. Solicitar cambios pertinentes al sistema.
Obligaciones*:	Tener conocimiento semestral sobre el estatus del sistema y sobre incidencias irregulares cuando se presenten; supervisar el trabajo de la persona encargada del sistema.
	Encargados:
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	M.A.T. Sergio Israel Franco García

Cargo*:	Responsable de Cómputo de las bibliotecas de estudios profesionales de la FI y Jefe de Proyectos de Cómputo de la CSB. Es el creador, diseñador y administrador del sistema.
Funciones*:	• Administrar el servidor o equipo del repositorio digital institucional. • Mantener la integridad del sistema y su correcto funcionamiento y el acceso a los contenidos del mismo.
Obligaciones*:	• Determinar el nivel de privilegio de acceso que tienen los usuarios responsables de la publicación y la edición de los trabajos o publicaciones que son ingresados al repositorio. • Realizar los cambios solicitados por la persona responsable de la Coordinación del Sistema de Bibliotecas en apoyo de las Jefaturas de las bibliotecas. • Asegurar los respaldos periódicos de la información, así como el adecuado soporte técnico del equipo de cómputo asignado para tal fin.
(Nombre del Usuario 2*)	Edith Galindo Morales
Cargo*:	Jefa de la Biblioteca “Ing. Antonio Dovalí Jaime”
Funciones*:	Revisar y aprobar el acceso de los trabajos escritos de titulación para los estudiantes de la Facultad de Ingeniería, nivel licenciatura.
Obligaciones*:	Mantener la confidencialidad de los datos proporcionados por el usuario, además del resguardo.
(Nombre del Usuario 3*)	Gabriela De Paz Mejía
Cargo*:	Responsable de Cómputo y Servicios de Información de la Biblioteca “Dr. Enzo Levi”
Funciones*:	Publicar, editar y aprobar el contenido de los trabajos escritos de titulación para los alumnos de la especialidad en Ingeniería.
Obligaciones*:	Mantener la integridad y confidencialidad de los datos proporcionados por el usuario.
(Nombre del Usuario 4*)	Personal administrativo asignado al área de titulación de la Biblioteca “Ing. Antonio Dovalí Jaime”
Cargo*:	Bibliotecario
Funciones*:	Asegurar el registro del trabajo que el usuario final coloca en el repositorio. Revisar los metadatos asociados a la información del trabajo escrito.
Obligaciones*:	Mantener la confidencialidad del usuario.
(Nombre del Usuario 5*)	Mtro. Arturo López Cardiel
Cargo*:	Coordinador de Tecnologías de la Información y Comunicación del Palacio de Minería
Funciones*:	Publicar, editar y aprobar el contenido de los cursos generados por la División de Educación Continua y a Distancia.
Obligaciones*:	Mantener la integridad y confidencialidad de los datos proporcionados por el autor.
(Nombre del Usuario 5*)	Lic. Patricia Eugenia García Naranjo
Cargo*:	Jefa de la Unidad de Apoyo Editorial
Funciones*:	Aprobar, editar y publicar el trabajo escrito de profesores de la Facultad de Ingeniería.
Obligaciones*:	Mantener la confidencialidad y asegurarse de la integridad de los datos proporcionados por el profesor.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-07-CSB-01
Nombre del sistema *	Repositorio digital institucional REPOFI
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos
Características del lugar donde se resguardan los soportes: *	Disco duro externo

3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 84 a 85.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-07-CSB-01
Nombre del sistema *	Repositorio digital institucional REPOFI

TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Mantener el acceso controlado y el disco duro de respaldo en un mueble bajo llave; sólo el responsable del sistema del repositorio tiene acceso al respaldo físico.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.
M.A.T. Sergio Israel Franco García. Jefe de Proyectos de Cómputo de la CSB. Administrador y diseñador del repositorio digital.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**

   a) En las bitácoras no se indican datos personales y cotidianamente sólo tiene acceso y las maneja directamente el encargado de este sistema.
   b) En el caso del soporte físico: no se utiliza.
   c) Para soportes electrónicos, únicamente el administrador y encargado del repositorio tiene acceso a la base de datos.
2. Las bitácoras están en soporte electrónico.
3. Las bitácoras se almacenan sólo en el equipo del encargado del repositorio, desde el 2º. semestre de 2017.
4. La integridad de las bitácoras se asegura con el acceso exclusivo del encargado del sistema. Su equipo tiene contraseña para el acceso y se encuentra en una oficina de uso personal que tiene llave.
5. Respecto del análisis de las bitácoras:
   a) La persona encargada del repositorio analiza semestralmente las bitácoras, para integrar esta actividad en su informe como técnico académico.
   b) La herramienta de análisis utilizada para las bitácoras en soporte electrónico es el uso de hoja de cálculo, para estadísticas.

IV. REGISTRO DE INCIDENTES

Los registros de incidentes se realizan mediante una bitácora elaborada en una hoja de cálculo, anotando el nombre de la incidencia y cómo fue resuelta; el archivo está de manera electrónica, resguardada por el encargado del repositorio en su equipo de trabajo personal, al cual sólo él tiene acceso mediante una clave, y que respalda en un disco SSD. El encargado del sistema, como parte de sus responsabilidades y funciones, es quien realiza la recuperación de datos, con la autorización de la persona al frente de la CSB.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

1. ¿Cómo las identifica?
No se cuenta con mecanismos de identificación
2. ¿Cómo las autentifica?
No se cuenta con mecanismos de autenticación
3. ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica? Se les identifica al ser parte de la CSB o de la comunidad académica de la Facultad de Ingeniería, o bien se les invita a que proporcionen sus datos de estatus y de procedencia.
2. ¿Cómo las autentifica? Si es necesario, se les solicita una identificación oficial.
3. ¿Cómo les autoriza el acceso? Autenticando su identidad y verificando el motivo por el cual se encuentran en el espacio.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En el caso de datos equivocados registrados por usuarios en el proceso de subir documentos al repositorio, el mismo sistema genera mecanismos para dar aviso sobre la necesidad de rectificar la información, hasta que se registran correctamente, lo que permite avanzar y concluir tal proceso.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Los perfiles de usuarios están perfectamente definidos y validados por el administrador del sistema y es mediante este mismo que se consultan. Cada perfil está asociado de acuerdo con la colección que ingresa el usuario, con un login y password que les permite subir, publicar o editar la información que es colocada en el repositorio, por lo que está basado en roles.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

Para acceder al sistema del repositorio digital institucional no se requiere de un software especial ni existe un sistema exclusivo o un navegador exclusivo, únicamente con el usuario y la contraseña.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

El repositorio digital institucional está configurado y creado a partir de la herramienta para la organización de colecciones digitales, que le da el tipo de soporte que requiere y permite su administración.

4. Administración de perfiles de usuario y contraseñas: El administrador es el encargado de crear nuevos perfiles en acuerdo con la Coordinación del Sistema de Bibliotecas; los alumnos que suben sus trabajos crean una cuenta que les permite depositar el trabajo. El registro de un nuevo perfil lo hace directamente el encargado del sistema, y estos se mantienen dentro del sistema.

5. Acceso remoto al sistema de tratamiento de datos personales:

Los usuarios que publican o tienen perfil de editor, tienen acceso remoto al equipo mediante la validación de usuario y contraseña, el administrador también mantiene un sistema de acceso para remotamente hacer revisiones o mantenimiento al equipo, en caso de ser necesario.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_x_ e incrementales_x_;
   b) De forma Manual _____x___,
   c) Periodicidad con que los realiza: ___Mensual_____
2. El tipo de medios: Disco Duro externo, para almacenar las copias de seguridad;
3. Cómo y dónde archiva esos medios: en la oficina del encargado del sistema; el disco se resguarda bajo llave.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero): el encargado del sistema.

IX. PLAN DE CONTINGENCIA

El plan de contingencia no está escrito; sin embargo, se realiza un monitoreo cotidiano. Cuando se presenta un problema con el equipo que respalda el sistema, se realiza la primera intervención, que consiste en la revisión física del mismo; en caso de que el problema no pueda ser atendido *in situ*, se solicita la intervención del mantenimiento correctivo mediante el SIC. Asimismo, se hace registro de las incidencias y se informa a usuarios y a todas las instancias afectadas en caso de que el problema tome un tiempo considerable de reparación y no se tenga acceso al mismo, pues no se cuenta con un equipo alternativo para solventar dicha situación.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-07-CSB-01	
Nombre del sistema *	Repositorio digital institucional REPOFI	
Recurso*	**Descripción***	**Control***
Para asegurar la integridad del sistema y de la protección de datos, se cuenta con un firewall.	El programa genera una bitácora que registra cualquier incidencia o evento.	Se trata de software libre.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-07-CSB-01	
Nombre del sistema *	Repositorio digital institucional REPOFI	
Medida de seguridad*	**Procedimiento***	**Responsable***
Un firewall a nivel de software se encuentra operando dentro del sistema todos los días las24 horas.	El programa crea una bitácora de eventos que es revisada diariamente.	Indicar: a) nombre del responsable del procedimiento Mtro. Sergio Israel Franco García b) tiempo máximo de ejecución en días: todos los días, pues está integrado en el sistema.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-07-CSB-01	
Nombre del sistema *	Repositorio digital institucional REPOFI	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
La instalación de un firewall.	Desde la implementación del servidor no se han reportado incidentes graves, el uso del firewall ha sido suficiente para la protección e integridad del sistema.	a) nombre del responsable de la evaluación: Mtro. Sergio Israel Franco García b) fecha de conclusión: semestral.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-07-CSB-01	
Nombre del sistema *	Repositorio digital institucional REPOFI	
Medida de seguridad*	**Acciones***	**Responsable***
Instalación de un firewall	a) acciones correctivas: se recomienda la instalación de un firewall por medio de hardware. b) acciones preventivas: mantener la versión actualizada del firewall, revisar a diario las bitácoras de incidencias y eventos, solicitar el mantenimiento preventivo por lo menos cada	a) nombre del responsable de las acciones: b) Mtro. Sergio Israel Franco García c) fecha límite de conclusión: semestral y según las necesidades.

	semestre o cada año.	

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-07-CSB-01		
Nombre del sistema *	Repositorio digital institucional REPOFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos que tengan como tema principal el aspecto de la seguridad informática. Cursos relacionados con la administración y seguridad en servidores. Cursos impartidos por el INAI en cuanto a la protección de datos personales.	Cursos de manera presencial o virtual que involucren el tema de la seguridad informática y la administración de servidores.	Cada semestre o cada año.	Fortalecer y mantenerse actualizado en aspectos de seguridad informática y administración de servidores; cada año como mínimo sería recomendable.

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-07-CSB-01		
Nombre del sistema *	Repositorio digital institucional REPOFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Incluir los avisos de protección a datos personales en el repositorio digital institucional.	Se incluye el link o enlace de aviso de protección de datos personales.	Elemento ya incluido de forma permanente en el sitio.	Dar a conocer mediante el sitio web el compromiso de la confidencialidad de los datos personales; la frecuencia dependerá del cambio en la legislación.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General	
Identificador único*	SG-07-CSB-01

Nombre del sistema *	Repositorio digital institucional REPOFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Asegurar que el equipo cuente con las últimas actualizaciones del sistema operativo. El administrador evaluará la pertinencia de compra de un software de licencia para soporte del firewall. Se sugiere la compra de un firewall físico para incrementar la seguridad. Se sugiere la instalación de un servidor espejo que asegure la continuidad de los procesos y la integridad de la información.	Actividad que es de vital importancia para el correcto funcionamiento del sistema (la actualización del sistema operativo). El sistema ha funcionado con software libre de manera óptima; sin embargo, una herramienta adicional es pertinente para reforzar la seguridad. Incrementará la seguridad de la información y la protección de la misma. Asegurar que se tendrá acceso a la información y al sistema.	Las actualizaciones pueden darse en tiempos variables, no tienen una fecha fija, hay que revisarlas a diario, el tiempo de actualización puede tomar de 1 a 2 horas. Una licencia de software se renueva anualmente, el tiempo de actualización puede variar entre 1 y 2 horas.	Con cada una de las actividades enlistadas se cubren de manera total los aspectos que tienen que ver con la seguridad del sistema de información.

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-07-CSB-01		
Nombre del sistema *	Repositorio digital institucional REPOFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Sostener un mantenimiento preventivo del equipo por lo menos cada año o período intersemestral; considerar la contratación de un servicio técnico que garantice la reparación y el reemplazo en caso de ser necesario. Establecer una petición de cambio de infraestructura física	Actividad que es de vital importancia para el correcto funcionamiento del sistema (mantenimiento preventivo). Actividad de suma importancia, ya que dependiendo de los accesos que se tengan y en un equipo que está a disposición las 24 horas del día, se	Las actividades de mantenimiento se pueden realizar cada año como mínimo, solicitándolas por medio de las instancias correspondientes de la dependencia.	Con cada una de las actividades enlistadas se cubre de manera total los aspectos que tienen que ver con la integridad del equipo de cómputo.

por lo menos en un período de 6 a 10 años. Asegurar el mantenimiento y en dado caso sustitución del UPS.	asegura el funcionamiento del mismo.		

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-07-CSB-01	
Nombre del sistema *	Repositorio digital institucional REPOFI	
Proceso*	**Descripción***	**Responsable***
Asegurar el buen funcionamiento del dispositivo que soporta el respaldo de la información, revisar su capacidad y según sea el caso se avisará de la pertinencia de adquisición de un dispositivo electrónico adicional.	En un disco duro externo se lleva a cabo el respaldo periódico de la base de datos, además de aquellos que son editores y publicadores se les proporcionan lineamientos para respaldar su información.	a) Nombre del responsable del proceso: Mtro. Sergio Israel Franco García b) Tiempo máximo de ejecución en días: 1 día

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General		
Identificador único*	SG-07-CSB-01	
Nombre del sistema *	Repositorio digital institucional REPOFI	
Proceso*	**Descripción***	**Responsable***
En caso de cambio de administrador, responsable o editor, se resetearán los accesos y contraseñas; en el caso de las cuentas de usuarios que directamente acceden a subir sus trabajos, las cuentas tienen vigencia de un año, posteriormente expiran los derechos.	El encargado del sistema se encargará de verificar los perfiles de usuario, mismos que están dentro del propio sistema y, a petición de la Coordinación del Sistema de Bibliotecas, de manera automática el sistema revoca los derechos del usuario que hizo su registro de manera directa.	a) Nombre del responsable del proceso: Mtro. Sergio Israel Franco García b) Tiempo máximo de ejecución en días: 1 día

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

ÍNDICE

Departamento de Información y Estadística (DIES)

El **Departamento de Información y Estadística** (DIES) es el órgano institucional que se encarga de realizar y adecuar los procedimientos necesarios para concentrar, clasificar y procesar la información estadística del personal académico de la Facultad, así como la de sus actividades, con el fin de obtener reportes que coadyuven en la toma de decisiones y que reflejen su productividad. Además, cumplir en tiempo y forma con los procesos académico-administrativos que le son encomendados por la Secretaría General y servir de enlace en aquellos en los que la Facultad está vinculada con la Universidad en materia de información académica.

Memoria Estadística

Es un sistema de información que se tiene en la Facultad de Ingeniería para el acopio de las actividades académicas que se realizan a lo largo del año. Una característica importante de este sistema es que se encuentra incorporado para su utilización vía Web, lo que permite ponerlo al alcance de sus distintos usuarios desde sitios remotos, al mismo tiempo en caso de ser necesario y prácticamente en cualquier momento.

Los encargados de actualizar la información requerida en los diversos rubros del sistema son cada una de las Divisiones o Secretarías que conforman la Facultad de Ingeniería, en donde cada una de ellas designa como usuario(s) responsable(s) a la(s) persona(s) que considera conveniente. Se debe contar con nombre de usuario y contraseña válidos para poder acceder a la Memoria Estadística.

Los datos que son recopilados por este sistema se utilizan para varios fines. Parte de ellos se convierten en información que se plasma en el Informe anual de actividades del Director de la Facultad de Ingeniería. Otra parte se procesa, con base en requerimientos específicos, para atender solicitudes de información tanto internas como externas a la Facultad.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-08-DIES-01
Nombre del sistema *	**Memoria Estadística**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos personales RFC, nombre, teléfono, correo electrónico particular, número de trabajador y número de cuenta del alumno. Datos laborales: Nombramiento Datos académicos: Actividades extracurriculares y grado académico.
Responsable*:	Departamento de Información y Estadística
Nombre*:	Ing. David Francisco Jiménez Román
Cargo*:	Jefe del Departamento de Información y Estadística.
Funciones*:	Administrar el correcto uso de los datos recabados en el sistema.
Obligaciones*:	Autorizar el acceso a los encargados designados por cada una de las áreas académicas de la Facultad de Ingeniería. Vigilar el mantenimiento e implementación de medidas de seguridad para la protección de los datos personales. Aprobación de la incorporación y actualización de módulos para recabar los datos reportados por las áreas académicas.
	Encargados:

Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	David Santiago Sobrevilla
Cargo*:	Encargado del área de sistemas.
Funciones*:	Mantenimiento del sistema y atención de requerimientos que permitan recabar de manera correcta los datos. Garantizar la disponibilidad y protección de los datos.
Obligaciones*:	Procurar la protección de los datos personales que recaba el sistema, a través de mecanismos implementados durante el mantenimiento del mismo.
(Nombre del Usuario 2*)	Ivonne Hernández López
Cargo*:	Colaboradora del Departamento de Información y Estadística
Funciones*:	Colaborar con el monitoreo y revisión del correcto funcionamiento del sistema.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 3*)	Véduar Allié Sarmiento Torres
Cargo*:	Técnica Académica
Funciones*:	Colaborar con el análisis y presentación de reportes.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 4*)	Jefes de departamento y colaboradores designados por cada una de las divisiones académicas.
Cargo*:	Jefes de departamento y colaboradores designados por cada una de las divisiones académicas.
Funciones*:	Actualizar la información relativa a la productividad académica de su área y/o de su personal académico.
Obligaciones*:	Resguardar los datos personales y cuidar su confidencialidad e integridad.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único¨*	SG-01-DIES-02
Nombre del sistema*	Memoria estadística
Tipo de soporte: *	Soporte electrónico
Descripción: *	Base de datos
Características del lugar donde se resguardan los soportes: *	Alojamiento en servidor local, ubicado dentro del área del departamento con acceso restringido.

3. ANÁLISIS DE RIESGOS

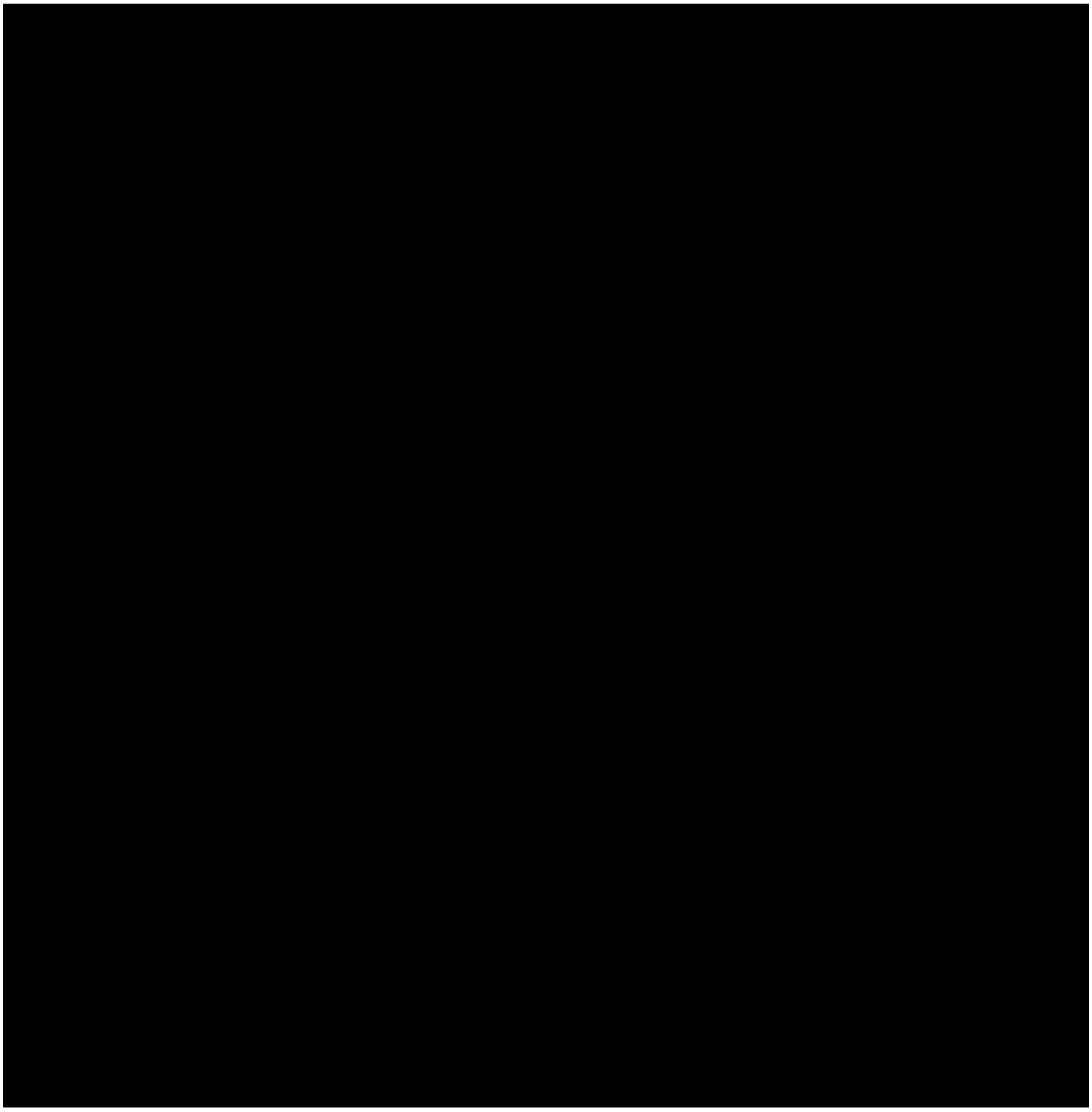
[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 96 a 98.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-08-DIES-01
Nombre del sistema *	Memoria Estadística
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado de sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No se realiza resguardo del sistema Memoria Estadística con soportes físicos, ya que se encuentra en su totalidad en soporte electrónico.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Se generan bitácoras (archivo .log almacenado en el servidor) para desempeño del servidor, donde se registran: intentos de acceso (exitosos y fallidos); fecha y hora de los eventos anteriores; quién accede y desde dónde.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento para la atención de incidentes.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con un mecanismo de identificación.

b) ¿Cómo las autentifica?
No se cuenta con un mecanismo de autenticación.

c) ¿Cómo les autoriza el acceso?
No se cuenta con un mecanismo de acceso.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Se solicita nombre y área de adscripción de las personas externas a la oficina.
   Se tienen los datos del personal autorizado.
2. ¿Cómo las autentifica?
   En caso de ser necesario la autenticación es mediante credencial de académico.
3. ¿Cómo les autoriza el acceso?
   Se tiene un timbre con cámara que permite identificar a la persona.
   La asignación de llaves es administrada por el jefe del departamento.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Únicamente los usuarios registrados en el sistema y designados por cada una de las áreas académicas que integran la Facultad, podrán actualizar los datos personales, a partir de que sea liberado el sistema de manera anual.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? No
b) ¿Es discrecional (matriz de control de acceso)? No
c) ¿Está basado en roles (perfiles) o grupos? Sí
d) ¿Está basado en reglas? No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? Sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? No

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Sí
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? No

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
El responsable del sistema Memoria Estadística
b) ¿Quién autoriza la creación de nuevos perfiles?
El responsable del sistema Memoria Estadística
c) ¿Se lleva registro de la creación de nuevos perfiles?
Sí se lleva registro de la creación de nuevos usuarios

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? No

c) ¿Cómo se evita el acceso remoto no autorizado? Con el uso de firewall y protección por usuario y contraseña

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos__, diferenciales ___ o incrementales_X__;
   b) De forma automática ____ o Manual __X___,
   c) Periodicidad con que los realiza: __Semanalmente_____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Disco duro en equipos alternos.
3. Cómo y dónde archiva esos medios: Bajo resguardo en el área
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   El área

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-08-DIES-01	
Nombre del sistema A1 *	Memoria Estadística	
Recurso*	**Descripción***	**Control***
Bitácora de accesos	Revisión aleatoria de archivo .log	Análisis e interpretación de los eventos. El responsable es el encargado del área de sistemas.
Escáner de seguridad web de código abierto	Prueba de penetración	Herramienta actualizada frecuentemente por la fundación desarrolladora. El responsable es el encargado del área de sistemas.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-08-DIES-01	
Nombre del sistema*	Memoria Estadística	
Medida de seguridad*	**Procedimiento***	**Responsable***
No se tiene un procedimiento para la revisión de las medidas de seguridad		

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-08-DIES-01	
Nombre del sistema*	Memoria Estadística	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No se cuenta con resultados de la evaluación y pruebas a las medidas de seguridad		

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-08-DIES-01	
Nombre del sistema*	Memoria Estadística	
Medida de seguridad*	**Acciones***	**Responsable***
No se cuenta con acciones para la corrección y actualización de las medidas de seguridad.		

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-08-DIES-01		
Nombre del sistema*	Memoria Estadística		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución Metodología de aprendizaje: Estudio de casos, Exposición, Discusión y Materiales audiovisuales Objetivo general: Capacitar al personal para la ejecución eficiente de sus responsabilidades en la protección de datos personales en su posesión. Objetivos específicos: • Identificar a nivel teórico y práctico la seguridad técnica, administrativa y física para la protección de datos personales. • Difundir y dar a conocer los instrumentos jurídicos en materia de cómputo en la nube. • Construir el documento de seguridad y el sistema de gestión de seguridad de datos personales de su área universitaria. • Analizar si sus sistemas son susceptibles de portabilidad. • Cuestionar y comprobar si requiere su área universitaria	4 sesiones con un total de 10 horas de duración. 22 al 25 de marzo de 2022 FECHA	Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.

	una evaluación de impacto a los sistemas informáticos. Modalidad virtual a través de la plataforma ZOOM Impartido por la Unidad de Transparencia de la UNAM.		

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-08-DIES-01		
Nombre del sistema A1 *	Memoria Estadística		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-08-DIES-01		
Nombre del sistema*	Memoria Estadística		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de formularios	Revisión de los tipos de datos requeridos al usuario para simplificar el tratamiento de datos personales.	2 meses	Eliminación del requerimiento de datos personales no necesarios.
Actualización de tablas de la base de datos	Revisión de los campos de las tablas de la base de datos para simplificar el tratamiento de datos personales.	6 meses	Eliminación de los campos de las tablas de la base de datos, que contienen datos personales no necesarios.

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-08-DIES-01		
Nombre del sistema*	Memoria Estadística		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema operativo	Revisar e instalar las actualizaciones que se liberan para el sistema operativo.	Mensualmente	Mejoras en la seguridad y funcionamiento del sistema.
Actualización automatizada del antivirus	Actualización de las definiciones de virus y análisis del equipo.	Semanalmente	Mejoras en la seguridad y verificación de presencia de malware en el equipo.
Mantenimiento de hardware	Limpieza física del equipo	Anualmente	Funcionamiento del equipo en condiciones adecuadas.

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-08-DIES-01	
Nombre del sistema A1 *	Memoria Estadística	
Proceso*	**Descripción***	**Responsable***
Respaldo del contenido de las bases de datos	Respaldo semanal mediante el sistema de administración de bases de datos.	El proceso es realizado por el responsable y el encargado del área de sistemas. 1 día de ejecución.
Respaldo del código fuente del sistema	Respaldo del código fuente del sistema utilizando un sistema de control de versiones.	El proceso es realizado por el responsable y el encargado del área de sistemas. 1 día de ejecución.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General	
Identificador único*	SG-08-DIES-01
Nombre del sistema A1 *	Memoria Estadística

Proceso*	Descripción*	Responsable*
Disposición final de equipo	Respaldo de la información contenida en el equipo en un medio alterno. Uso de software para borrado seguro de datos en el equipo que será dado de baja.	El responsable es el encargado del área de sistemas. 1 día de ejecución.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema.

ÍNDICE

Departamento de Personal Académico y Movilidad Estudiantil (DPAME)

El Departamento de Personal Académico y Movilidad Estudiantil (DPAME) coordina, verifica y efectúa las operaciones administrativas tendientes a concretar y regularizar los movimientos de contratación y trámites, autorizados por el Consejo Técnico, del personal académico de la Facultad de Ingeniería, ante las dependencias centralizadoras, para dar cumplimiento en tiempo y forma a los requisitos establecidos en la Legislación Universitaria, el Contrato Colectivo de Trabajo, así como la normatividad que señala la Administración Central de la UNAM.

Además en el DPAME se coordinan las actividades relacionadas a Movilidad Estudiantil, entre las que se encuentran gestionar las solicitudes ante la Comisión de Movilidad de los alumnos de licenciatura de la Facultad que deseen realizar estancias en otras instituciones de educación superior y dar seguimiento a los trámites subsecuentes; procesar las solicitudes de estudiantes de otras instituciones que deseen realizar un estancia en nuestra Facultad; dar atención a las visitas de los representantes de otras Universidades interesadas en establecer convenios para realizar movilidad estudiantil.

SISTEMA DE MOVILIDAD ESTUDIANTIL DE LA FACULTAD DE INGENIERÍA (SIMOVE)

El sistema permite dar trámite y seguimiento a las estancias de movilidad estudiantil del alumnado de licenciatura de la Facultad de Ingeniería. A través de este se desarrolla el proceso desde la solicitud de participación y hasta el registro escolar de con el que concluye la movilidad, emitiendo notificaciones a los responsables académicos de las carreras y al alumnado, para ingresar al mismo a realizar las acciones que correspondan al avance del trámite.

Funge además como el repositorio de los expedientes de movilidad que documentan las estancias del alumnado y que significan los antecedentes documentales de revalidación que, como parte final del proceso, se entregan a la administración escolar de la Facultad.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-09-DPAME-01
Nombre del sistema *	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**
Datos personales (sensibles o no) contenidos en el sistema*:	**Alumnado:** **Datos de identificación**: Nombre, teléfono particular, teléfono celular, correo electrónico, CURP, idioma, domicilio en sitio de estancia de movilidad. **Datos académicos**: Carrera y módulo, generación, semestre, promedio, avance. **Datos personales sensibles:** Datos de póliza de seguro de gastos médicos durante la estancia.
Responsable*:	**Departamento de Personal Académico y Movilidad Estudiantil**
Nombre*:	Ing. Rocío Gabriela Alfaro Vega
Cargo*:	Jefa del Departamento
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se le da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todos los requerimientos de funcionalidad para los trámites a los que da soporte.
	Encargados:
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	

	Usuarios:
(Nombre del Usuario 1*)	**Ing. Rocío Gabriela Alfaro Vega**
Cargo*:	Responsable del Programa de Movilidad Estudiantil
Funciones*:	Validar y presentar a los responsables académicos las solicitudes de movilidad estudiantil y revalidación de asignaturas. Dar seguimiento a los trámites de movilidad que se realizan por el sistema y gestionar la postulación de solicitudes de movilidad estudiantil.
Obligaciones*:	Verificar el cumplimiento de la normatividad relativa a la movilidad y los requisitos establecidos por las convocatorias. Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 2*)	**Ing. Ígor Clavel Herrera**
Cargo*:	Apoyo académico al Programa de Movilidad Estudiantil
Funciones*:	Apoyo a la Responsable de Movilidad en los procesos de revisión de las solicitudes de movilidad estudiantil y revalidación de asignaturas. Apoyo al seguimiento de los trámites de movilidad que se realizan por el sistema y a la gestión de la postulación de solicitudes de movilidad estudiantil.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 3*)	**Ing. Lucía Méndez Hernández**
Cargo*:	Apoyo a la Responsable de Movilidad en los procesos de revisión de las solicitudes de movilidad estudiantil y revalidación de asignaturas. Apoyo al seguimiento de los trámites de movilidad que se realizan por el sistema y a la gestión de la postulación de solicitudes de movilidad estudiantil.
Funciones*:	Cumplir con la obligación legal de resguardar los datos personales.
Obligaciones*:	Apoyo a la Responsable de Movilidad en los procesos de revisión de las solicitudes de movilidad estudiantil y revalidación de asignaturas. Apoyo al seguimiento de los trámites de movilidad que se realizan por el sistema y a la gestión de la postulación de solicitudes de movilidad estudiantil.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único¨*	SG-09-DPAME-01
(Nombre del sistema A1*)	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**
Tipo de soporte: *	Soporte electrónico.
Descripción: *	Base de datos relacional, manejador de base de datos.

Características del lugar donde se resguardan los soportes: *	Alojado en servidor de la Secretaría de Servicios Académicos. Localizado en un espacio cerrado y de acceso controlado por el personal de la misma Secretaría.

3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las paginas 109 a 110.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

[redacted]

[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Departamento de Personal Académico y Movilidad Estudiantil, Secretaría General	
Identificador único*	SG-09-DPAME-01
Nombre del sistema *	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**
TRANSFERENCIAS DE DATOS PERSONALES	

Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales almacenados en el sistema, mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales almacenados en el sistema, mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales almacenados en el sistema, mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema de Movilidad Estudiantil de la Facultad de Ingeniería no realiza tratamiento de datos personales mediante soporte físico. La información se encuentra soportada mediante el uso de base de datos y almacenamiento de archivos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Bitácora para acceso y operación del software operativo y plataforma: Los propios del servidor que aloja el sistema, en cuanto a acceso a base de datos y sistema de archivo.

Bitácora para acceso y operación del software aplicativo: El sistema SIMOVE no contempla aún una bitácora que registre accesos de usuarios con acceso a datos personales de terceros. Se implantará una bitácora que permita identificar los periodos de acceso en correlación con las actividades propias del proceso de movilidad que opera a través del sistema.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención a incidentes en la plataforma operativa del sistema.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación para acceso a las instalaciones de la Facultad de Ingeniería.

b) ¿Cómo las autentifica?
No se cuenta con mecanismos de autenticación para acceso a las instalaciones de la Facultad de Ingeniería.

c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso a las instalaciones de la Facultad de Ingeniería.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Determinado por el área a la que pertenece el servidor y brinda el apoyo de alojamiento.

2. ¿Cómo las autentifica?
   Determinado por el área a la que pertenece el servidor y brinda el apoyo de alojamiento.
3. ¿Cómo les autoriza el acceso?
   Determinado por el área a la que pertenece el servidor y brinda el apoyo de alojamiento.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los usuarios en sus distintos niveles de participación, una vez autenticados en el sistema, pueden acceder a la opción de “Mis datos” en el menú de éste, donde pueden actualizar datos de contacto y ubicación (para el caso de académicos y personal operativo del Programa de Movilidad) así como a datos personales, datos escolares y datos de contacto (para el caso del alumnado).

En el caso del alumnado, el sistema detecta cuando han transcurrido más de tres meses desde la última actualización (tiempo aproximado que corresponde al cambio de semestre) y emite un aviso en pantalla para que ingresen a actualizar sus datos escolares.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
No
b) ¿Es discrecional (matriz de control de acceso)?
No
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  Sí
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  Sí, depende del área que brinda el apoyo de alojamiento.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
  Sí
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  No

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles?
  Encargados y usuarios administrativos
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
  Responsable del sistema (Responsable de Movilidad)
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?
  Sí

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
Sí

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí

c) ¿Cómo se evita el acceso remoto no autorizado?
Mediante usuario y contraseña a nivel aplicativo. Usuario y contraseña más IP registrada, para acceso a base de datos y sistema de archivos.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   1. Completos_X_, diferenciales ___ o incrementales___;
   2. De forma automática ____ o Manual __X__,
   3. Periodicidad con que los realiza: ___semanal____

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
HDD externo, HDD local

3. Cómo y dónde archiva esos medios, y
HDD externo y en HDD de la máquina de desarrollo.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
El área universitaria (Depto. de Personal Académico y Movilidad Estudiantil).

IX. PLAN DE CONTINGENCIA

No se tiene un plan de contingencia del sistema de tratamiento de datos.
No se cuenta con sitio redundante.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-09-DPAME-01	
Nombre del sistema *	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**	
Recurso*	**Descripción***	**Control***
Bitácora del sistema (en desarrollo)	Revisión de frecuencia y horarios de acceso.	Se revisará de manera regular la frecuencia en que acceden los usuarios con acceso a datos de terceros, así como los horarios, a fin de definir comportamientos típicos y poder identificar accesos atípicos.

Herramientas implantadas por el área que brinda el apoyo de alojamiento.	Medidas y herramientas que tengan implantadas.	El control queda a cargo del área que brinda el apoyo de alojamiento

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-09-DPAME-01	
Nombre del sistema *	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del Mínimo Privilegio (PoLP)	Se asigna a un usuario de prueba, distintos niveles de privilegios para acceder al sistema y verificar que la información a la que accede esté limitada a su nivel de privilegios.	Usuarios responsables del sistema.
Verificar compatibilidad del sistema con las versiones más actuales de la plataforma aplicativa y de base de datos	Se actualizan en el equipo de desarrollo las versiones del lenguaje de programación, librerías y manejador de base de datos, para verificar la compatibilidad del código.	Usuarios responsables del sistema.
Mantener actualizado el software antivirus y antimalware en equipo de desarrollo.	Revisión y actualización del paquete antivirus instalado en el equipo de desarrollo.	Usuarios responsables del sistema.
Medidas implantadas por el área que brinda el apoyo de alojamiento.	Medidas y procedimientos que se tengan implantadas.	El control queda a cargo del área que brinda el apoyo de alojamiento

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-09-DPAME-01	
Nombre del sistema *	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del Mínimo Privilegio (PoLP)	Se verificó que la información a la que accede cada nivel de usuario corresponde a su ámbito de participación en el proceso.	Encargados del sistema.

Verificar compatibilidad del sistema con las versiones más actuales de la plataforma aplicativa y de base de datos	Se verificó que el código es compatible con las versiones más actuales del lenguaje de programación, librerías y manejador de base de datos en el equipo de desarrollo, a la par de operar con las versiones disponibles en el servidor de alojamiento.	Encargados del sistema.
Mantener actualizado el software antivirus y antimalware en equipo de desarrollo.	Se cuenta con la versión actualizada del software antivirus y su base de datos de virus.	Encargados del sistema.
Medidas implantadas por el área que brinda el apoyo de alojamiento.	Los resultados de estas medidas quedan en el ámbito del área que brinda el apoyo de alojamiento.	El control queda a cargo del área que brinda el apoyo de alojamiento

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-09-DPAME-01	
Nombre del sistema *	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**	
Medida de seguridad*	**Acciones***	**Responsable***
Actualización del software operativo, aplicativo y del manejador de base de datos en el servidor de alojamiento.	Actualizar las versiones del lenguaje de programación y del manejador de la base de datos a las más actuales, a fin de reducir el riesgo de brecha de seguridad por esta causa.	Depende por completo del área que brinda el apoyo de alojamiento.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-09-DPAME-01		
Nombre del sistema *	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación.			

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-09-DPAME-01		
Nombre del sistema *	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión.			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-09-DPAME-01		
Nombre del sistema *	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mudanza a servidor de alojamiento propio de la Secretaría General.	Contar en la Secretaría General con un servidor que permita alojar el sistema SIMOVE.	Dependerá del área designada para administrar la operación del servidor.	Posibilidad de definir requisitos de medidas de seguridad y solicitarlas al área administradora del servidor como requerimientos del servicio.

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-09-DPAME-01		
Nombre del sistema *	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Adquisición de un servidor de la Secretaría General.	Disponer de un servidor que permita alojar al sistema SIMOVE dentro del entorno de la Secretaría sin depender de áreas ajenas a ésta.	Depende de la Secretaría General.	Espacio en un servidor compartido.

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-09-DPAME-01	
Nombre del sistema *	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**	
Proceso*	**Descripción***	**Responsable***
Respaldo en texto plano del contenido de la base de datos.	Se realiza un respaldo periódico (prácticamente diario) del contenido de la base en archivo .sql almacenado en el equipo de desarrollo.	Encargados del sistema.
Respaldo del sistema de archivos.	Se realiza un respaldo periódico (prácticamente diario) del contenido del repositorio de archivos en el servidor, al almacenamiento del equipo de desarrollo.	Encargados del sistema.
Respaldo externo de información.	Se realiza un respaldo semanal en medio de almacenamiento externo.	Encargados del sistema.
Proceso de respaldo de información del servidor en que se brinda el apoyo de alojamiento.	Depende del área que brinda el apoyo de alojamiento.	Corresponde al área que brinda el apoyo de alojamiento

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General		
Identificador único*	SG-09-DPAME-01	
Nombre del sistema *	**Sistema de Movilidad Estudiantil de la Facultad de Ingeniería (SIMOVE)**	
Proceso*	**Descripción***	**Responsable***
No se cuenta con un proceso de borrado seguro. La disposición final de equipos, se apega al proceso institucional de bajas (Secretaría Administrativa).		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del Sistema SIMOVE.

ÍNDICE

Unidad de Servicios de Cómputo Académico (UNICA)

La Unidad de Servicios de Cómputo Académico UNICA, gestiona el avance y crecimiento informático de la Facultad de Ingeniería a través de procesos articuladores de avanzada, con esquemas de colaboración-alianza sinérgicas al interior y exterior, promoviendo el manejo ágil y seguro, de mayores capacidades del conocimiento y de la información, generando un campo fértil para el emprendimiento y vinculación, por medio de proyectos de innovación científico-tecnológico; lo anterior a través del amplio acceso, uso y apropiación de las Tecnologías de la Información y la Comunicación TIC.

RIPBE

El sistema de inscripción al programa de Formación de Becarios de la Unidad de Servicios de Cómputo Académico, UNICA es un sistema Web que permite a los interesados en pertenecer al programa de formación de Becarios de UNICA, solicitar su inscripción al registrarse para ser candidatos a dicho programa, cumpliendo con todos los requisitos establecidos para tal efecto.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-10-UNICA-01
Nombre del sistema *	RIPBE
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre Carrera Número de cuenta Semestre actual Promedio RFC Número de teléfono particular Correo electrónico Fotografía del titular de la información Avance de créditos
Responsable*:	Unidad de Servicios de Cómputo Académico de la Secretaría General
Nombre*:	Enrique Barranco vite
Cargo*:	**Coordinador de la Unidad de Servicios de Cómputo Académico**
Funciones*:	Coordinar y supervisar las actividades del grupo de trabajo del sistema de tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y promover su uso, exclusivamente para los fines que han sido recabados
	Encargados:
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	Beatriz Barrera Hernández
Cargo*:	Jefa de Departamento
Funciones*:	Coordinar y supervisar las actividades operativas del sistema de tratamiento de datos personales

Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 2*)	María del Rosario Barragán Paz
Cargo*:	Jefe de departamento
Funciones*:	Coordinar y supervisar las actividades operativas del sistema de tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados
(Nombre del Usuario 3*)	César Mauricio Ramos Villaseñor
Cargo*:	Ayudante de Profesor
Funciones*:	Operar el sistema de tratamiento de datos personales, manejo de base de datos
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 4*)	Carolina Kennedy Villa
Cargo*:	Becaria
Funciones*:	Operar el sistema de tratamiento de datos personales, actualización, alta y baja de usuarios
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.

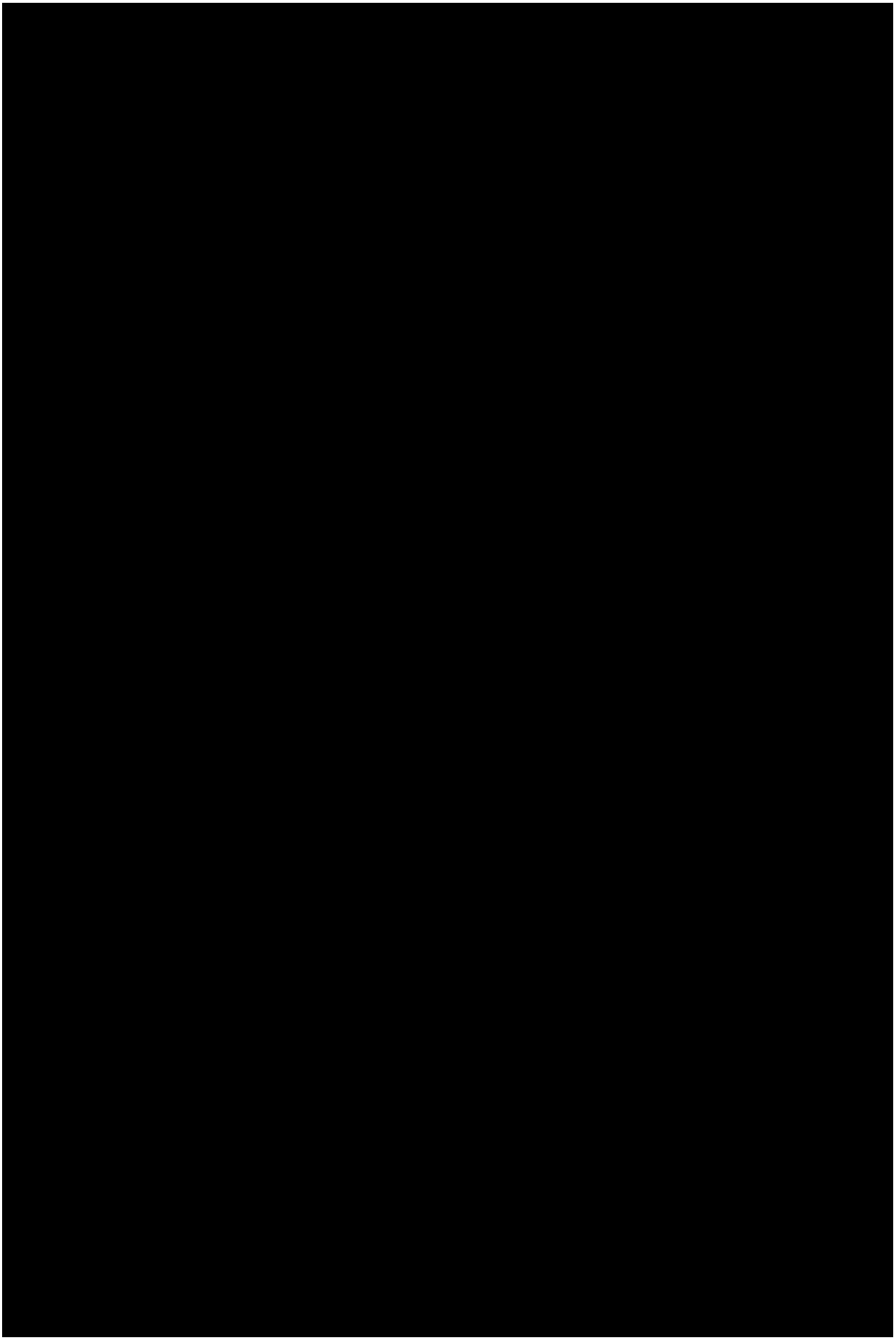
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

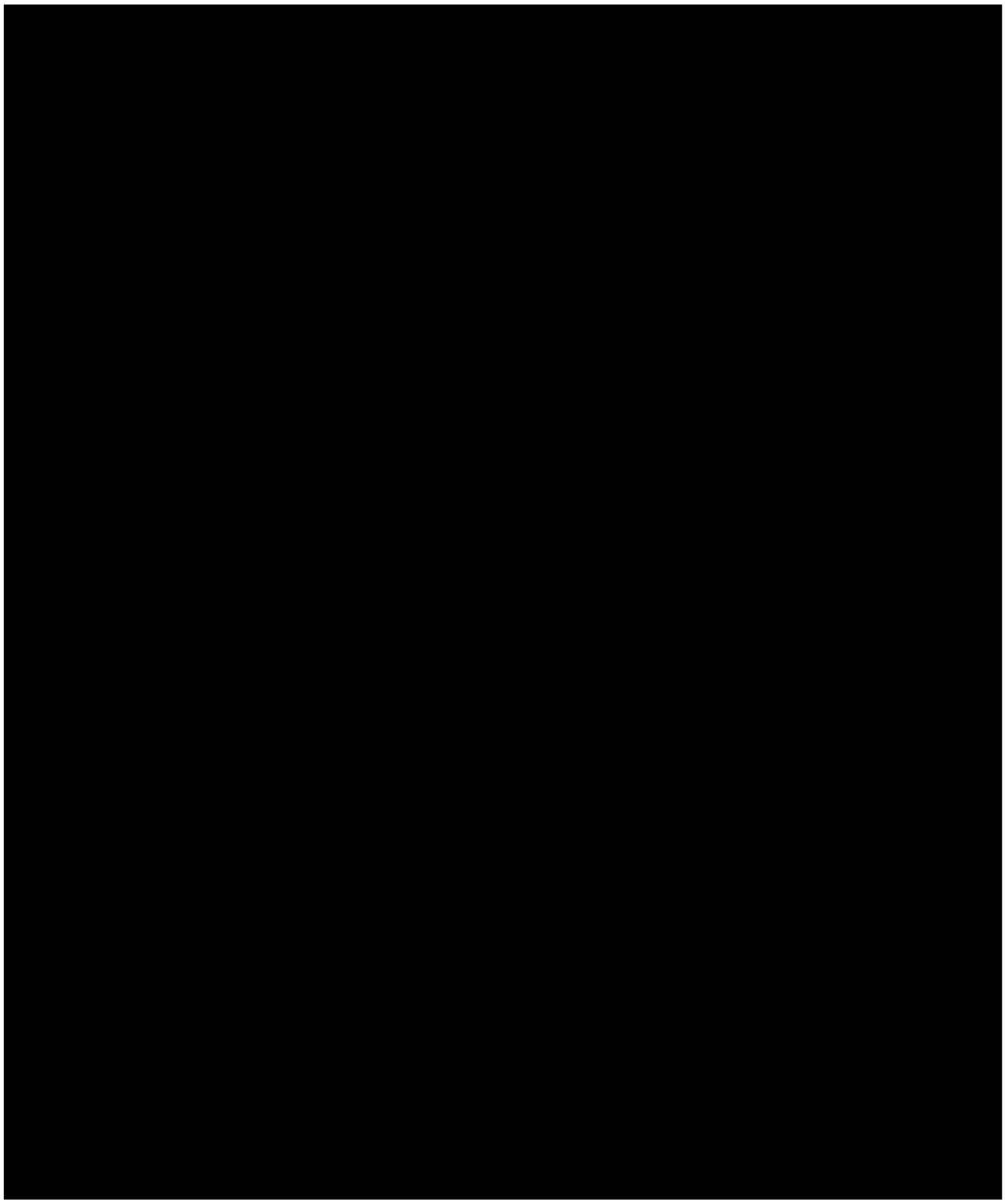
Secretaría General	
Identificador único¨*	SG-10-UNICA-01
Nombre del sistema *	RIPBE
Tipo de soporte: *	Soporte electrónico
Descripción: *	Sistema de Base de datos
Características del lugar donde se resguardan los soportes[1]:*	Alojamiento en un servidor local. Localizado en un espacio cerrado y de acceso controlado

3. ANÁLISIS DE RIESGOS

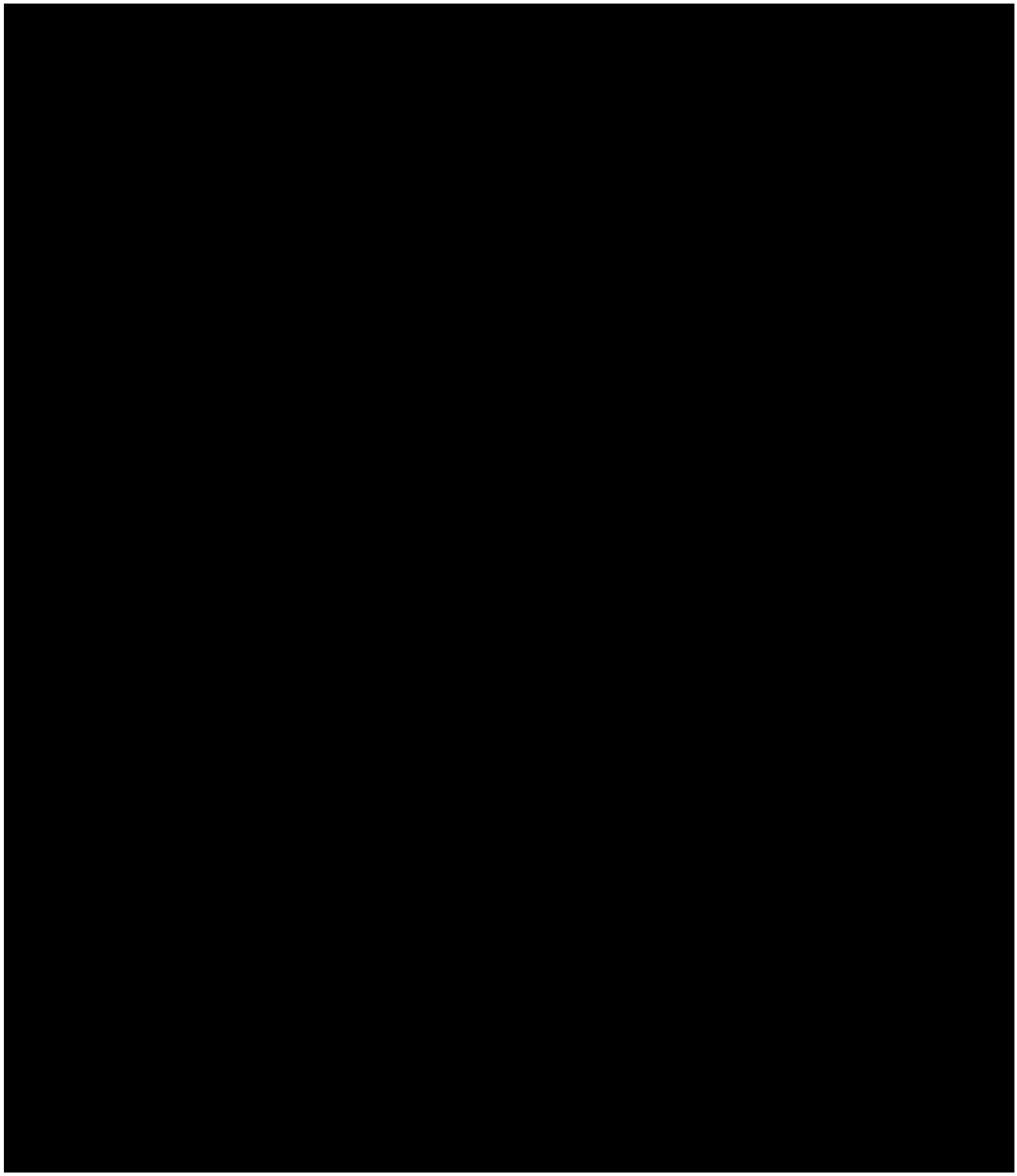
[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 120 a 125.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

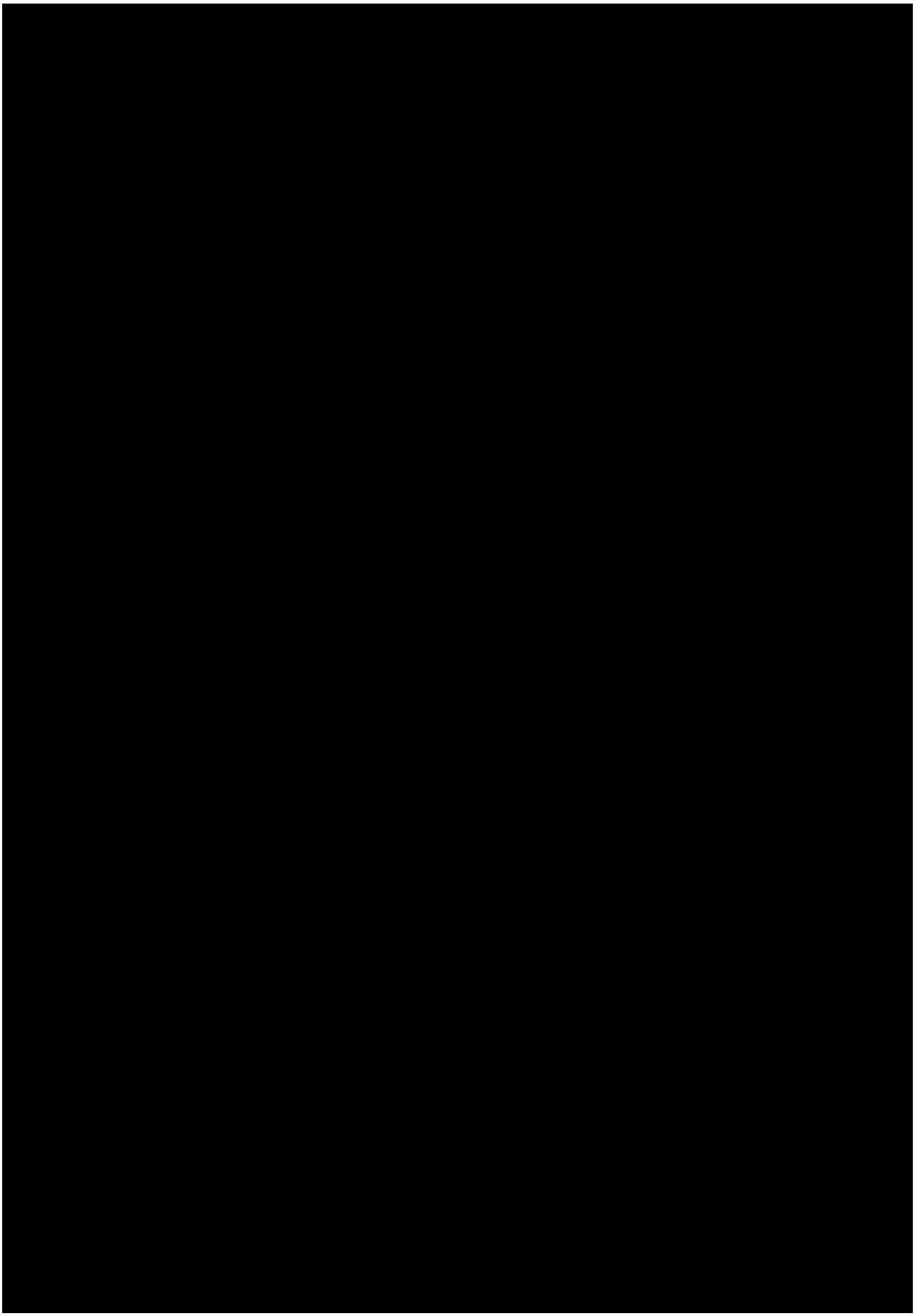


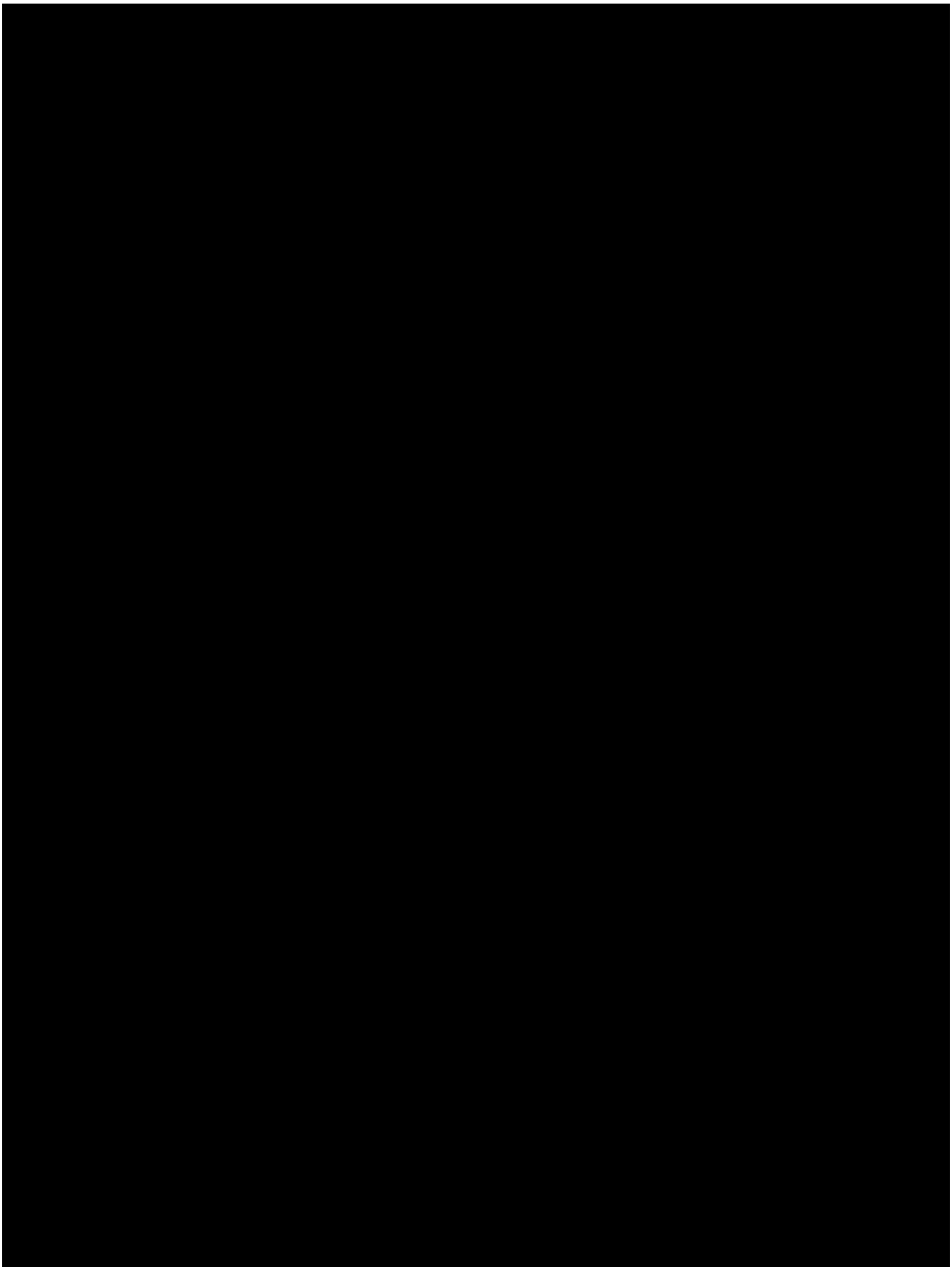


4. ANÁLISIS DE BRECHA



5. PLAN DE TRABAJO





6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-10-UNICA-01
(Nombre del sistema)*	RIPBE
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema RIPBE no realiza tratamiento de datos personales con soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema que almacena el sistema RIPBE

IV. REGISTRO DE INCIDENTES:

El procedimiento para la atención de incidentes consiste en hacer la verificación de las bitácoras del sistema, identificando a partir de ello de intentos de acceso o accesos que no correspondan a las actividades de operación, rastreo de las acciones maliciosas dentro del sistema, eliminación de las actividades maliciosas, formulación de un plan de fortalecimiento del sistema y generación de informe dirigido al responsable del área.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

   Para las personas que acceden a sus instalaciones:

   1. ¿Cómo las identifica?
   No se cuenta con mecanismos de identificación
   2. ¿Cómo las autentifica?
   No se cuenta con mecanismos de autenticación
   3. ¿Cómo les autoriza el acceso?
   No se cuenta con mecanismos de control de acceso

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
   No se cuenta con mecanismo de autenticación
3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado, previa presentación de orden de trabajo u oficio.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El titular de los datos que desee realizar la actualización de sus datos personales debe enviar un oficio al área que opera el sistema indicando la actualización de sus datos personales.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

Es discrecional

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Se cifran solo las contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo las contraseñas

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Los usuarios 3 y 4

b) ¿Quién autoriza la creación de nuevos perfiles?
El usuario 1

c) ¿Se lleva registro de la creación de nuevos perfiles?
El sistema almacena en bitácoras el registro

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas

de mantenimiento?

Sí

c) ¿Cómo se evita el acceso remoto no autorizado?

- El acceso remoto a la red se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Se cuenta en el servidor con un sistema de control de acceso de identidades basado en usuario y contraseña y es discrecional.
- Se cuenta con controles de acceso discrecional.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos X, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual X,
   c) Periodicidad con que los realiza: Onpremise el respaldo es semanal, lo contenido en la nube pública no se respalda
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Onpremise en IAAS
3. Cómo y dónde archiva esos medios: en IAAS
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

Para este sistema no se cuenta con un plan de contingencia.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

N/A

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

No se cuenta con sitio redundante

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-10-UNICA-01	
(Nombre del sistema)*	RIPBE	
Recurso*	**Descripción***	**Control***
Bitácoras del sistema	Revisiones aleatorias	Revisar de forma aleatoria la bitácora con el fin de indagar si hubiera algún uso o

		comportamiento inusual en el sistema. Responsables: Usuarios 2 y 4

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-10-UNICA-01	
(Nombre del sistema)*	RIPBE	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	Responsable: Usuarios 2, 3 y 4 Tiempo: 1 día hábil
Generación de respaldos	Revisión de la existencia de respaldos conforme a la calendarización programada por IAAS	Responsable: Usuarios 2, 3 y 4. Tiempo: 1 día hábil

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-10-UNICA-01	
(Nombre del sistema)*	**RIPBE**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se eliminaron cuentas que ya no estaban activas y las que se mantienen cumplen con el principio de menor privilegio con base al rol asignado.	Usuarios 1 y 2
Generación de respaldos	Se verificó la existencia de los respaldos y que su fecha de creación correspondiera al	Usuarios 2 y 3

	calendario de generación de respaldos.	

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-10-UNICA-01	
(Nombre del sistema)*	**RIPBE**	
Medida de seguridad*	**Acciones***	**Responsable***
Bitácoras del sistema	• Con base en las Políticas de desarrollo seguro de software de tratamiento de datos personales, desarrollar módulos que den seguimiento a las actividades de los usuarios dentro del sistema de tratamiento de datos personales. • Homologar el tipo de registro de las bitácoras para que estas se puedan recolectar y correlacionar en un SIEM	Responsables: Titular de la Secretaría General y Usuarios 1 y 2 Fecha: una vez creadas y aprobadas las políticas de desarrollo seguro de software, trabajar en la homologación de bitácoras en los sistemas de tratamiento de datos personales

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-10-UNICA-01		
(Nombre del sistema)*	RIPBE		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Ver videos de los cursos ofrecidos para el tema de protección de datos personales por la Unidad de Transparencia de la UNAM.	Videos grabados por la Unidad de Transparencia de la UNAM relativos al tema de protección de datos personales	Actividad permanente	Todo el personal que trate datos personales
Asistir a cursos de protección de datos personales ofrecidos por la Unidad de Transparencia de la UNAM	Solicitar a la Unidad de Transparencia el acceso en línea y asíncrono a cursos sobre protección de datos personales	Actividad permanente	Todo el personal que trate datos personales

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-10-UNICA-01		
(Nombre del sistema)*	RIPBE		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-10-UNICA-01		
(Nombre del sistema)*	RIPBE		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema de tratamiento de datos personales	Actualizar conforme se da el avance tecnológico, las políticas de desarrollo seguro de software y la normatividad en el tratamiento de	Permanente	Total

	datos personales del software que aloja el sistema que trata datos personales		

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-10-UNICA-01		
(Nombre del sistema)*	RIPBE		
Actividad*	**Descripción***	**Duración***	**Cobertura***
RIPBE está alojado en el sistema SG-15-UNICA-06, por lo que en la descripción de ese sistema se describe lo solicitado en este punto.			

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-10-UNICA-01	
(Nombre del sistema)*	RIPBE	
Proceso*	**Descripción***	**Responsable***
RIPBE está alojado en el sistema SG-15-UNICA-06, por lo que en la descripción de ese sistema se describe lo solicitado en este punto.		

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General	
Identificador único*	SG-10-UNICA-01
(Nombre del sistema)*	RIPBE

Proceso*	Descripción*	Responsable*
ACEOC está alojado en el sistema SG-15-UNICA-06, por lo que en la descripción de ese sistema se describe lo solicitado en este punto.		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

LMSE

La plataforma educativa EDUCAFI es un sistema de gestión de aprendizaje (LMS) que permite tener un espacio idóneo para la creación de entornos virtuales, favoreciendo el aprendizaje colaborativo y significativo, así como la comunicación e interacción síncrona y asíncrona entre el docente y los estudiantes con la ventaja de acceder a la información de forma ágil y segura mediante dispositivos móviles y de escritorio con los diferentes navegadores del mercado, en cualquier momento y lugar del mundo.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-11-UNICA-02
Nombre del sistema *	**LMSE**
Datos personales (sensibles o no) contenidos en el sistema*:	Alumnos Nombre Número de cuenta Correo electrónico Grupo Asignatura Nombre del profesor Profesores Nombre Correo electrónico División Asignatura(s) Grupo(s) Número de trabajador RFC
Responsable*:	Unidad de Servicios de Cómputo Académico de la Secretaría General
Nombre*:	Enrique Barranco Vite
Cargo*:	Coordinador de la Unidad de Servicios de Cómputo Académico
Funciones*:	Coordinar y supervisar las actividades del grupo de trabajo del sistema de tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y promover su uso, exclusivamente para los fines que han sido recabados
Encargados:	
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:

(Nombre del Usuario 1*)	Beatriz Barrera Hernández
Cargo*:	Jefa de Departamento
Funciones*:	Coordinar y supervisar las actividades operativas del Servicio de la plataforma, así como el tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 2*)	Laura Gabriela Ramírez Sánchez
Cargo*:	Administradora de LMSE
Funciones*:	Atención a académicos y estudiantes.
Obligaciones*:	Atención a académicos y estudiantes sobre el servicio de la plataforma educativa, así como cuidar la confidencialidad de la información.
(Nombre del Usuario 3*)	Francisco Javier Montoya Cervantes
Cargo*:	Administrador de EDUCAFI
Funciones*:	Atención a académicos y estudiantes
Obligaciones*:	Atención a académicos y estudiantes sobre el servicio de la plataforma educativa, así como cuidar la confidencialidad de la información.
(Nombre del Usuario 4*)	Carlos Amaya López
Cargo*:	Administrador de EDUCAFI
Funciones*:	Atención a académicos y estudiantes
Obligaciones*:	Atención a académicos y estudiantes sobre el servicio de la plataforma educativa, así como cuidar la confidencialidad de la información
(Nombre del Usuario 5*)	Marco Antonio López Lara
Cargo*:	Administrador de EDUCAFI
Funciones*:	A Atención a académicos y estudiantes
Obligaciones*:	Atención a académicos y estudiantes sobre el servicio de la plataforma educativa, así como cuidar la confidencialidad de la información
(Nombre del Usuario 6*)	Héctor David Pineda Villagran
Cargo*:	Administrador de EDUCAFI
Funciones*:	Atención a académicos y estudiantes
Obligaciones*:	Atención a académicos y estudiantes sobre el servicio de la plataforma educativa, así como cuidar la confidencialidad de la información
(Nombre del Usuario 7*)	Daniela Boquer Ramírez
Cargo*:	Administradora de EDUCAFI

Funciones*:	Atención a académicos y estudiantes
Obligaciones*:	Atención a académicos y estudiantes sobre el servicio de la plataforma educativa, así como cuidar la confidencialidad de la información
(Nombre del Usuario 8*)	Axel Arturo Bautista Beltrán
Cargo*:	Administrador de EDUCAFI
Funciones*:	Atención a académicos y estudiantes
Obligaciones*:	Atención a académicos y estudiantes sobre el servicio de la plataforma educativa, así como cuidar la confidencialidad de la información
(Nombre del Usuario 9*)	Parada Pérez Jesús Bryan
Cargo*:	Administrador de EDUCAFI
Funciones*:	Atención a académicos y estudiantes
Obligaciones*:	Atención a académicos y estudiantes sobre el servicio de la plataforma educativa, así como cuidar la confidencialidad de la información

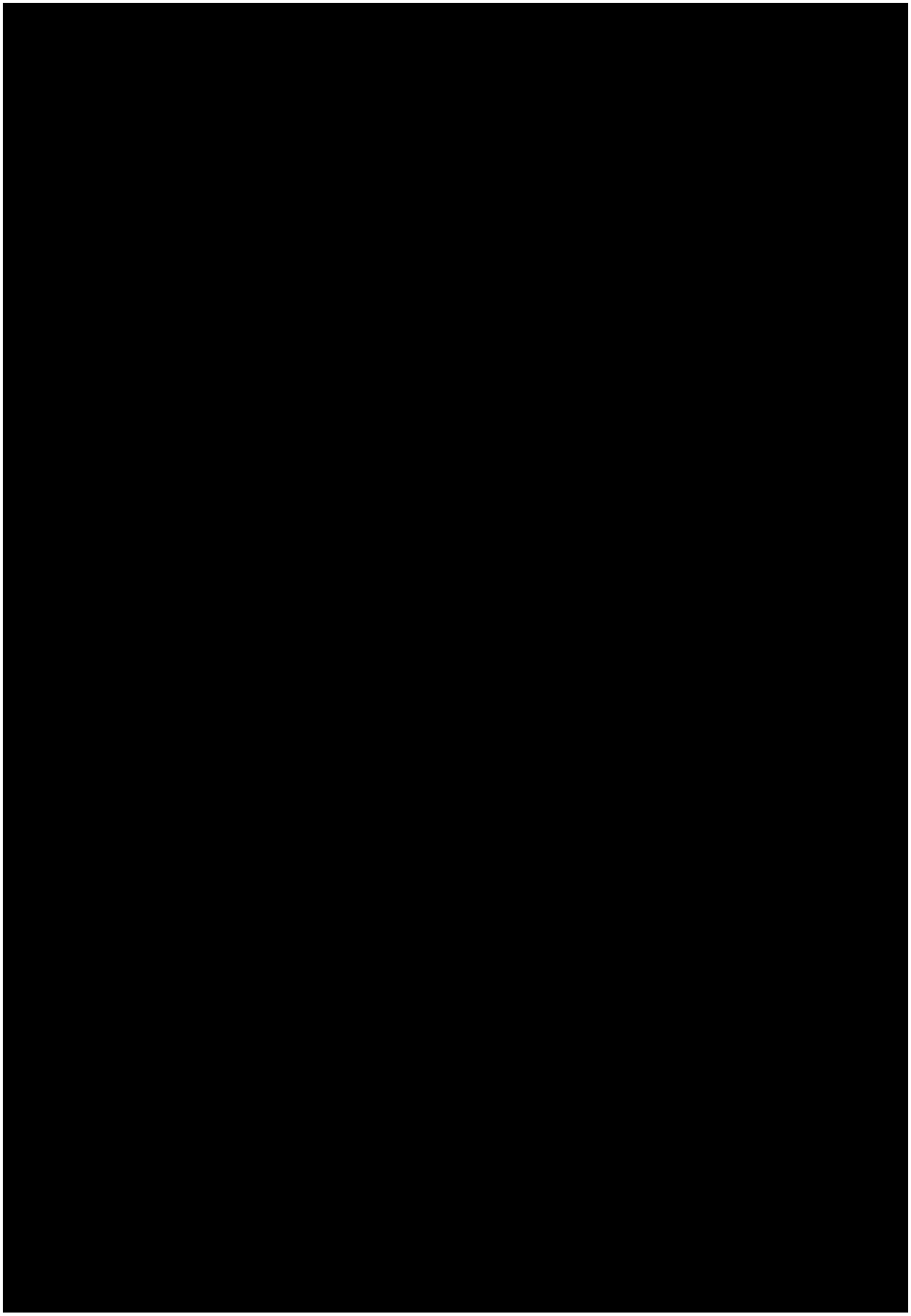
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único¨*	SG-11-UNICA-02
Nombre del sistema *	**LMSE**
Tipo de soporte[2]:*	Soporte electrónico
Descripción[3]:*	Sistema que recolecta y trata datos relacionados y estructurados que permiten validar el vínculo laboral o académico del titular de los datos con la dependencia, para posteriormente crear cuentas a los solicitantes que usarán para tener acceso a las aplicaciones colaborativas.
Características del lugar donde se resguardan los soportes:*	Alojamiento local, ubicado en SG-15-UNICA-06

3. ANÁLISIS DE RIESGOS

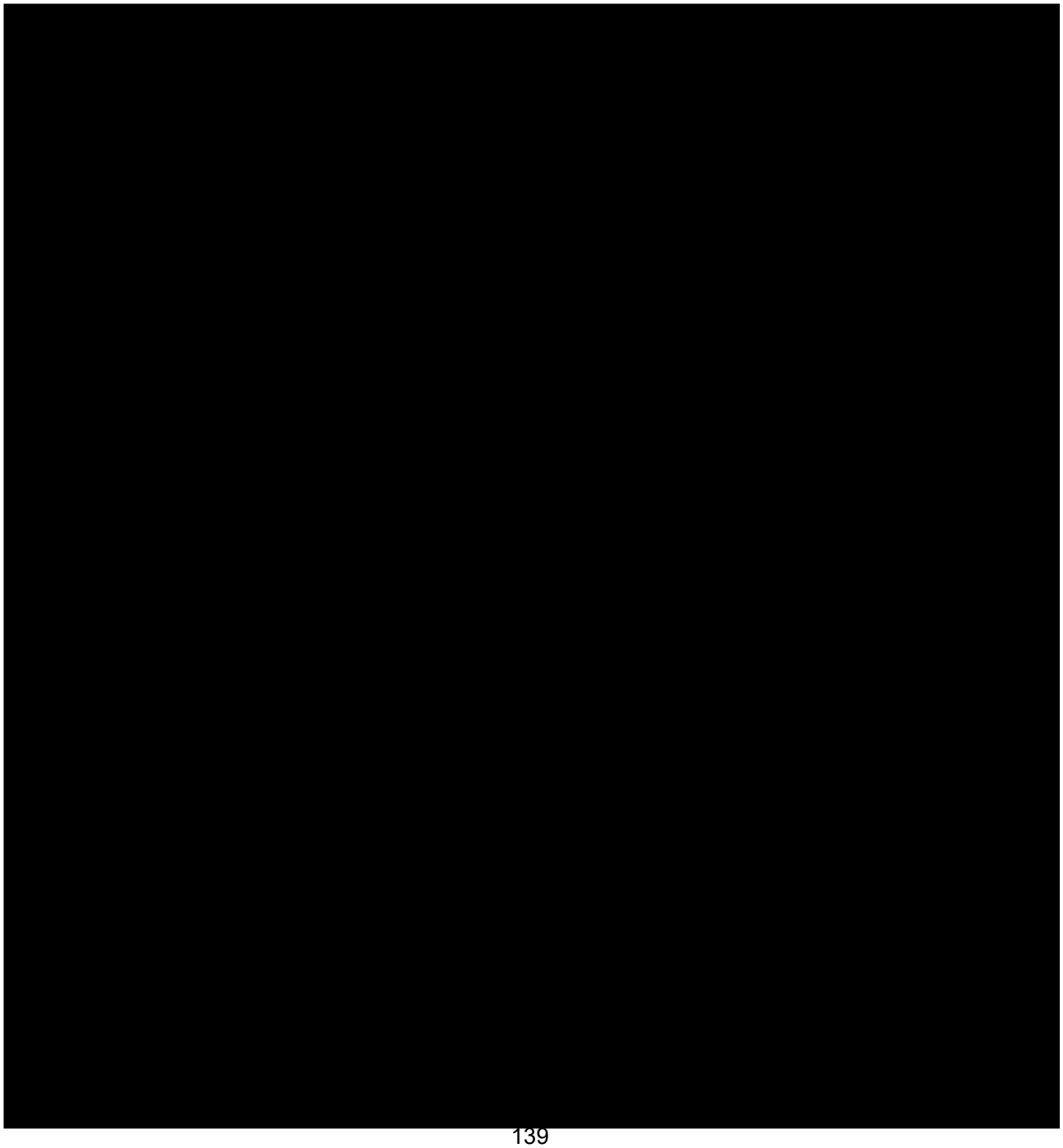
[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 136 a 140.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.



4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-11-UNICA-02
Nombre del sistema *	**LMSE**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[4]	No se realizan trasferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Nota: Ninguno de los sistemas realiza tratamiento de datos personales con soportes físicos

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema que almacena los sistemas SG-11-UNICA-02, SG-12-UNICA-03, SG-13-UNICA-04 y SG-14-UNICA-05

IV. REGISTRO DE INCIDENTES:

El procedimiento para la atención de incidentes consiste en hacer la verificación de las bitácoras del sistema, identificando a partir de ello de intentos de acceso o accesos que no correspondan a las actividades de operación rastreo de las acciones maliciosas, formulación de un pan de fortalecimiento del sistema y generación de informe dirigido al responsable del área.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica? No se cuenta con mecanismos de identificación
b) ¿Cómo las autentifica? No se cuenta con mecanismos de autenticación
c) ¿Cómo les autoriza el acceso? No se cuenta con mecanismos de control de acceso

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica? Se tiene definida una lista de acceso para el personal autorizado
2. ¿Cómo las autentifica? No se cuenta con mecanismos de autenticación
3. ¿Cómo les autoriza el acceso? Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado, previa presentación de orden de trabajo u oficio.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El titular de los datos que desee realizar la actualización de sus datos personales, debe enviar un oficio al área que opera el sistema indicando la actualización de sus datos personales.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

Es discrecional

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Se cifran solo las contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
sí
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo las contraseñas

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Los usuarios 1 y 2

b) ¿Quién autoriza la creación de nuevos perfiles?
El usuario 1

c) ¿Se lleva registro de la creación de nuevos perfiles?
El sistema almacena en bitácoras el registro

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
sí

c) ¿Cómo se evita el acceso remoto no autorizado?

- El acceso remoto a la red se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Se cuenta en el servidor con un sistema de control de acceso de identidades basado en usuario y contraseña y es discrecional.
- Se cuenta con controles de acceso discrecional.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos X, diferenciales ___ o incrementales___;

b) De forma automática ____ o Manual X,

c) Periodicidad con que los realiza: Onpremise el respaldo es semanal, lo contenido en la nube pública no se respalda

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Onpremise en IAAS

3. Cómo y dónde archiva esos medios: en IAAS

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
El área universitaria

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
No se cuenta con un plan de contingencia para este sistema

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
No existe

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
No se cuenta con sitio redundante

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-11-UNICA-02	
Nombre del sistema *	**LMSE**	
Recurso*	**Descripción***	**Control***
Bitácoras del sistema	Revisiones aleatorias	Revisar de forma aleatoria la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en el sistema. Responsables: Usuarios 2, 3, 4, 5, 6, 7, 8 y 9

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-11-UNICA-02	
Nombre del sistema *	**LMSE**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Generación de respaldos	Revisión de los respaldos conforme a la planeación del servicio	Usuarios: 2, 3, 4, 5, 6, 7, 8 y 9

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-11-UNICA-02	
Nombre del sistema *	**LMSE**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Generación de respaldos	Se verificó la existencia de los respaldos y que su fecha de creación correspondiera al	Usuarios 2, 3, 4, 5 6, 7, 8 y 9

	calendario de generación de respaldos.	

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-11-UNICA-02	
(Nombre del sistema)*	**LMSE**	
Medida de seguridad*	**Acciones***	**Responsable***
Bitácoras del sistema	• Con base en las Políticas de desarrollo seguro de software de tratamiento de datos personales, desarrollar módulos que den seguimiento a las actividades de los usuarios dentro del sistema de tratamiento de datos personales. • Homologar el tipo de registro de las bitácoras para que estas se puedan recolectar y correlacionar en un SIEM	Responsables: Titular de la Secretaría General y Usuarios 1 y 2 Fecha: una vez creadas y aprobadas las políticas de desarrollo seguro de software, trabajar en la homologación de bitácoras en los sistemas de tratamiento de datos personales

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-11-UNICA-02		
Nombre del sistema *	**LMSE**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Ver videos de los cursos ofrecidos para el tema de protección de datos personales	Videos grabados por la Unidad de Transparencia de la UNAM relativos	Actividad permanente	Todo el personal que trate datos personales

por la Unidad de Transparencia de la UNAM.	al tema de protección de datos personales		
Asistir a cursos de protección de datos personales ofrecidos por la Unidad de Transparencia de la UNAM	Solicitar a la Unidad de Transparencia el acceso en línea y asíncrono a cursos sobre protección de datos personales	Actividad permanente	Todo el personal que trate datos personales

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-11-UNICA-02		
Nombre del sistema *	**LMSE**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-11-UNICA-02		
Nombre del sistema *	**LMSE**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del sistema de información	Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término	Mencione los aspectos del sistema de información que son resueltos, total o parcialmente, por la actividad.

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-11-UNICA-02		
Nombre del sistema *	**LMSE**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
LMSE está alojado en el sistema SG-15-UNICA-06, por lo que en la descripción de ese sistema se describe lo solicitado en este punto.			

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-11-UNICA-02	
Nombre del sistema *	LMSE	
Proceso*	**Descripción***	**Responsable***
LMSE está alojado en el sistema SG-15-UNICA-06 por lo que en la descripción de ese sistema se describe lo solicitado en este punto.		

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General		
Identificador único*	SG-11-UNICA-02	
Nombre del sistema *	**LMSE**	
Proceso*	**Descripción***	**Responsable***
LMSE está alojado en el sistema SG-15-UNICA-06, por lo que en la descripción de este sistema se describe lo solicitado en este punto		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

SIRES

El sistema de registro en Salas de Cómputo es una herramienta de apoyo en la gestión de las Salas de Cómputo de UNICA, donde se recaban la información requerida para el control de préstamo de servicios.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-12-UNICA-03
Nombre del sistema *	**SIRES**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre Número de cuenta Carrera Semestre actual
Responsable*:	Unidad de Servicios de Cómputo Académico de la Secretaría General
Nombre*:	Enrique Barranco Vite
Cargo*:	Coordinador de la Unidad de Servicios de Cómputo Académico
Funciones*:	Coordinar y supervisar las actividades del grupo de trabajo del sistema de tratamiento de datos personales.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y promover su uso, exclusivamente para los fines que han sido recabados.
Encargados:	
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	Beatriz Barrera Hernández
Cargo*:	Jefa de Departamento S A
Funciones*:	Coordinación del servicio en Salas de Cómputo para estudiantes
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso de ellos exclusivamente para los fines que han sido recabados.
(Nombre del Usuario 2*)	Cruz Sergio Aguilar Díaz
Cargo*:	Gestión de Salas de Cómputo
Funciones*:	Gestionar los procesos para brindar el servicio en las Salas de Cómputo para estudiantes

Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso de ellos exclusivamente para los fines que han sido recabados.
(Nombre del Usuario 3*)	Rosa María Juárez Cisneros
Cargo*:	Ayudante de profesor
Funciones*:	Atención en Salas de Cómputo, así como la operación del sistema y tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso de ellos exclusivamente para los fines que han sido recabados.
(Nombre del Usuario 4*)	Becarios
Cargo*:	Becario
Funciones*:	Atención en Salas de Cómputo, así como la operación del sistema y tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso de ellos exclusivamente para los fines que han sido recabados.

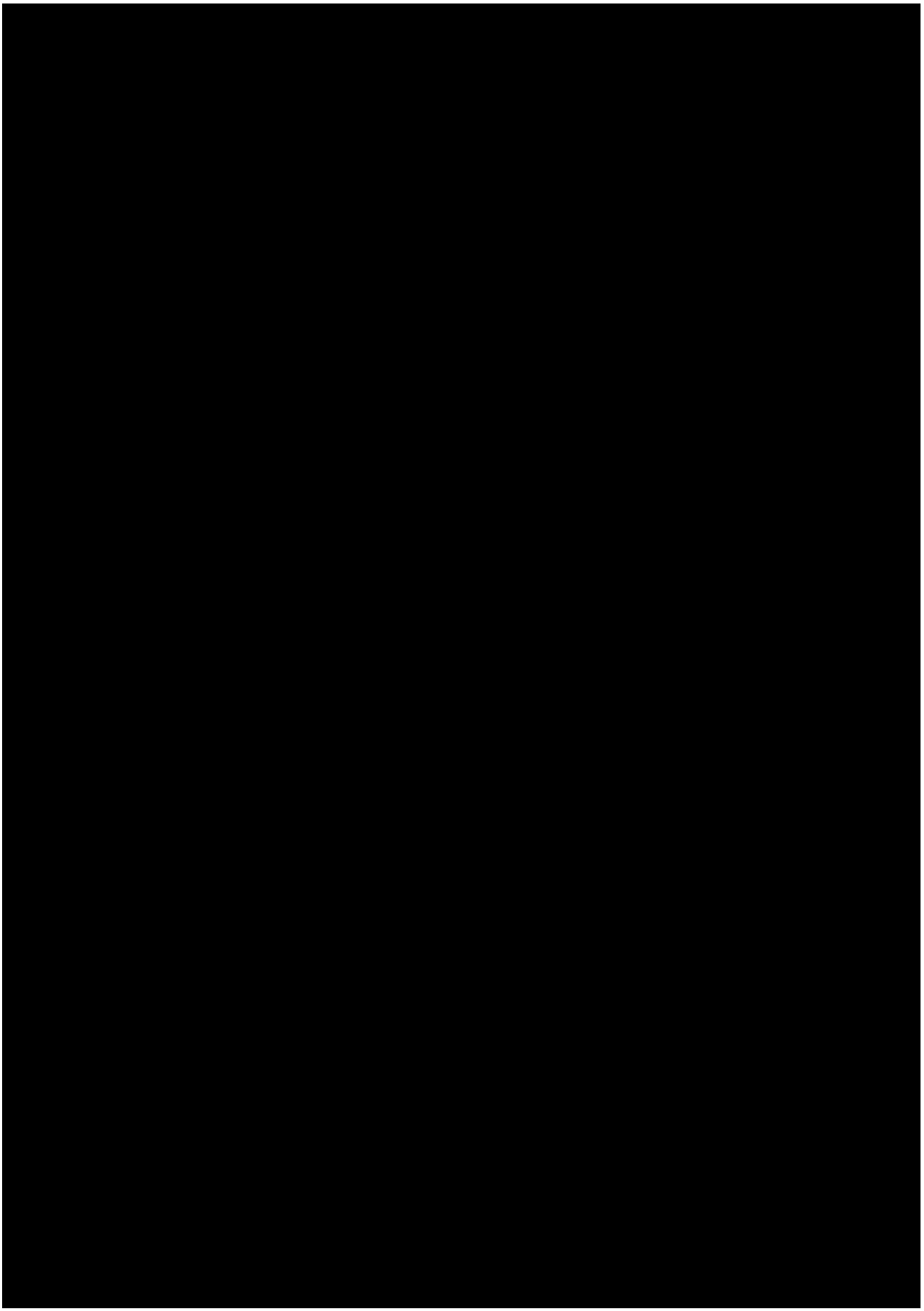
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único¨*	SG-12-UNICA-03
Nombre del sistema *	**SIRES**
Tipo de soporte:*	Soporte electrónico
Descripción:*	Sistema que recolecta y trata datos relacionados y estructurados que permiten validar el vínculo académico del titular de los datos con la dependencia, para posteriormente generar registros para uso de los servicios en Salas.
Características del lugar donde se resguardan los soportes:*	Alojamiento local, ubicado en SG-15-UNICA-06

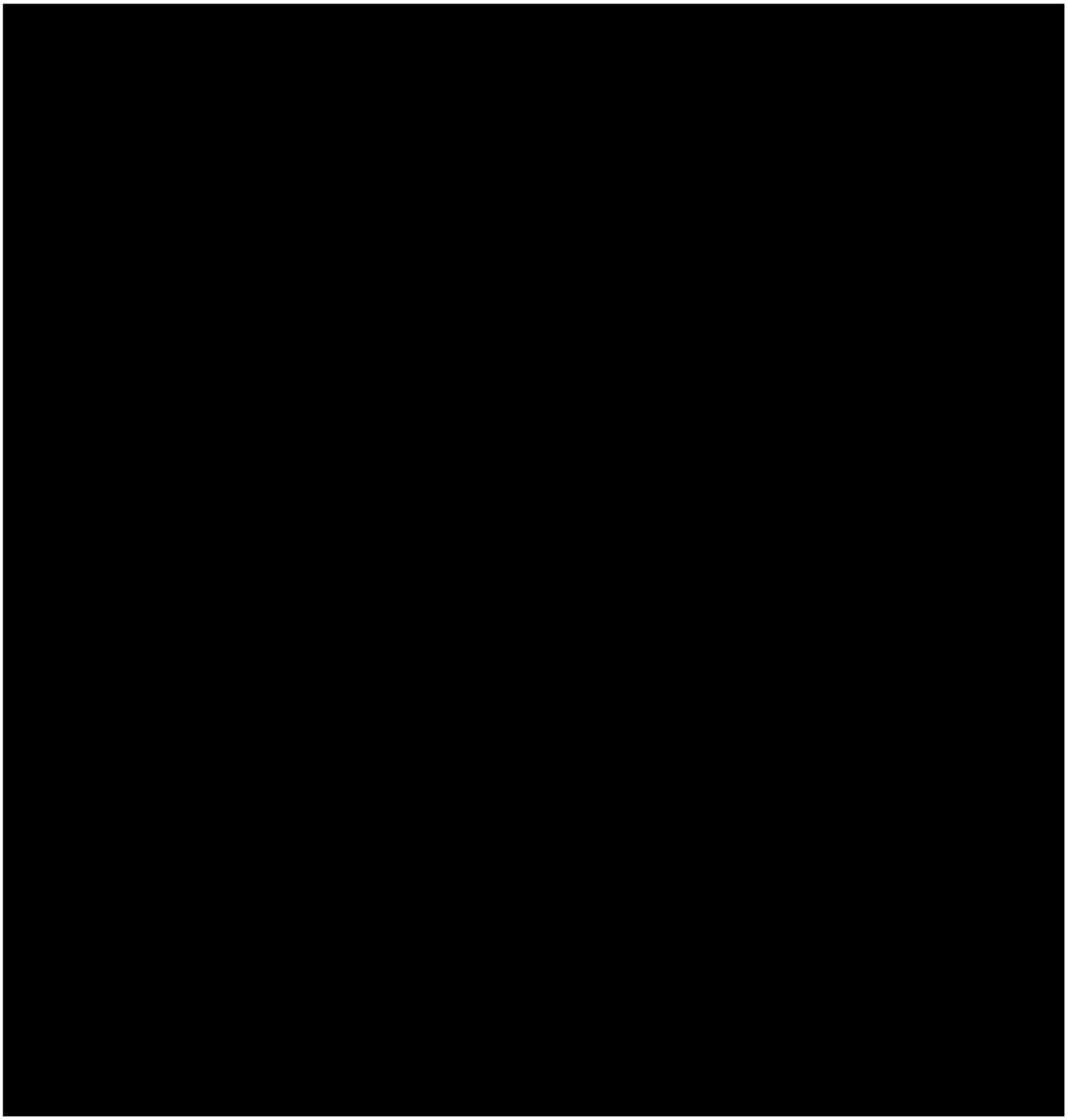
3. ANÁLISIS DE RIESGOS

[redacted]

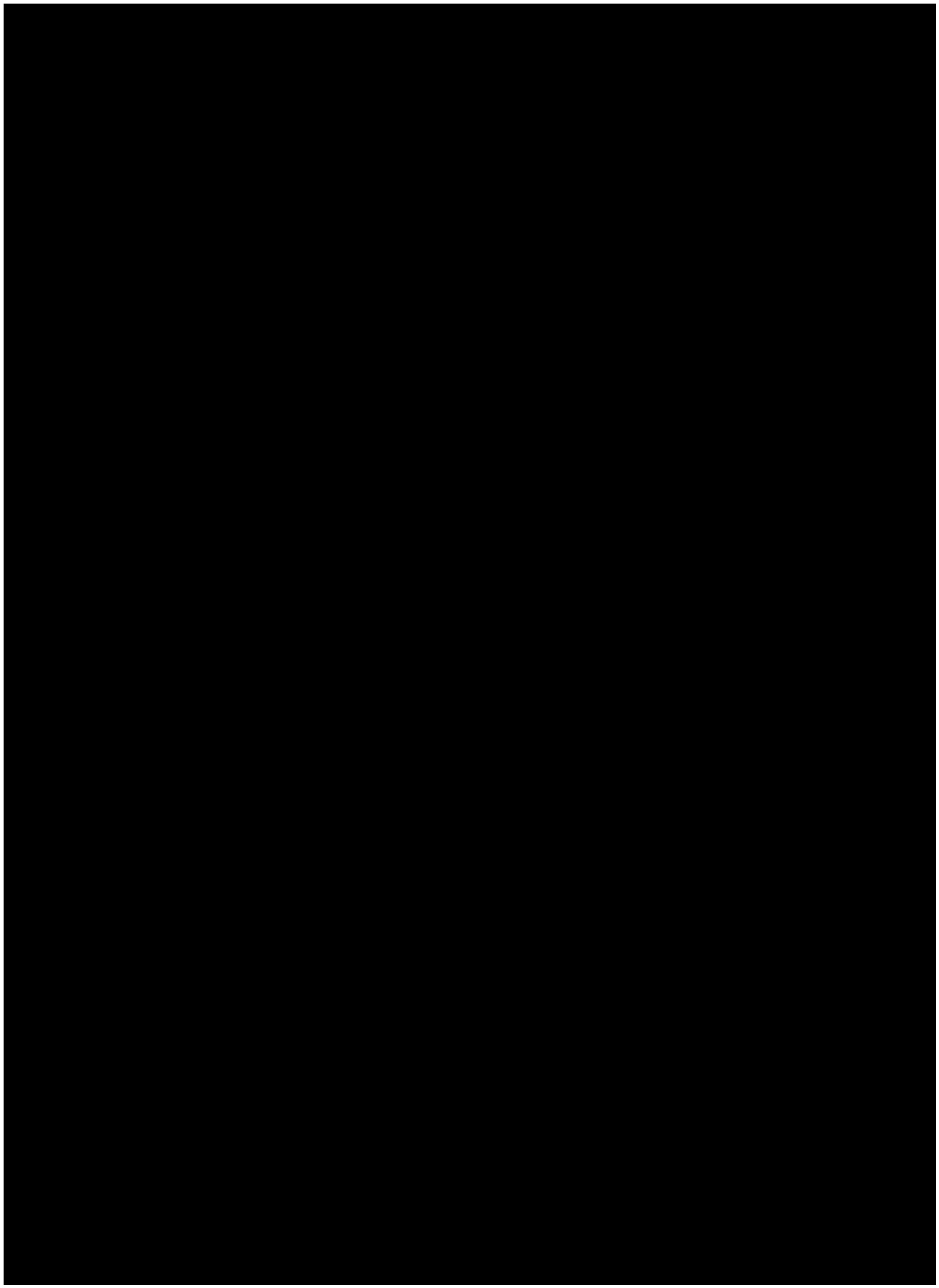
Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 148 a 151.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.



4. ANÁLISIS DE BRECHA



5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-12-UNICA-03
Nombre del sistema *	**SIRES**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[5]	No se realizan trasferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Nota: Ninguno de los sistemas realiza tratamiento de datos personales con soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema que almacena este sistema.

IV. REGISTRO DE INCIDENTES:

El procedimiento para la atención de incidentes consiste en hacer la verificación de las bitácoras del sistema, identificando a partir de ello de intentos de acceso o accesos que no correspondan a las actividades de operación rastreo de las acciones maliciosas, formulación de un pan de fortalecimiento del sistema y generación de informe dirigido al responsable del área.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

- **a)** ¿Cómo las identifica? No se cuenta con mecanismos de identificación
- **b)** ¿Cómo las autentifica? No se cuenta con mecanismos de autenticación
- **c)** ¿Cómo les autoriza el acceso? No se cuenta con mecanismos de control de acceso

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica? Se tiene definida una lista de acceso para el personal autorizado
2. ¿Cómo las autentifica? No se cuenta con mecanismos de autenticación
3. ¿Cómo les autoriza el acceso? Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado, previa presentación de orden de trabajo u oficio.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El titular de los datos que desee realizar la actualización de sus datos personales, debe enviar un oficio al área que opera el sistema indicando la actualización de sus datos personales.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

Es discrecional

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
sí

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
sí

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Se cifran solo las contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
sí

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo las contraseñas

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Los usuarios 1 y 2

b) ¿Quién autoriza la creación de nuevos perfiles?
El usuario 1

c) ¿Se lleva registro de la creación de nuevos perfiles?
El sistema almacena en bitácoras el registro

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
sí

c) ¿Cómo se evita el acceso remoto no autorizado?

- El acceso remoto a la red se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Se cuenta en el servidor con un sistema de control de acceso de identidades basado en usuario y contraseña y es discrecional.
- Se cuenta con controles de acceso discrecional.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos X, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual X,
   c) Periodicidad con que los realiza: Onpremise el respaldo es semanal, lo contenido en la nube pública no se respalda
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Onpremise en IAAS
3. Cómo y dónde archiva esos medios: en IAAS
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
No se cuenta con un plan de contingencia para los sistemas SG-03-UNICA-03

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
No existe

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
No se cuenta con sitio redundante

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-12-UNICA-03	
Nombre del sistema *	**SIRES**	
Recurso*	**Descripción***	**Control***
Bitácoras del sistema	Revisiones aleatorias	Revisar de forma aleatoria la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en el sistema. Responsables: Usuarios 2, 3 y 4

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-12-UNICA-03	
Nombre del sistema *	**SIRES**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Generación de respaldos	Revisión de los respaldos conforme a la planeación del servicio	Usuario: 4

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-12-UNICA-03	
Nombre del sistema *	SIRES	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Generación de respaldos	Se verificó la existencia de los respaldos y que su fecha de creación correspondiera al calendario de generación de respaldos.	Usuarios 2, 3, 4, 5 y 6

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-12-UNICA-03	
(Nombre del sistema)*	SIRES	
Medida de seguridad*	**Acciones***	**Responsable***
Bitácoras del sistema	• Con base en las Políticas de desarrollo seguro de software de tratamiento de datos personales, desarrollar módulos que den seguimiento a las actividades de los usuarios dentro del sistema de tratamiento de datos personales.	Responsables: Titular de la Secretaría General y Usuarios 1 y 2 Fecha: una vez creadas y aprobadas las políticas de desarrollo seguro de software, trabajar en la homologación de bitácoras en los sistemas de

	• Homologar el tipo de registro de las bitácoras para que estas se puedan recolectar y correlacionar en un SIEM	tratamiento de datos personales

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-12-UNICA-03		
(Nombre del sistema)*	SIRES		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Ver videos de los cursos ofrecidos para el tema de protección de datos personales por la Unidad de Transparencia de la UNAM.	Videos grabados por la Unidad de Transparencia de la UNAM relativos al tema de protección de datos personales	Actividad permanente	Todo el personal que trate datos personales
Asistir a cursos de protección de datos personales ofrecidos por la Unidad de Transparencia de la UNAM	Solicitar a la Unidad de Transparencia el acceso en línea y asíncrono a cursos sobre protección de datos personales	Actividad permanente	Todo el personal que trate datos personales

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-12-UNICA-03		
(Nombre del sistema)*	SIRES		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales			

9 MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-12-UNICA-03		
(Nombre del sistema)*	**SIRES**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema de tratamiento de datos personales	Actualizar conforme se da el avance tecnológico, las políticas de desarrollo seguro de software y la normatividad en el tratamiento de datos personales del software que aloja el sistema que trata datos personales	Permanente	Total

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-12-UNICA-03		
(Nombre del sistema)*	**SIRES**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
SIRES está alojado en el sistema SG-15-UNICA-06, por lo que en la descripción de ese sistema se describe lo solicitado en este punto.			

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General	
Identificador único*	SG-12-UNICA-03

(Nombre del sistema)*	SIRES	
Proceso*	**Descripción***	**Responsable***
SIRES está alojado en el sistema SG-15-UNICA-06, por lo que en la descripción de ese sistema se describe lo solicitado en este punto.		

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General		
Identificador único*	SG-12-UNICA-03	
(Nombre del sistema)*	SIRES	
Proceso*	**Descripción***	**Responsable***
SIRES está alojado en el sistema SG-15-UNICA-06, por lo que en la descripción de ese sistema se describe lo solicitado en este punto.		

10 PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

SICC

El SICC es un sistema que apoya a la gestión de los cursos que imparte UNICA.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-13-UNICA-04
Nombre del sistema *	**SICC**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre CURP Número de teléfono particular Correo electrónico Procedencia
Responsable*:	Unidad de Servicios de Cómputo Académico de la Secretaría General
Nombre*:	Enrique Barranco Vite
Cargo*:	Coordinador de la Unidad de Servicios de Cómputo Académico
Funciones*:	Coordinar y supervisar las actividades del grupo de trabajo del sistema de tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y promover su uso, exclusivamente para los fines que han sido recabados.
Encargados:	
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	Beatriz Barrera Hernández
Cargo*:	Jefa de Departamento
Funciones*:	Coordinar y supervisar las actividades del grupo de trabajo del sistema de tratamiento de datos personales.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso, exclusivamente de ellos para los fines que han sido recabados.
(Nombre del Usuario 2*)	Cruz Sergio Aguilar Díaz
Cargo*:	Responsable de Salas de Cómputo UNICA
Funciones*:	Supervisar las actividades operativas del sistema con respecto al tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso, exclusivamente de ellos para los fines que han sido recabados

(Nombre del Usuario 3*)	María del Rosario Barragán Paz
Cargo*:	Jefa de Departamento
Funciones*:	Coordinar y supervisar las actividades operativas del sistema de tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados. Generación de constancias a los asistentes a los cursos.
(Nombre del Usuario 4*)	Alfonso Arriaga Bautista
Cargo*:	Becario
Funciones*:	Operación del sistema y resguardo de datos personales
Obligaciones*:	Conocer los datos personales, operar y hacer uso exclusivamente para los fines que han sido recabados

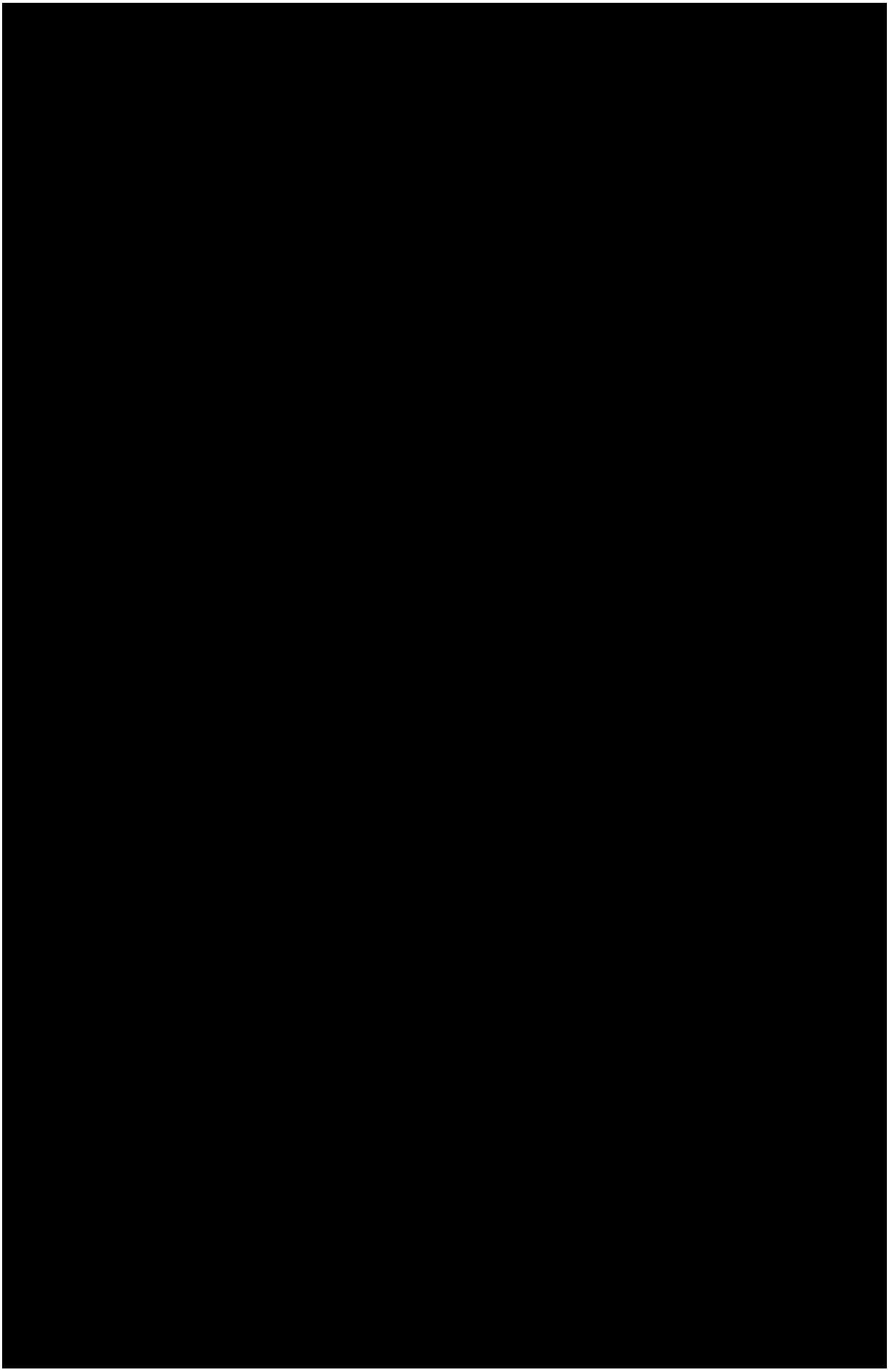
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único¨*	SG-13-UNICA-04
Nombre del sistema *	SICC
Tipo de soporte[6]:*	Soporte electrónico
Descripción[7]:*	Sistema que recolecta y trata datos relacionados y estructurados que permiten validar el vínculo laboral o académico del titular de los datos con la dependencia, para posteriormente crear cuentas a los solicitantes que usarán para tener acceso a las aplicaciones colaborativas.
Características del lugar donde se resguardan los soportes:*	Alojamiento local, ubicado en SG-15-UNICA-06

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 160 a 163.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

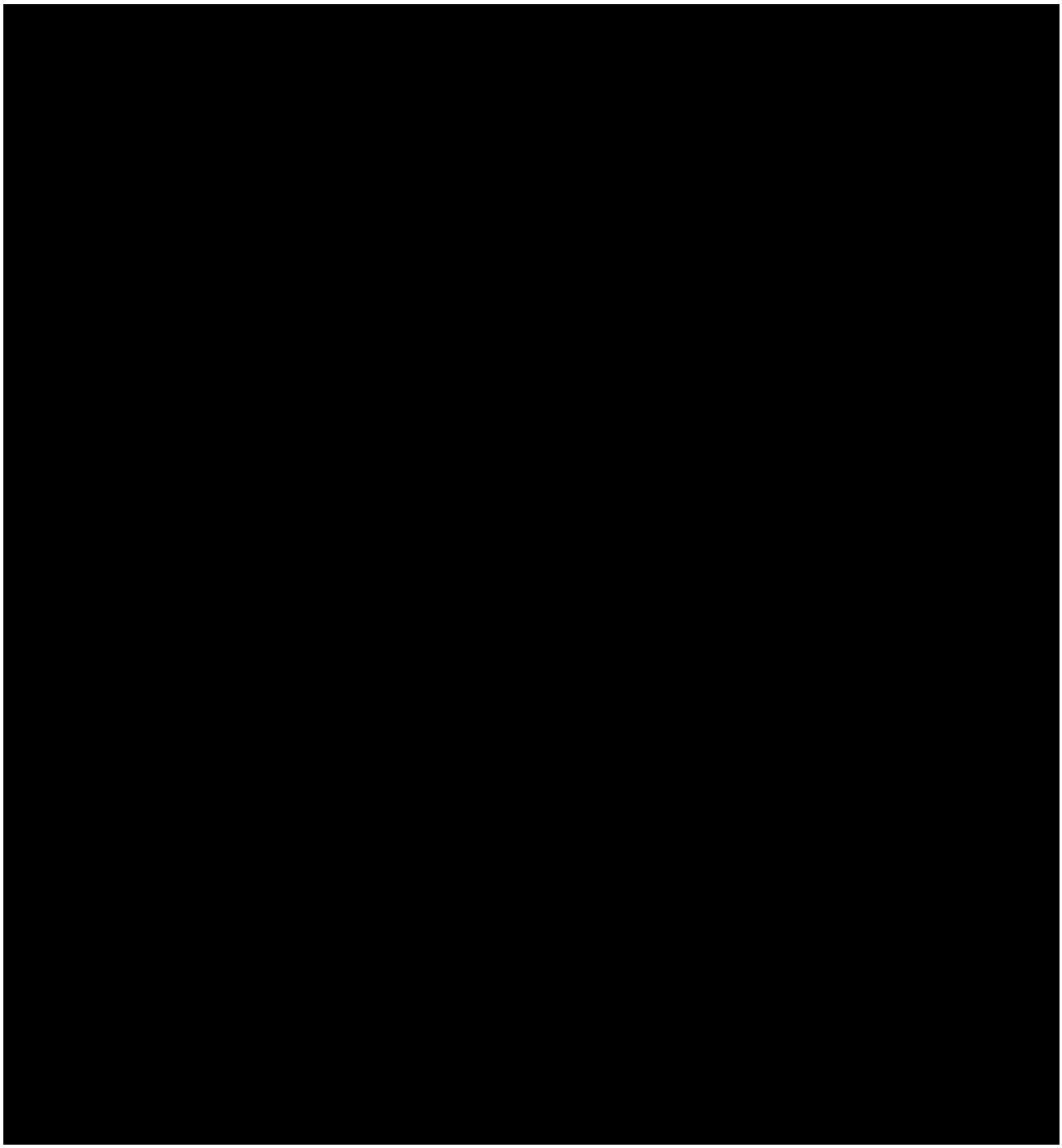


[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-13-UNICA-04
Nombre del sistema *	**SICC**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[8]	No se realizan trasferencias de datos personales mediante el traslado de soportes físicos

Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Nota: Ninguno de los sistemas realiza tratamiento de datos personales con soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema.

IV. REGISTRO DE INCIDENTES:

El procedimiento para la atención de incidentes consiste en hacer la verificación de las bitácoras del sistema, identificando a partir de ello de intentos de acceso o accesos que no correspondan a las actividades de operación rastreo de las acciones maliciosas, formulación de un pan de fortalecimiento del sistema y generación de informe dirigido al responsable del área.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica? No se cuenta con mecanismos de identificación
b) ¿Cómo las autentifica? No se cuenta con mecanismos de autenticación
c) ¿Cómo les autoriza el acceso? No se cuenta con mecanismos de control de acceso

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica? Se tiene definida una lista de acceso para el personal autorizado
2. ¿Cómo las autentifica? No se cuenta con mecanismos de autenticación
3. ¿Cómo les autoriza el acceso? Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado, previa presentación de orden de trabajo u oficio.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El titular de los datos que desee realizar la actualización de sus datos personales, debe enviar un oficio al área que opera el sistema indicando la actualización de sus datos personales.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

Es discrecional

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
sí

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
sí

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Se cifran solo las contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
sí

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo las contraseñas

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Los usuarios 1 y 2

b) ¿Quién autoriza la creación de nuevos perfiles?
El usuario 1

c) ¿Se lleva registro de la creación de nuevos perfiles?
El sistema almacena en bitácoras el registro

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
sí

c) ¿Cómo se evita el acceso remoto no autorizado?

- El acceso remoto a la red se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Se cuenta en el servidor con un sistema de control de acceso de identidades basado en usuario y contraseña y es discrecional.
- Se cuenta con controles de acceso discrecional.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos X, diferenciales ___ o incrementales___;

b) De forma automática ____ o Manual X,

c) Periodicidad con que los realiza: Onpremise el respaldo es semanal, lo contenido en la nube pública no se respalda

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Onpremise en IAAS

3. Cómo y dónde archiva esos medios: en IAAS
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   No se cuenta con un plan de contingencia para este sistema.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No existe

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   No se cuenta con sitio redundante

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-13-UNICA-04	
Nombre del sistema *	SICC	
Recurso*	**Descripción***	**Control***
Bitácoras del sistema	Revisiones aleatorias	Revisar de forma aleatoria la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en el sistema. Responsables: Usuario 2

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-13-UNICA-04	
Nombre del sistema *	SICC	
Medida de seguridad*	**Procedimiento***	**Responsable***

Generación de respaldos	Revisión de los respaldos conforme a la planeación del servicio	Usuario: 2

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-13-UNICA-04	
Nombre del sistema *	SICC	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Generación de respaldos	Se verificó la existencia de los respaldos y que su fecha de creación correspondiera al calendario de generación de respaldos.	Usuario 2

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-13-UNICA-04	
(Nombre del sistema)*	SICC	
Medida de seguridad*	**Acciones***	**Responsable***
Bitácoras del sistema	• Con base en las Políticas de desarrollo seguro de software de tratamiento de datos personales, desarrollar módulos que den seguimiento a las actividades de los usuarios dentro del sistema de tratamiento de datos personales. • Homologar el tipo de registro de las bitácoras para que estas se puedan recolectar y correlacionar en un SIEM	Responsables: Titular de la Secretaría General y Usuarios 1 y 2 Fecha: una vez creadas y aprobadas las políticas de desarrollo seguro de software, trabajar en la homologación de bitácoras en los sistemas de tratamiento de datos personales

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-13-UNICA-04		
Nombre del sistema *	**SICC**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Ver videos de los cursos ofrecidos para el tema de protección de datos personales por la Unidad de Transparencia de la UNAM.	Videos grabados por la Unidad de Transparencia de la UNAM relativos al tema de protección de datos personales	Actividad permanente	Todo el personal que trate datos personales
Asistir a cursos de protección de datos personales ofrecidos por la Unidad de Transparencia de la UNAM	Solicitar a la Unidad de Transparencia el acceso en línea y asíncrono a cursos sobre protección de datos personales	Actividad permanente	Todo el personal que trate datos personales

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-13-UNICA-04		
Nombre del sistema *	SICC		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-13-UNICA-04		
Nombre del sistema *	SICC		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema de	Actualizar conforme se da el avance	Permanente	Total

tratamiento de datos personales	tecnológico, las políticas de desarrollo seguro de software y la normatividad en el tratamiento de datos personales del software que aloja el sistema que trata datos personales		

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-13-UNICA-04		
Nombre del sistema *	**SICC**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
SICC está alojado en el sistema SG-15-UNICA-06, por lo que en la descripción de ese sistema se describe lo solicitado en este punto.			

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-13-UNICA-04	
Nombre del sistema *	SICC	
Proceso*	**Descripción***	**Responsable***
SICC está alojado en el sistema SG-15-UNICA-06, por lo que en la descripción de ese sistema se describe lo solicitado en este punto.		

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General	
Identificador único*	SG-13-UNICA-04

Nombre del sistema *	SICC	
Proceso*	**Descripción***	**Responsable***
LMSE está alojado en el sistema SG-15-UNICA-06, por lo que en la descripción del sistema se describe lo solicitado en este punto		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

SSPCC

Programa de Servicio Social para los estudiantes interesados en realizar su Servicio Social en temas relativos al cómputo y nuevas tecnologías.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-14-UNICA-05
Nombre del sistema *	SSPCC
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre Número de cuenta Correo electrónico Fecha de nacimiento Género CURP Teléfono particular Domicilio Carrera y clave Avance de créditos Porcentaje de avance Promedio Semestre Fecha de ingreso Historial académico División Coordinador de carrera
Responsable*:	Unidad de Servicios de Cómputo Académico de la Secretaría General
Nombre*:	Enrique Barranco Vite
Cargo*:	Coordinador de la Unidad de Servicios de Cómputo Académico
Funciones*:	Coordinar y supervisar las actividades del sistema de tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y promover su uso, exclusivamente para los fines que han sido recabados.
Encargados:	
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	Beatriz Barrera Hernández
Cargo*:	Jefa de Departamento

Funciones*:	Coordinar y supervisar las actividades del Programa así como lo referente al tratamiento de datos personales.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso, exclusivamente de ellos para los fines que han sido recabados.
(Nombre del Usuario 2*)	Ibeth Graciela Flores Muñoz
Cargo*:	Asistente ejecutiva
Funciones*:	Operar el sistema de tratamiento de datos personales
Obligaciones*:	Recabar los datos personales contenidos en el sistema y hacer uso, exclusivamente de ellos para los fines que han sido recabados

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único¨*	SG-14-UNICA-05
Nombre del sistema *	SSPCC
Tipo de soporte[9]:*	Soporte electrónico
Descripción[10]:*	Sistema que recolecta y trata datos relacionados y estructurados que permiten validar el vínculo académico del titular de los datos con la dependencia, para posteriormente tener una base de datos
Características del lugar donde se resguardan los soportes:*	Alojamiento híbrido, localmente alojado en computadora personal y la nube. El servicio de nube pública es proporcionado por terceros.

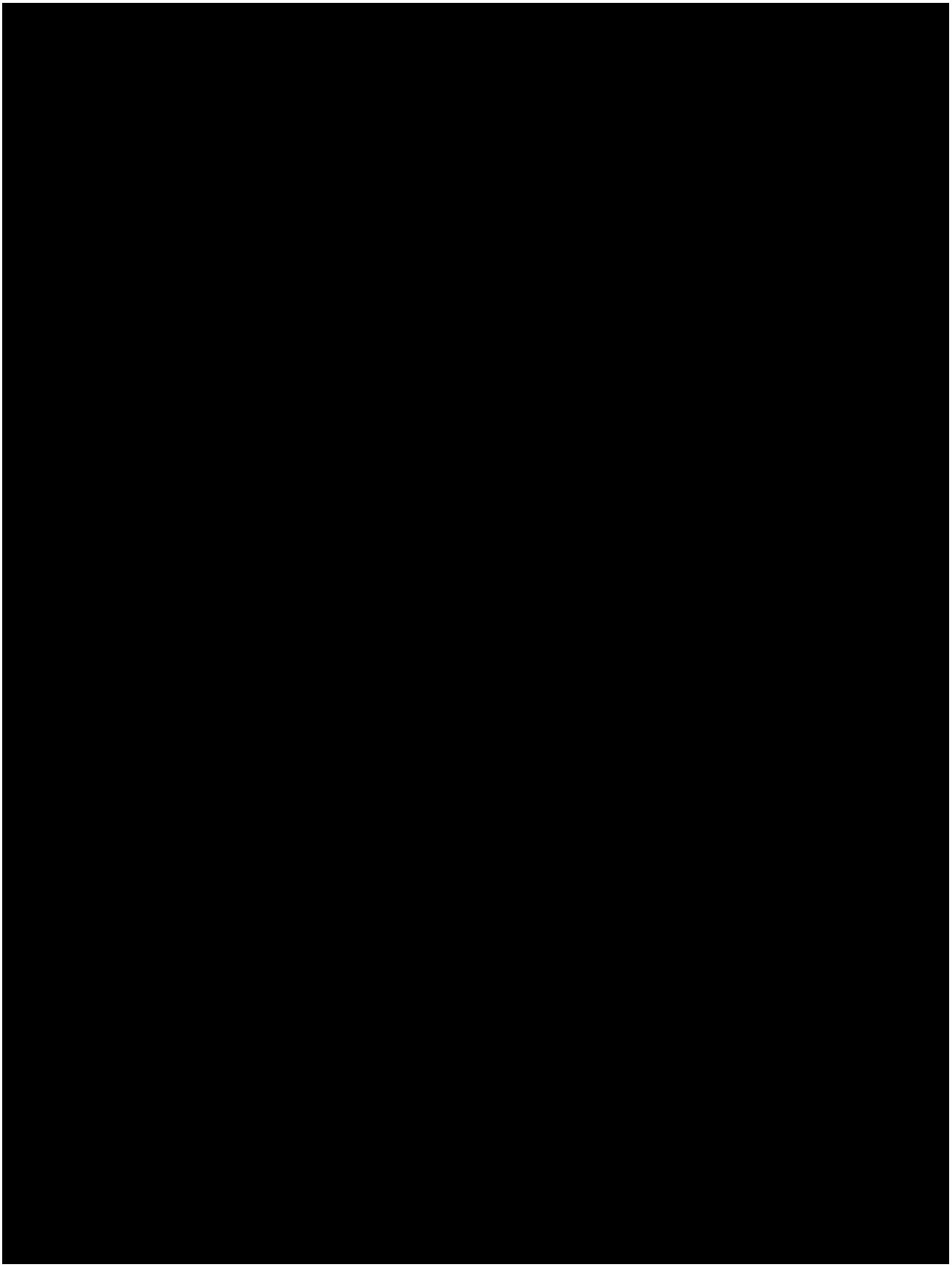
3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO¨, contenidos en las páginas 172 a 174.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-14-UNICA-05
Nombre del sistema *	**SSPCC**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[11]	No se realizan trasferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Nota: Ninguno de los sistemas realiza tratamiento de datos personales con soportes físicos

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.exe almacenado en un equipo personal, así como en la nube.

IV. REGISTRO DE INCIDENTES:

El procedimiento para la atención de incidentes consiste en hacer la verificación de las bitácoras del sistema, identificando a partir de ello de intentos de acceso o accesos que no correspondan a las actividades de operación rastreo de las acciones maliciosas, formulación de un plan de fortalecimiento del sistema y generación de informe dirigido al responsable del área.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica? No se cuenta con mecanismos de identificación
b) ¿Cómo las autentifica? No se cuenta con mecanismos de autenticación
c) ¿Cómo les autoriza el acceso? No se cuenta con mecanismos de control de acceso

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica? Se tiene definida una lista de acceso para el personal autorizado

.

2. ¿Cómo las autentifica? No se cuenta con mecanismos de autenticación
3. ¿Cómo les autoriza el acceso? Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado, previa presentación de orden de trabajo u oficio.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El titular de los datos que desee realizar la actualización de sus datos personales debe solicitarlo al área que opera el sistema indicando la actualización de sus datos personales.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

Es discrecional

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
sí

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
sí

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Se cifran solo las contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
sí

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo las contraseñas

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Usuario 2

b) ¿Quién autoriza la creación de nuevos perfiles?
El usuario 1

c) ¿Se lleva registro de la creación de nuevos perfiles?
El sistema almacena en bitácoras el registro

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
sí

c) ¿Cómo se evita el acceso remoto no autorizado?

- El acceso remoto a la red se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.

- Se cuenta en el servidor con un sistema de control de acceso de identidades basado en usuario y contraseña y es discrecional.
- Se cuenta con controles de acceso discrecional.

VIII. ROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos X, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual X,
   c) Periodicidad con que los realiza: El respaldo es semanal, lo contenido en la nube pública no se respalda
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Disco duro
3. Cómo y dónde archiva esos medios: Disco duro externo y nube
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). Usuario 2

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

   No se cuenta con un plan de contingencia para para este sistema

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No existe

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   No se cuenta con sitio redundante

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-14-UNICA-05	
Nombre del sistema *	SSPCC	
Recurso*	**Descripción***	**Control***
Revisión de base de datos	Revisiones periódicas	Revisar de forma periódica la base de datos con el fin de indagar si hubiera algún uso o comportamiento inusual en el sistema. Responsables: Usuario 2

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-14-UNICA-05	
Nombre del sistema *	SSPCC	
Medida de seguridad*	**Procedimiento***	**Responsable***
Generación de respaldos	Revisión de los respaldos conforme a la planeación del servicio	Usuario: 2

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-14-UNICA-05	
Nombre del sistema *	SSPCC	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Generación de respaldos	Se verificó la existencia de los respaldos y que su fecha de creación correspondiera al calendario de generación de respaldos.	Usuarios 2

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-14-UNICA-05	
(Nombre del sistema)*	SSPCC	
Medida de seguridad*	**Acciones***	**Responsable***
Bitácoras del sistema	• Con base en las Políticas de desarrollo seguro de software de tratamiento de datos personales, desarrollar	Responsables: Titular de la Secretaría General y Usuarios 1 y 2

	módulos que den seguimiento a las actividades de los usuarios dentro del sistema de tratamiento de datos personales. • Homologar el tipo de registro de las bitácoras para que estas se puedan recolectar y correlacionar en un SIEM	Fecha: una vez creadas y aprobadas las políticas de desarrollo seguro de software, trabajar en la homologación de bitácoras en los sistemas de tratamiento de datos personales

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-14-UNICA-05		
Nombre del sistema *	**SSPCC**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Ver videos de los cursos ofrecidos para el tema de protección de datos personales por la Unidad de Transparencia de la UNAM.	Videos grabados por la Unidad de Transparencia de la UNAM relativos al tema de protección de datos personales	Actividad permanente	Todo el personal que trate datos personales
Asistir a cursos de protección de datos personales ofrecidos por la Unidad de Transparencia de la UNAM	Solicitar a la Unidad de Transparencia el acceso en línea y asíncrono a cursos sobre protección de datos personales	Actividad permanente	Todo el personal que trate datos personales

8.2. Programa de difusión de la protección a los datos personales

Secretaría General	
Identificador único*	SG-14-UNICA-05
Nombre del sistema *	SSPCC

Actividad*	Descripción*	Duración*	Cobertura*
No se cuenta con un programa de difusión de la protección de datos personales			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-14-UNICA-05		
Nombre del sistema *	SSPCC		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema de tratamiento de datos personales	Actualizar conforme se da el avance tecnológico, las políticas de desarrollo seguro de software y la normatividad en el tratamiento de datos personales del software que aloja el sistema que trata datos personales	Permanente	Total

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-14-UNICA-05		
Nombre del sistema *	SSPCC		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Esta actividad se realiza según las políticas del prestador de servicios de cómputo de nube pública.			

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-14-UNICA-05	
Nombre del sistema *	SSPCC	
Proceso*	**Descripción***	**Responsable***
Respaldos	Se respalda la información en la nube y equipo personal	Indicar: a) Usuario 2 b) 6 horas

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General		
Identificador único*	SG-14-UNICA-05	
Nombre del sistema *	SSPCC	
Proceso*	**Descripción***	**Responsable***
Esta actividad se realiza según las políticas del prestador de servicios de cómputo de nube pública.		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

IAAS

Sistema informático de entrega de recursos bajo demanda por Internet

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

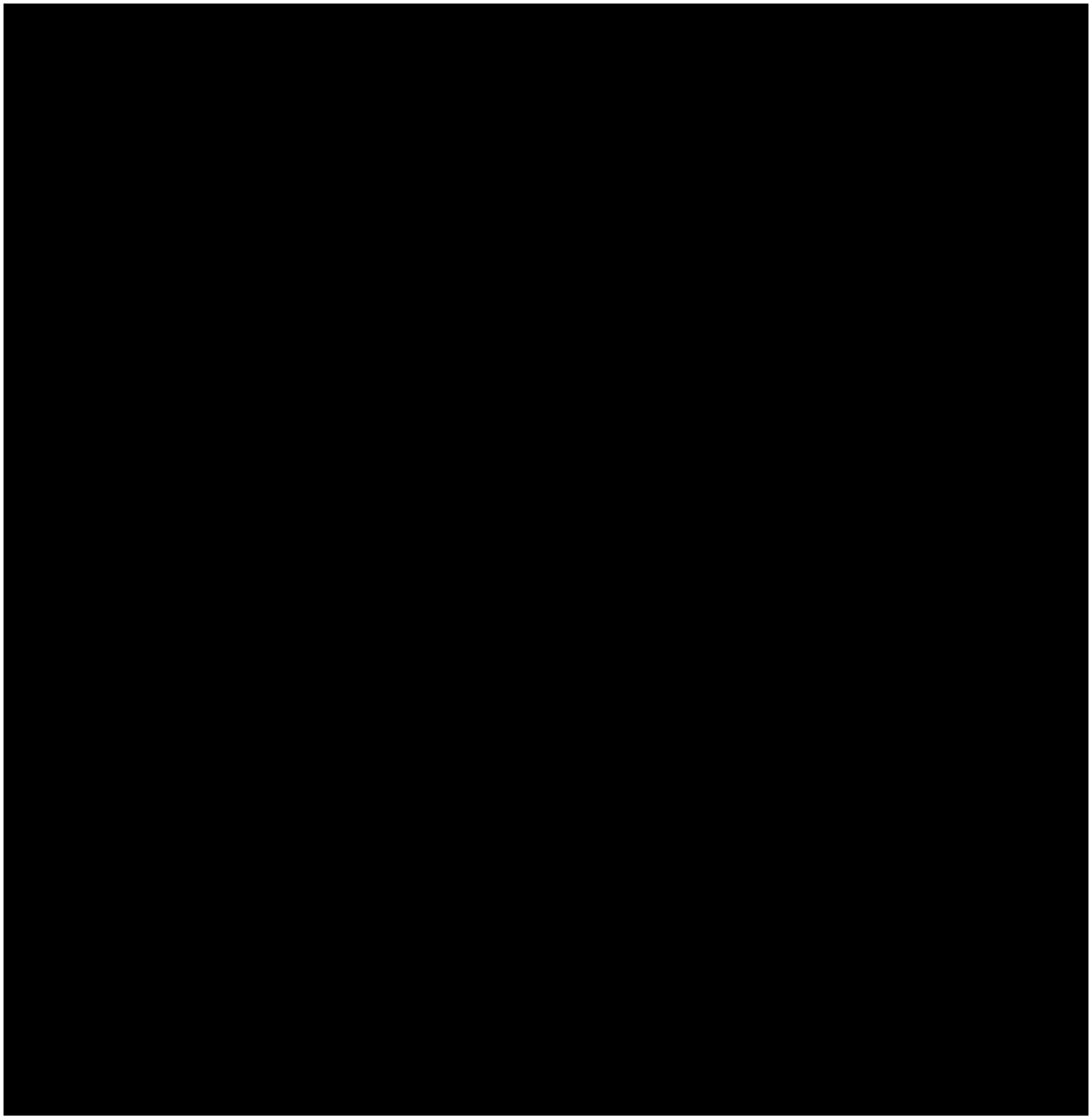
Secretaría General	
Identificador único*	SG-15-UNICA-06
(Nombre del sistema) *	**IAAS**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre Correo electrónico
Responsable*:	Unidad de Servicios de Cómputo Académico de la Secretaría General
Nombre*:	Enrique Barranco vite
Cargo*:	Coordinador de la Unidad de Servicios de Cómputo Académico
Funciones*:	Coordinar y supervisar las actividades del grupo de trabajo del sistema de tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y promover su uso, exclusivamente para los fines que han sido recabados.
	Encargados:
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	Rafael Sandoval Vázquez
Cargo*:	Jefe de Departamento
Funciones*:	Coordinar y supervisar las actividades operativas del sistema de tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 2*)	Luis Iván Navarrete Guerra
Cargo*:	Ayudante de Profesor
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 3*)	José Antonio Torres Galván

Cargo*:	Ayudante de Profesor
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 4*)	Jorge Refugio Santillán Gallegos
Cargo*:	Ayudante de Profesor
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 5*)	Carla Itzel Tapia Maceda
Cargo*:	Ayudante de Profesor
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 6*)	Erick Iván Pazarán Estrada
Cargo*:	Becario
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 7*)	Elvia Bautista Ortega
Cargo*:	Becaria
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios.
Obligaciones*:	
(Nombre del Usuario 8*)	Ángel Eduardo Moreno Peralta
Cargo*:	Becario
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.

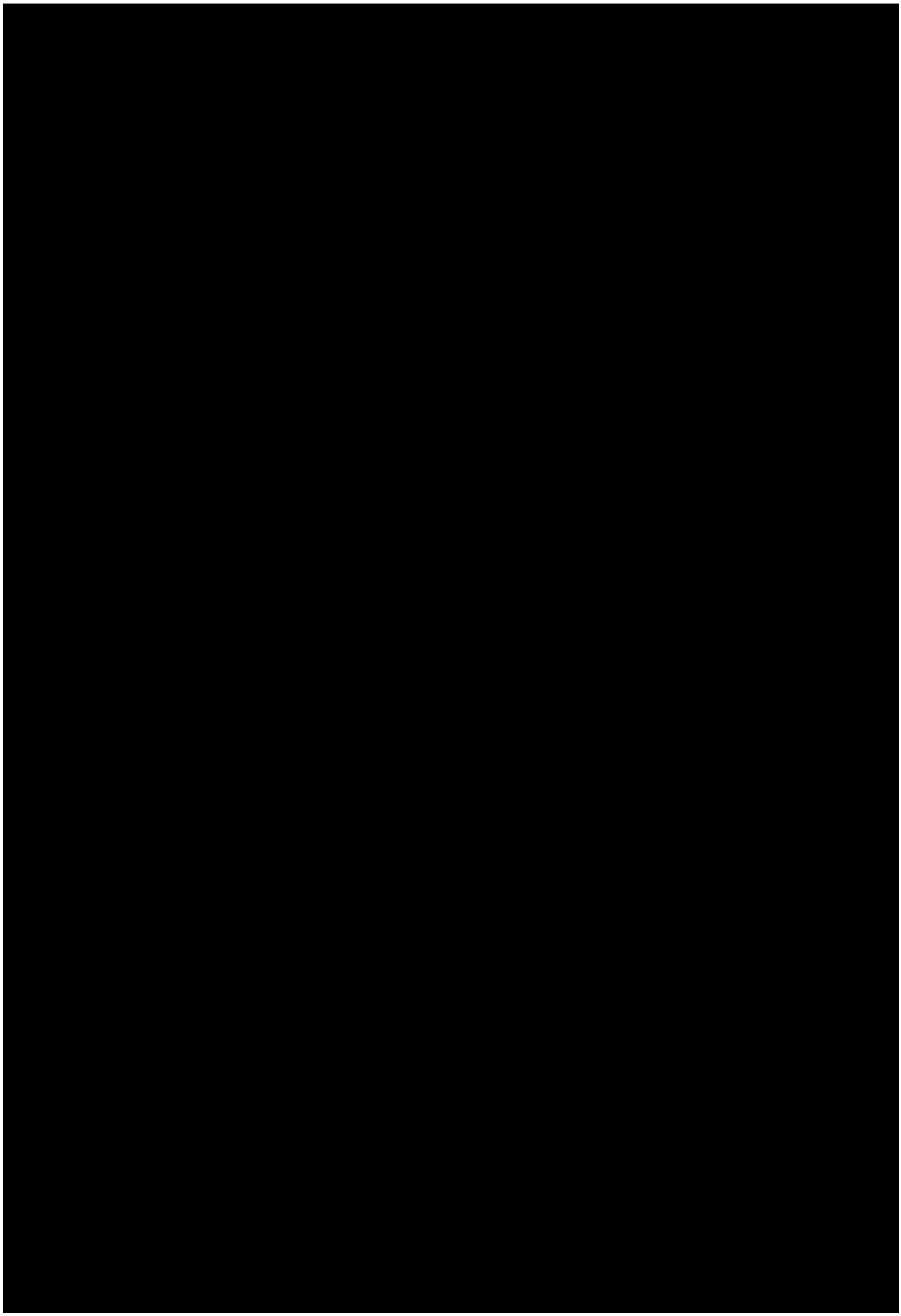
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

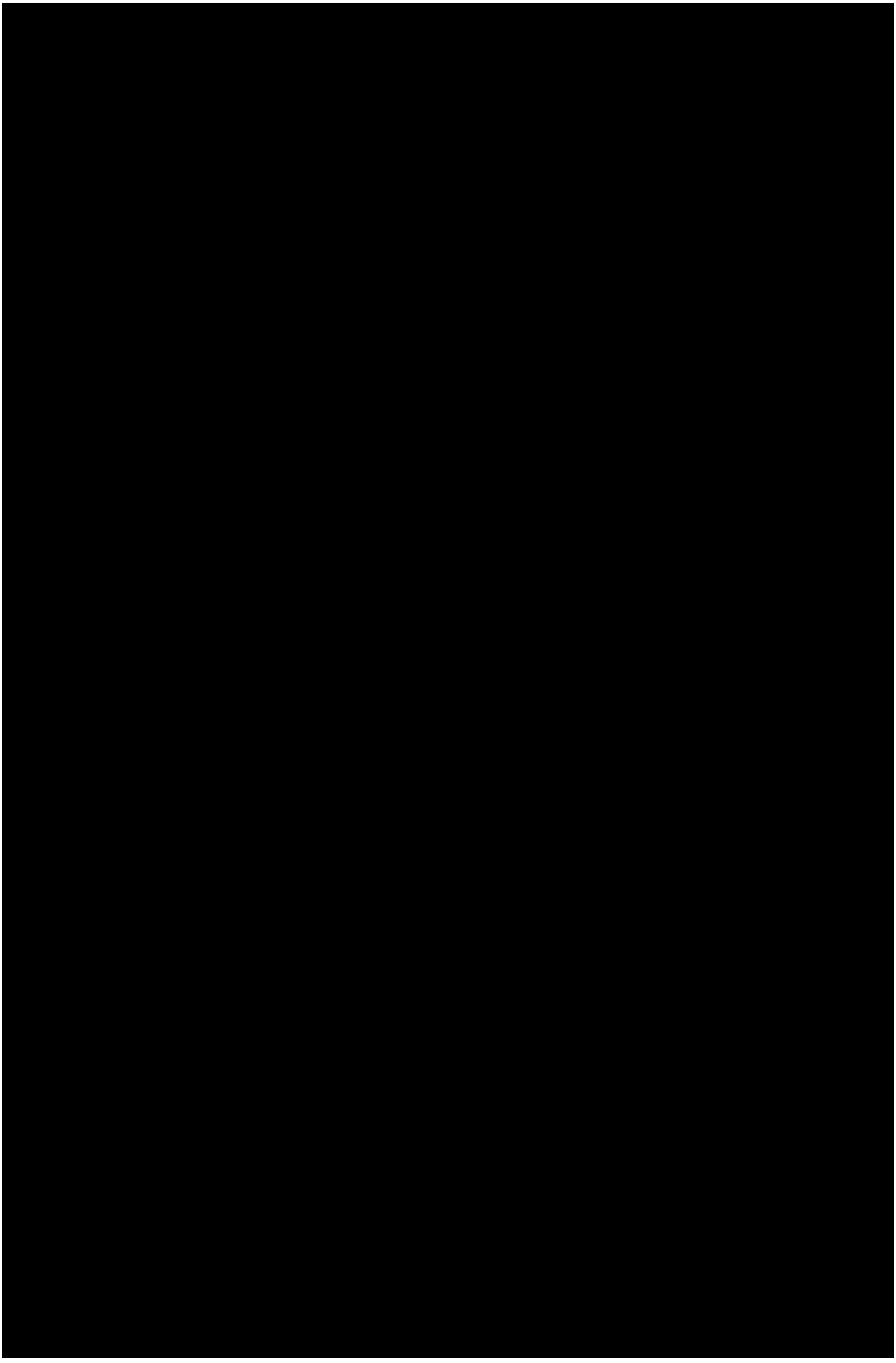
Secretaría General	
Identificador único¨*	SG-15-UNICA-06
(Nombre del sistema)	**IAAS**
Tipo de soporte:*	Soporte electrónico
Descripción:*	Sistema de Base de datos y conjunto de servicios que conectan a los usuarios con los servicios suministrados
Características del lugar donde se resguardan los soportes:*	Alojamiento en servidor local. Ubicado en un espacio cerrado y de acceso controlado

3. ANÁLISIS DE RIESGOS

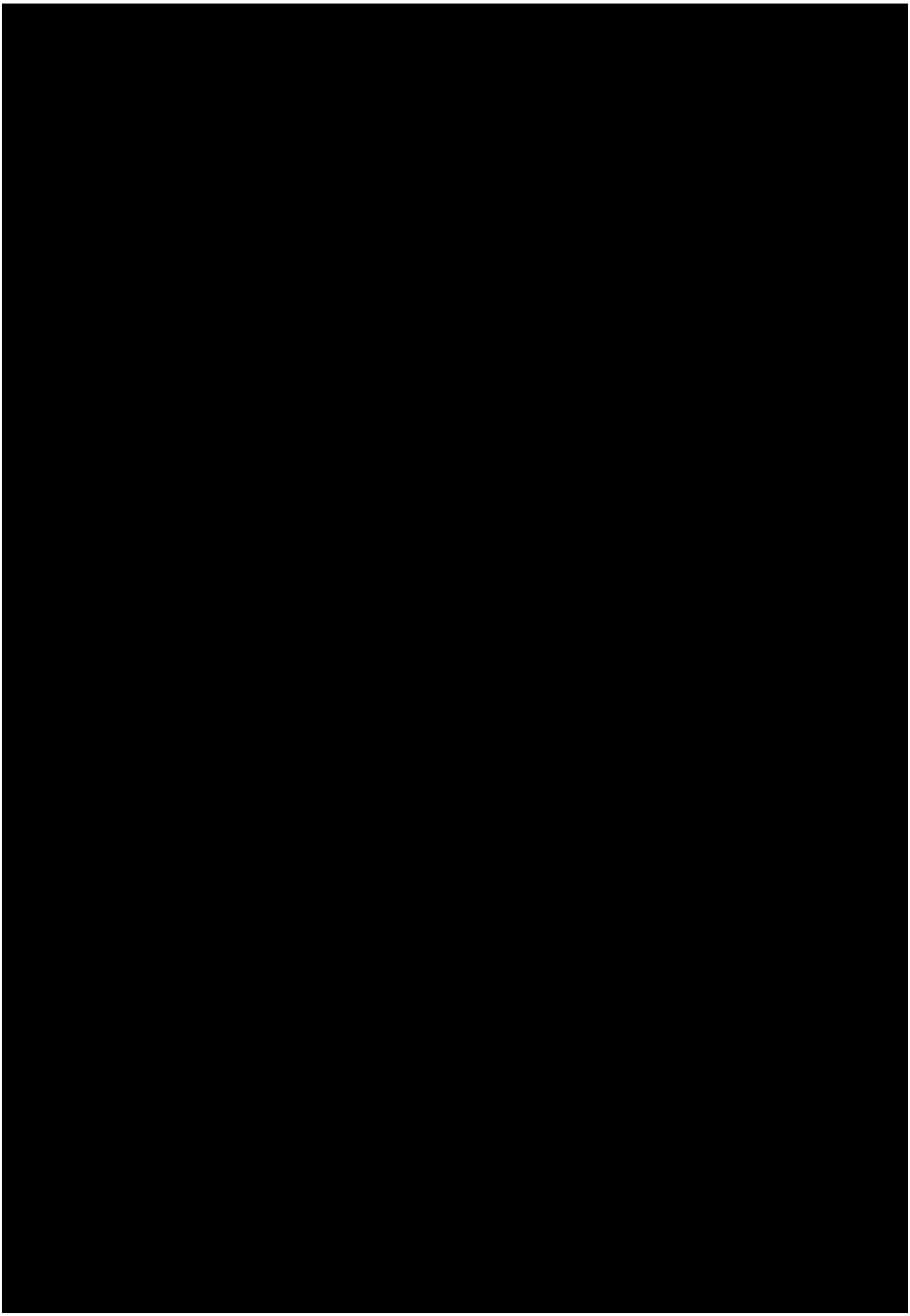


Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 184 a 190.
Período de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

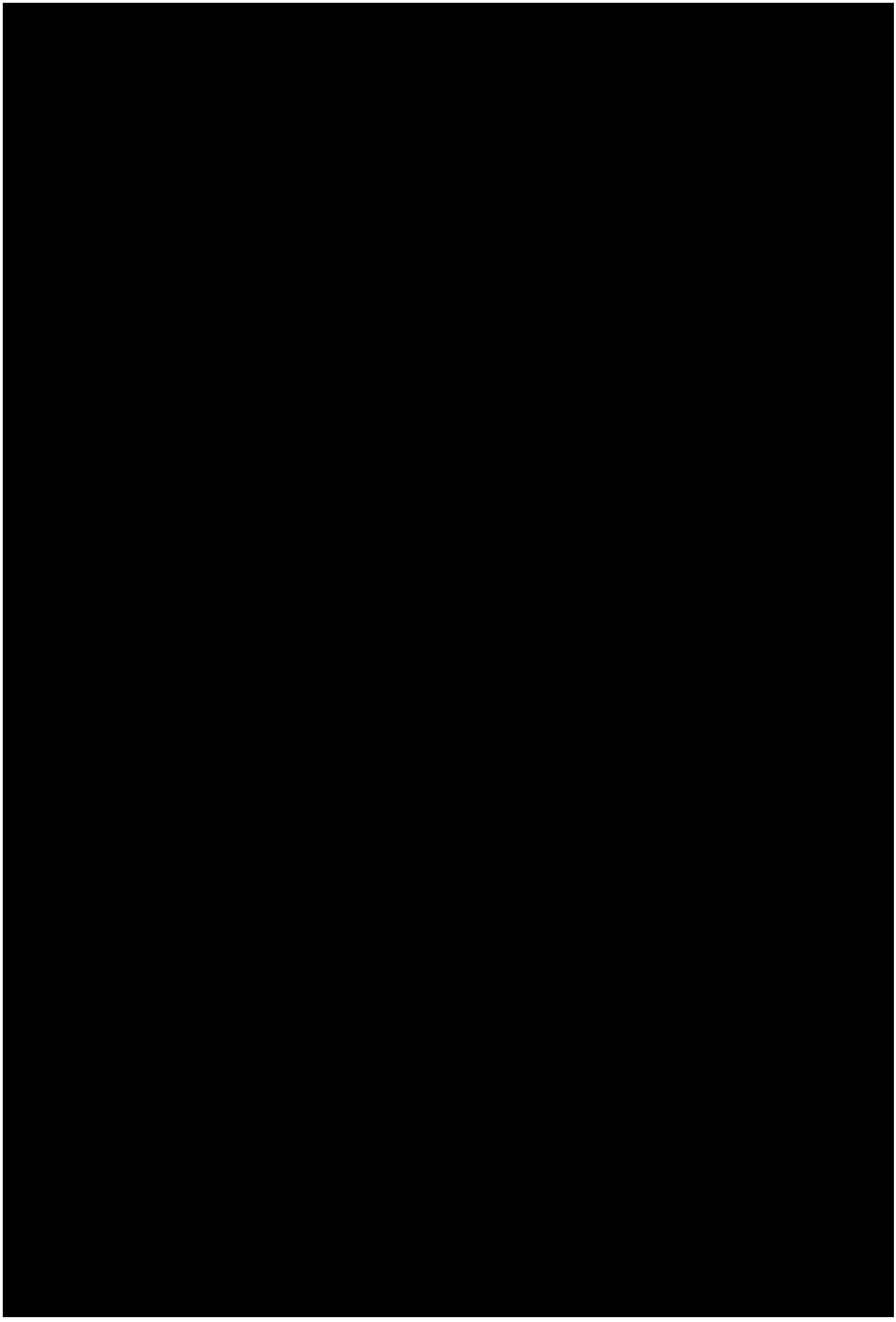




4. ANÁLISIS DE BRECHA



5. PLAN DE TRABAJO



[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-15-UNICA-06

(Nombre del sistema)*	IAAS
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[12]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema IAAS no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema en el servidor.

IV. REGISTRO DE INCIDENTES:

El procedimiento para la atención de incidentes consiste en hacer la verificación de las bitácoras del sistema, identificando a partir de ello de intentos de acceso o accesos que no correspondan a las actividades de operación, rastreo de las acciones maliciosas dentro del sistema, eliminación de las actividades maliciosas, formulación de un plan de fortalecimiento del sistema y generación de informe dirigido al responsable del área.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

   Para las personas que acceden a sus instalaciones:

   1. ¿Cómo las identifica?
      No se cuenta con mecanismos de identificación
   2. ¿Cómo las autentifica?
      No se cuenta con mecanismos de autenticación
   3. ¿Cómo les autoriza el acceso?
      No se cuenta con mecanismos de control de acceso

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

   Para las personas que acceden a dichos espacios interiores:

   1. ¿Cómo las identifica?
      Se tiene definida una lista de acceso para el personal autorizado.
   2. ¿Cómo las autentifica?

No se cuenta con mecanismo de autenticación

3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado, previa presentación de orden de trabajo u oficio.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El titular de los datos que desee realizar la actualización de sus datos personales debe enviar un oficio al área que opera el sistema indicando la actualización de sus datos personales

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

Está basado en roles

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
sí

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
sí

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
sí

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
sí

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo las contraseñas

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Los usuarios 1 y 2

b) ¿Quién autoriza la creación de nuevos perfiles?
El usuario 1

c) ¿Se lleva registro de la creación de nuevos perfiles?
El sistema almacena en bitácoras el registro

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
sí

c) ¿Cómo se evita el acceso remoto no autorizado?

- El acceso remoto a la red se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Se cuenta en el servidor con un sistema de control de acceso de identidades basado en usuario y contraseña.
- Se cuenta con controles de acceso basados en roles y privilegios.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos X, diferenciales ___ o incrementales___;
b) De forma automática ____ o Manual X,
c) Periodicidad con que los realiza: 1 mes

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: 13: Discos duros y de estado sólido

3. Cómo y dónde archiva esos medios: Almacenamiento directo mediante copia del servidor en storage de respaldo.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

Se cuenta con plan de contingencia, se anexa en documento DRP-SG-06-UNICA-06.pdf

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

No se realizan pruebas eficiencia

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

No se cuenta con sitio redundante

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General	
Identificador único*	SG-15-UNICA-06

(Nombre del sistema)*	IAAS	
Recurso*	**Descripción***	**Control***
Bitácoras del sistema	Revisiones aleatorias	Revisar de forma aleatoria la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en el sistema. Responsables: Usuarios 2, 3, 4, 5, 6, 7 y 8.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-15-UNICA-06	
(Nombre del sistema)*	**IAAS**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	Responsable: Usuarios 2, 3, 4, 5, 6, 7 y 8. Tiempo: 1 día hábil
Generación de respaldos	Revisión de la existencia de respaldos conforme a la calendarización programada.	Responsable: Usuarios 2, 3, 4, 5, 6, 7 y 8. Tiempo: 1 día hábil

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-15-UNICA-06	
(Nombre del sistema)*	**IAAS**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***

Principio del menor privilegio	Se eliminaron cuentas que ya no estaban activas y las que se mantienen cumplen con el principio de menor privilegio con base al rol asignado.	Usuarios 1 y 2
Generación de respaldos	Se verificó la existencia de los respaldos y que su fecha de creación correspondiera al calendario de generación de respaldos.	Usuarios 1 y 2

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-15-UNICA-06	
Nombre del sistema *	**IAAS**	
Medida de seguridad*	**Acciones***	**Responsable***
Actualización del software que habilita el sistema de tratamiento de datos personales	a) Adquirir (comprar) las licencias correspondientes para poder descargar e instalar las actualizaciones b) Mantener un esquema de control de acceso por redes privadas virtuales y autenticación por roles y privilegios.	Responsables: Titular de la Secretaría General y Usuarios 1 y 2

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-15-UNICA-06		
Nombre del sistema *	**IAAS**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Ver videos de los cursos ofrecidos para el tema de protección de datos personales por la Unidad de Transparencia de la UNAM.	Videos grabados por la Unidad de Transparencia de la UNAM relativos al tema de protección de datos personales	Actividad permanente	Todo el personal que trate datos personales
Asistir a cursos de protección de datos personales ofrecidos por la Unidad de Transparencia de la UNAM	Solicitar a la Unidad de Transparencia el acceso en línea y asíncrono a cursos sobre protección de datos personales	Actividad permanente	Todo el personal que trate datos personales

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-15-UNICA-06		
Nombre del sistema *	**IAAS**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General			
Identificador único*	SG-15-UNICA-06		
Nombre del sistema *	**IAAS**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del software que habilita el sistema de tratamiento de datos personales	Actualizar conforme se da el avance tecnológico las licencias del software que aloja el sistema que trata datos personales	Conforme el fabricante del software libere nuevas versiones estables del sistema	Total

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-15-UNICA-06		
Nombre del sistema *	**IAAS**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Sistema de enfriamiento de precisión en el Centro de datos	Capacidad de mantener la operación cuidando los aspectos de precisión temperatura, humedad y partículas de polvo en los rangos que debe operar el hardware del centro de datos	6 meses, una vez que se tenga presupuesto	Total
Expansión de la SAN (Storage Área Network) para garantizar en cuanto a capacidad los planes de respaldos y continuidad de las operaciones	Capacidad de espacio de almacenamiento para cumplir con el plan de respaldos y con ello robustecer el plan de recuperación ante desastres	6 meses, una vez que se tenga presupuesto	Total
Programa de renovación oficial de equipos de cómputo del Centro de datos	Capacidad de mantener la operación una vez que los equipos de cómputo han alcanzado su vida útil o su límite de tiempo de garantía	6 meses, una vez que se tenga presupuesto	Total
Añadir a la Seguridad perimetral la capacidad de Prevención de intrusos a través de un IPS	Identificación de amenazas hacia los activos de información y toma de decisiones para el bloqueo de ataques a la confidencialidad, integridad y disponibilidad de los datos personales	6 meses, una vez que se tenga presupuesto	Total

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-15-UNICA-06	
Nombre del sistema *	**IAAS**	
Proceso*	**Descripción***	**Responsable***
Plan de respaldos	Se clasifica la información conforme a la frecuencia en que cambia. Se crea un calendario de respaldos conforme a la clasificación anterior Se respalda la información en discos duros y de estado sólido conforme a la capacidad de estos Se verifica la existencia y funcionamiento de los respaldos	Usuarios 2, 3, 4, 5, 6 ,7 y 8 Tiempo máximo de ejecución: 1 día hábil

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General		
Identificador único*	SG-15-UNICA-06	
Nombre del sistema *	**IAAS**	
Proceso*	**Descripción***	**Responsable***
Formateo de bajo nivel de discos de almacenamiento	Uso de herramientas open source para el borrado seguro y sobre escritura de los discos.	Responsables: Usuarios 1 y 2

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

ACEOC

Sistema de obtención de información y validación del vínculo laboral o académico del solicitante con la dependencia, y posterior creación de la cuenta de usuario onpremise o en plataformas de nube pública, según la solicitud, para tener acceso a las aplicaciones colaborativas o de mensajería.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-16-UNICA-07
(Nombre del sistema) *	**ACEOC**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre Número de trabajador CURP Correo electrónico Número de cuenta
Responsable*:	Unidad de Servicios de Cómputo Académico de la Secretaría General
Nombre*:	Enrique Barranco vite
Cargo*:	Coordinador de la Unidad de Servicios de Cómputo Académico
Funciones*:	Coordinar y supervisar las actividades del grupo de trabajo del sistema de tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y promover su uso, exclusivamente para los fines que han sido recabados.
	Encargados:
Conforme al Artículo 3, párrafo XV de la LGPDPPSO, y artículo 2, párrafo XIII de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad. **La figura de Encargado no está presente para este sistema.**	
	Usuarios:
(Nombre del Usuario 1*)	Rafael Sandoval Vázquez
Cargo*:	Jefe de Departamento
Funciones*:	Coordinar y supervisar las actividades operativas del sistema de tratamiento de datos personales
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 2*)	Luis Iván Navarrete Guerra
Cargo*:	Ayudante de Profesor

Funciones*:	Operar el sistema de tratamiento de datos personales, verificar vínculo laboral o académico del solicitante con la dependencia
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 3*)	José Antonio Torres Galván
Cargo*:	Ayudante de Profesor
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 4*)	Jorge Refugio Santillán Gallegos
Cargo*:	Ayudante de Profesor
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 5*)	Carla Itzel Tapia Maceda
Cargo*:	Ayudante de Profesor
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 6*)	Erick Iván Pazarán Estrada
Cargo*:	Becario
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 7*)	Elvia Bautista Ortega
Cargo*:	Becaria
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.
(Nombre del Usuario 8*)	Ángel Eduardo Moreno Peralta

Cargo*:	Becario
Funciones*:	Operar el sistema de tratamiento de datos personales, alta y baja de usuarios.
Obligaciones*:	Conocer los datos personales contenidos en el sistema y hacer uso exclusivo para los fines que han sido recabados.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

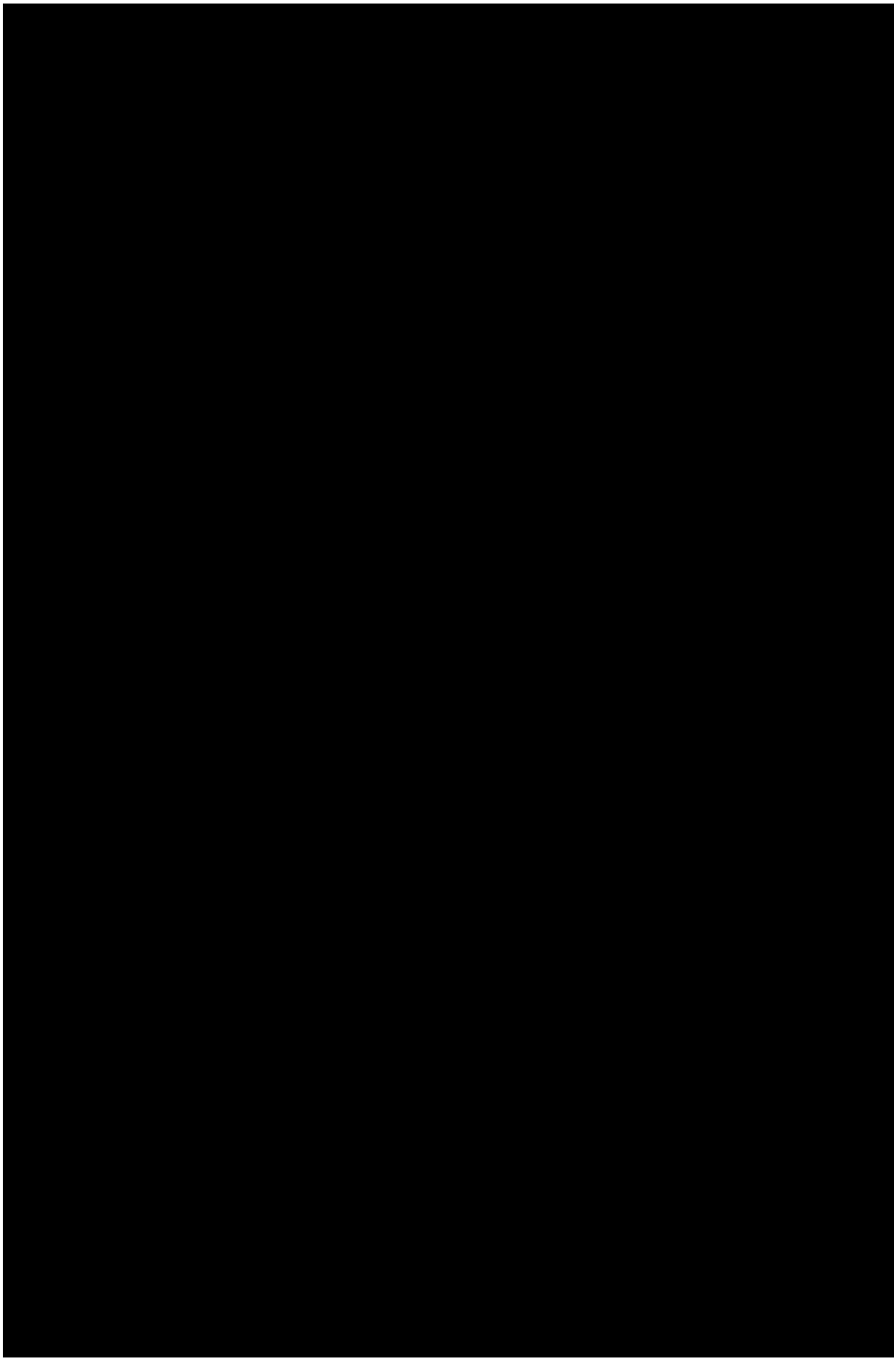
Secretaría General	
Identificador único¨*	SG-16-UNICA-07
(Nombre del sistema *)	**ACEOC**
Tipo de soporte[14]:*	Soporte electrónico
Descripción[15]:*	Sistema que recolecta y trata datos relacionados y estructurados que permiten validar el vínculo laboral o académico del titular de los datos con la dependencia, para posteriormente crear cuentas a los solicitantes, que usaran para tener acceso a las aplicaciones colaborativas o de mensajería.
Características del lugar donde se resguardan los soportes[16]:*	Alojamiento híbrido, localmente alojado en SG-15-UNICA-06 y en sistema de nube pública. El servicio de nube pública es proporcionado por terceros.

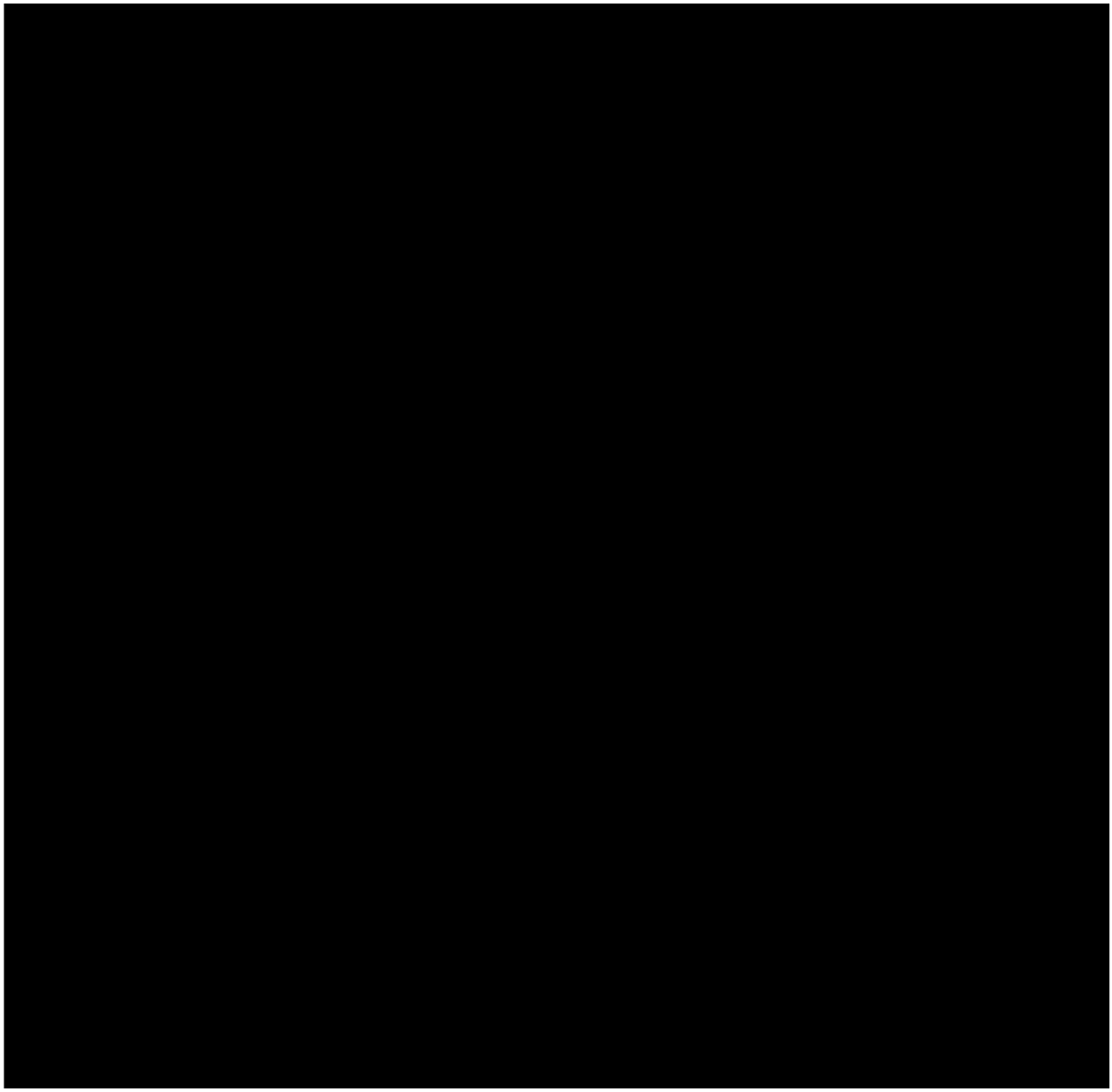
3. ANÁLISIS DE RIESGOS

[redacted]

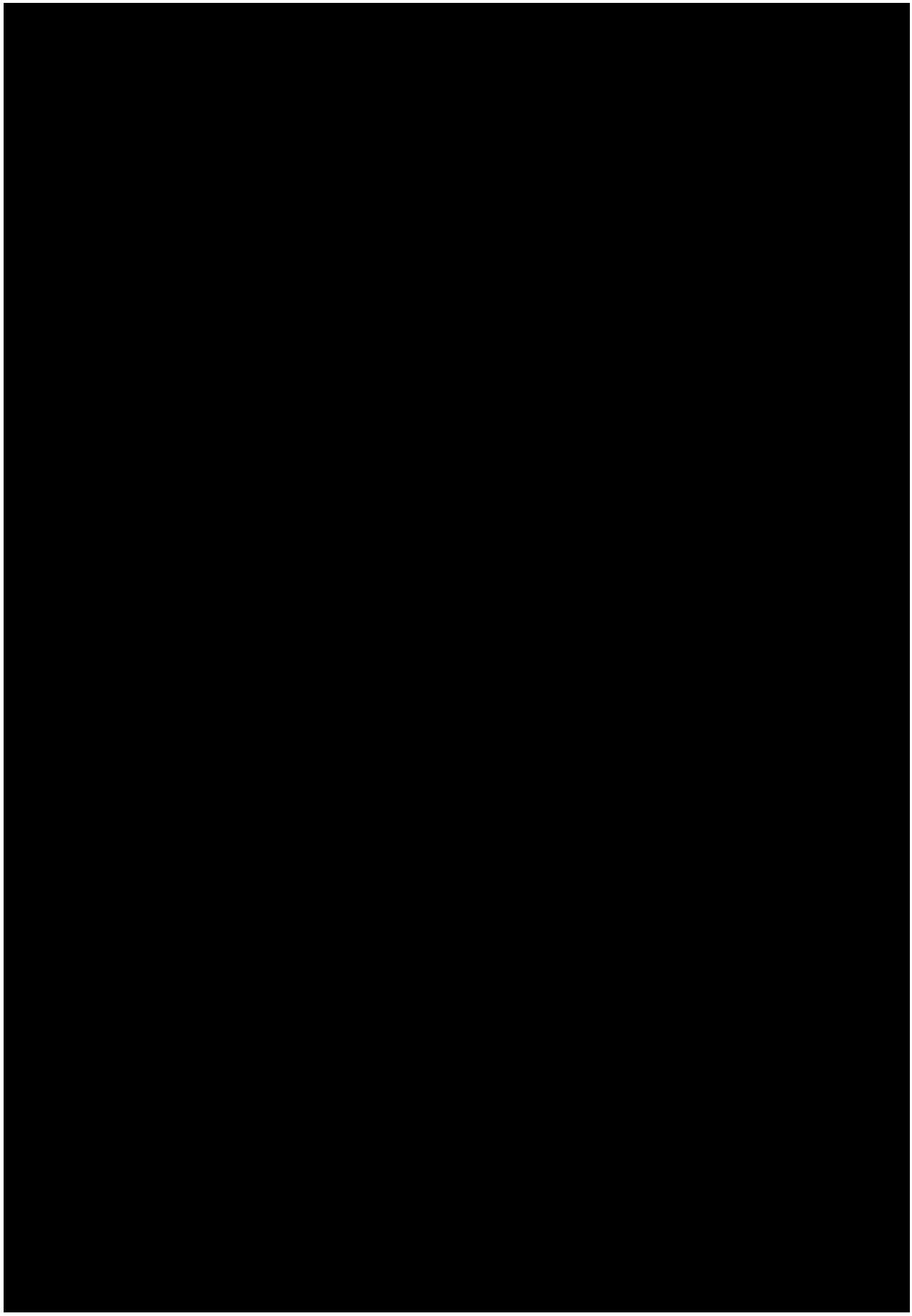
Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 201 a 207.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

.
.

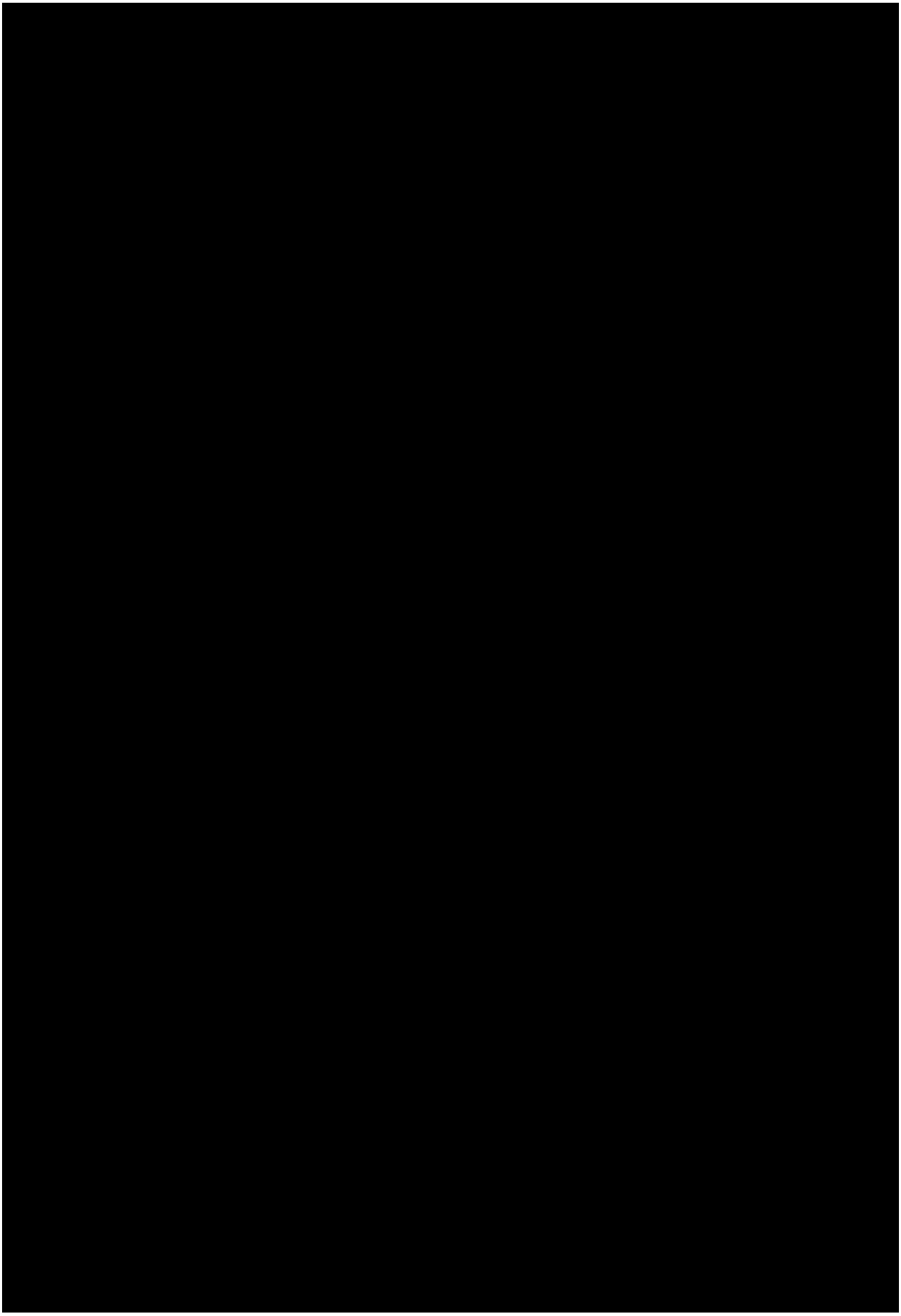




4. ANÁLISIS DE BRECHA



5. PLAN DE TRABAJO



[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría General	
Identificador único*	SG-16-UNICA-07
(Nombre del sistema)*	**ACEOC**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.

Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema ACEOC no realiza tratamiento de datos personales con soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema que almacena el sistema ACEOC

IV. REGISTRO DE INCIDENTES:

El procedimiento para la atención de incidentes consiste en hacer la verificación de las bitácoras del sistema, identificando a partir de ello de intentos de acceso o accesos que no correspondan a las actividades de operación, rastreo de las acciones maliciosas dentro del sistema, eliminación de las actividades maliciosas, formulación de un plan de fortalecimiento del sistema y generación de informe dirigido al responsable del área.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

   Para las personas que acceden a sus instalaciones:

   1. ¿Cómo las identifica?
      No se cuenta con mecanismos de identificación
   2. ¿Cómo las autentifica?
      No se cuenta con mecanismos de autenticación
   3. ¿Cómo les autoriza el acceso?
      No se cuenta con mecanismos de control de acceso

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

   Para las personas que acceden a dichos espacios interiores:

   1. ¿Cómo las identifica?
      Se tiene definida una lista de acceso para el personal autorizado.
   2. ¿Cómo las autentifica?
      No se cuenta con mecanismo de autenticación
   3. ¿Cómo les autoriza el acceso?
      Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado, previa presentación de orden de trabajo u oficio.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El titular de los datos que desee realizar la actualización de sus datos personales debe enviar un oficio al área que opera el sistema indicando la actualización de sus datos personales

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

Es discrecional

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
sí

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
sí

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Se cifran solo las contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
sí

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo las contraseñas

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Los usuarios 1 y 2

b) ¿Quién autoriza la creación de nuevos perfiles?
El usuario 1

c) ¿Se lleva registro de la creación de nuevos perfiles?
El sistema almacena en bitácoras el registro

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
sí

c) ¿Cómo se evita el acceso remoto no autorizado?

- El acceso remoto a la red se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Se cuenta en el servidor con un sistema de control de acceso de identidades basado en usuario y contraseña y es discrecional.
- Se cuenta con controles de acceso discrecional.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos X, diferenciales ___ o incrementales___;

b) De forma automática ____ o Manual X,

c) Periodicidad con que los realiza: Onpremise el respaldo es semanal, lo contenido en la nube pública no se respalda

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Onpremise en IAAS

3. Cómo y dónde archiva esos medios: en IAAS

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

Para este sistema no se cuenta con un plan de contingencia.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

N/A

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

No se cuenta con sitio redundante

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría General		
Identificador único*	SG-16-UNICA-07	
(Nombre del sistema)*	**ACEOC**	
Recurso*	**Descripción***	**Control***
Bitácoras del sistema	Revisiones aleatorias	Revisar de forma aleatoria la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en el sistema. Responsables: Usuarios 2, 3, 4, 5, 6, 7 y 8.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría General		
Identificador único*	SG-16-UNICA-07	
(Nombre del sistema)*	**ACEOC**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	Responsable: Usuarios 2, 3, 4, 5, 6, 7 y 8. Tiempo: 1 día hábil
Generación de respaldos	Revisión de la existencia de respaldos conforme a la calendarización programada por IAAS	Responsable: Usuarios 2, 3, 4, 5, 6, 7 y 8. Tiempo: 1 día hábil

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría General		
Identificador único*	SG-16-UNICA-07	
(Nombre del sistema)*	**ACEOC**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se eliminaron cuentas que ya no estaban activas y las que se mantienen cumplen con el principio de menor privilegio con base al rol asignado.	Usuarios 1 y 2
Generación de respaldos	Se verificó la existencia de los respaldos y que su fecha de creación correspondiera al calendario de generación de respaldos.	Usuarios 1 y 2

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría General		
Identificador único*	SG-16-UNICA-07	
(Nombre del sistema)*	**ACEOC**	
Medida de seguridad*	**Acciones***	**Responsable***
Bitácoras del sistema	• Con base en las Políticas de desarrollo seguro de software de tratamiento de datos personales, desarrollar módulos que den seguimiento a las actividades de los usuarios dentro del sistema de tratamiento de datos personales. • Homologar el tipo de registro de las bitácoras para que estas se puedan recolectar y correlacionar en un SIEM	Responsables: Titular de la Secretaría General y Usuarios 1 y 2 Fecha: una vez creadas y aprobadas las políticas de desarrollo seguro de software, trabajar en la homologación de bitácoras en los sistemas de tratamiento de datos personales

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría General			
Identificador único*	SG-16-UNICA-07		
(Nombre del sistema)*	**ACEOC**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Ver videos de los cursos ofrecidos para el tema de protección de datos personales por la Unidad de Transparencia de la UNAM.	Videos grabados por la Unidad de Transparencia de la UNAM relativos al tema de protección de datos personales	Actividad permanente	Todo el personal que trate datos personales
Asistir a cursos de protección de datos personales ofrecidos por la Unidad de Transparencia de la UNAM	Solicitar a la Unidad de Transparencia el acceso en línea y asíncrono a cursos sobre protección de datos personales	Actividad permanente	Todo el personal que trate datos personales

8.2. Programa de difusión de la protección a los datos personales

Secretaría General			
Identificador único*	SG-16-UNICA-07		
(Nombre del sistema)*	**ACEOC**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría General	
Identificador único*	SG-16-UNICA-07

(Nombre del sistema)*	**ACEOC**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema de tratamiento de datos personales	Actualizar conforme se da el avance tecnológico, las políticas de desarrollo seguro de software y la normatividad en el tratamiento de datos personales del software que aloja el sistema que trata datos personales	Permanente	Total

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría General			
Identificador único*	SG-16-UNICA-07		
(Nombre del sistema)*	**ACEOC**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
ACEOC está alojado en el sistema SG-15-UNICA-06 por lo que en la descripción de ese sistema se indica lo solicitado en este punto. También se encuentra alojado en una nube pública, aquí se aplica lo que el proveedor determine para este punto.			

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría General		
Identificador único*	SG-16-UNICA-07	
(Nombre del sistema)*	**ACEOC**	
Proceso*	**Descripción***	**Responsable***
ACEOC está alojado en el sistema SG-15-UNICA-06 por lo que en la descripción de ese sistema se indica lo solicitado en este punto. También se encuentra alojado en una nube pública, aquí se aplica lo que el proveedor determine para este punto.		

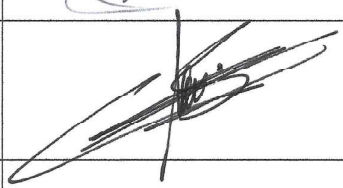
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría General		
Identificador único*	SG-16-UNICA-07	
(Nombre del sistema)*	**ACEOC**	
Proceso*	**Descripción***	**Responsable***
ACEOC está alojado en el sistema SG-15-UNICA-06 por lo que en la descripción de ese sistema se indica lo solicitado en este punto. También se encuentra alojado en una nube pública, aquí se aplica lo que el proveedor determine para este punto.		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsables del desarrollo:	M.A. Víctor Hugo Tovar Pérez Coordinador de Procesos e Información del Consejo Técnico 5556220910 contecfi@unam.mx	
	Esp. María de Guadalupe Flor Díaz de León Fernández de Castro Coordinadora del Sistema de Bibliotecas 5556220865 diazdeleonflor@ingenieria.unam.mx	
	Ing. David Francisco Jiménez Román Jefe del Departamento de Información y Estadística 5556220872 david@ingenieria.unam.mx	
	Ing. Rocío Gabriela Alfaro Vega Jefa del Departamento de Personal Académico y Movilidad Estudiantil 5556220900 gaby@ingenieria.unam.edu	
	Ing. Enrique Barranco Vite Coordinador de la Unidad de Cómputo Académico 5556220951 barranco@ingenieria.unam.edu	
Revisó:	Mtro. Rafael Sandoval Vázquez Jefe de Redes, Seguridad y Servidores, UNICA. 5556220951 rafael@infosec.unam.mx	
Autorizó:	M.I. Gerardo Ruiz Solorio Secretario General 5556220873 grs@unam.mx	
Fecha de aprobación:	22 de agosto de 2022	
Fecha de actualización:	22 de agosto de 2022	

SECRETARÍA ADMINISTRATIVA

ÍNDICE

SECRETARÍA ADMINISTRATIVA

Con el compromiso permanente, con la satisfacción de nuestros usuarios y un esquema de mejora continua de la calidad de los servicios que se proporcionan, se presenta el nuevo sitio Web de la Secretaría Administrativa, sitio a través del cual se busca tener una herramienta de trabajo, de información y de difusión que permita, de una manera dinámica, interactuar entre la Secretaría Administrativa y sus usuarios.

Las Secretaría Administrativa de la Facultad de Ingeniería de la UNAM, está comprometida a proporcionar servicios administrativos de calidad que satisfagan las necesidades y expectativas de nuestros usuarios y partes interesadas, a través del cumplimiento de la normatividad institucional aplicable, el fortalecimiento del liderazgo, la planificación administrativa, el desarrollo de competencias del personal administrativo, el acceso al conocimiento administrativo institucional y la mejora continua de los Procesos del Sistema de Gestión de la Calidad.

Ser una administración ágil y coordinada que brinde un apoyo eficaz y eficiente a las actividades sustantivas de la UNAM, que promueva la calidad de los servicios que presta, simplifique los trámites, disminuya tiempos de respuesta y dé certeza de la transparencia en el ejercicio de los recursos.

La secretaria Administrativa de la Facultad de ingeniería por medio de su Departamento de Sistemas, ha desarrollado una amplia gama de sistemas para coadyuvar a desarrollar las actividades a las diferentes coordinaciones pertenecientes a esta secretaría de manera ágil y amigable.

Dentro de estos sistemas se encuentra 11 desarrollos de software que hacen tratamiento de datos personales que son los siguientes:

Identificador único de sistema	Coordinación/Departamento	Nombre del sistema
SA-01-PA-01	Personal Administrativo	REPEVU
SA-02-SG-01	Servicios Generales	SISEG
SA-03-SG-02	Servicios Generales	SIPEA
SA-04-FN -01	Finanzas	SIBEFI
SA-05-FN -02	Finanzas	SITRAP
SA-06-FN -03	Finanzas	SIEPFI
SA-07-BYS-01	Bienes y Suministros	SIVALE
SA-08-ACPYGC-01	Asignación y Control Presupuestal y Sistema de Gestión de la Calidad	MIR
SA-09-SIS-01	Sistemas	SIST
SA-10-SIS-02	Sistemas	SICAE
SA-11-SIS-03	Sistemas	SICAAFI

Sistema de Registro de Personal Vulnerable REPEVU

Sistema que lleva el control de las solicitudes para el registro de la población vulnerable ante la pandemia de COVID-19

El empleado solicitante llena el formato correspondiente en el que introduce sus datos personales, datos sobre su área de trabajo y sobre su condición de vulnerabilidad, adjuntando información médica que respalde la misma. Lo anterior con la finalidad de justificar su ausencia en actividades presenciales.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-01-PA-01
(Nombre del sistema) *	REPEVU
Datos personales (sensibles o no) contenidos en el sistema*:	Datos Sensibles Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios.
Responsable*:	Ing.Francisco Xavier Jimaréz Rodríguez
Nombre*:	Ing.Francisco Xavier Jimaréz Rodríguez
Cargo*:	Jefe del departamento de sistemas de la secretaría Administrativa
Funciones*:	Administrar, resguardar, manipular las bases de datos donde se alojan los datos personales, así como garantizar el correcto acceso a dichos datos.
Obligaciones*:	-Designa roles de acceso a usuarios del sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargado:
(Nombre del Encargado 1*)	Ing. Marco Antonio Delgado Gonzalez
Cargo*:	Desarrollador en jefe del departamento de sistemas
Funciones*:	-Programar las funciones que el responsable haya aprobado -respaldar las bases de datos que contienen datos personales -garantizar el correcto funcionamiento de los sistemas
Obligaciones*:	Mantener en correcto funcionamiento los sistemas de software de la Secretaría Administrativa, validando su disponibilidad para el uso del personal administrativo, asegurando la integridad de la información que se maneja en los mismos y salvaguardando la confidencialidad de los datos tratados por los sistemas.

	Realizar respaldos de las bases de datos que utilizan los sistemas.
	Usuarios:
(Nombre del Usuario 1*)	Superadministrador
Cargo*:	Funcionario
Funciones*:	Registro de solicitudes: aprobación y/o rechazo
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos.
(Nombre del Usuario 2*)	Usuario de consulta
Cargo*:	Funcionario
Funciones*:	Descargar constancias de solicitudes aprobadas
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos.
(Nombre del Usuario 3*)	Evaluador
Cargo*:	Funcionarios y personal administrativo.
Funciones*:	Revisar las solicitudes: aprueba y/o rechazo de las mismas.
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos.
(Nombre del Usuario 4*)	Usuario general
Cargo*:	Personal académico y personal administrativo.
Funciones*:	Realizar solicitudes
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único¨*	SA-01-PA-01
(Nombre del sistema *)	REPEVU
Tipo de soporte:*	Soporte electrónico
Descripción:*	Base de datos alojada en un servidor local
Características del lugar donde se resguardan los soportes:*	Site de cómputo ubicado en las instalaciones de la Secretaría Administrativa.

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 220 a 222.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

5. PLAN DE TRABAJO

[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-01-PA-01
(Nombre del sistema)*	REPEVU
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza envió físico de información
Transferencias mediante el traslado de soportes electrónicos:	La información enviada no es cifrada antes de ser enviada, pero es cifrada al momento de ser almacenada, con un número de identificación único y un nivel de protección de 128 bits.
Transferencias mediante el traslado sobre redes electrónicas:	-se realiza envío de información a través de internet bajo protocolos seguros

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

a) Solamente tienen acceso a la información las áreas involucradas con la inspección del departamento de sistemas
b) Para soportes físicos: N/A
c) Para soportes electrónicos: Fecha, hora, nombre de usuario, dirección ip y tipo de acción (lectura, escritura, borrado o reasignación).
2. Bitácoras en soporte electrónico

3. Se almacena en un servidor por un año
4. Se respalda semanalmente las bitácoras en conjunto con las bases de datos
5. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas: Personal del Departamento de sistemas, mensualmente o de ser necesario cuando sea requerido

b) Para el caso de que las bitácoras estén en soporte electrónico: No se analizan con herramientas de software .

IV. REGISTRO DE INCIDENTES:

Se realiza levantamiento de un ticket que se entrega inmediatamente después de ser detectado el incidente, que es recibido por el departamento de sistemas de la SA, que consta de:

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen en un servidor del centro de datos y respaldándola en un servidor de soporte.
   c) Para soportes electrónicos: se recuperan todos los campos que decidan las áreas involucradas y de ser el caso un respaldo previo anterior.
2. El registro se encuentra en un medio digital.
3. Se garantiza el resguardo a través de respaldos semanal
4. Para la autorización de la recuperación de datos, los responsables de área deciden.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Se Accesa a las áreas mediante un punto de acceso con lector biométrico de huellas digitales, como primer filtro, para acceder al centro de datos, previa autorización, un responsable del departamento de sistemas contara con las llaves de la cerradura del centro de datos y estará en todo momento en el lugar hasta que se hayan realizado las acciones necesarias. Se cuenta con un sistema CCTV, que vigila la entrada del centro de datos.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaria Administrativa y previa entrevista

b) ¿Cómo las autentifica?
Previa entrevista

c) ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la Secretaria Administrativa.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El centro de datos cuenta con cerraduras y apertura de puerta reducida.
Las llaves de las cerraduras están en manos del departamento de sistemas de la facultad.

1. ¿Cómo las identifica?

Previa autorización de autoridades de la Secretaria Administrativa y previa entrevista

2. ¿Cómo las autentifica?

Previa entrevista

3. ¿Cómo les autoriza el acceso?

Previa autorización de una autoridad de la Secretaria Administrativa.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización está dada previa solicitud del o las áreas involucradas mediante aviso por correo electrónico o en el mismo sistema, la frecuencia dependerá de la administración de la UNAM, no hay periodicidad.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los perfiles y sus respectivas contraseñas están dadas por nomenclatura, basadas en roles y reglas, el departamento de sistemas y el área involucrada decidirán como, cuando y para que se da de alta un usuario o no, se da de baja o se actualiza

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? si
b) ¿Es discrecional (matriz de control de acceso)? si
c) ¿Está basado en roles (perfiles) o grupos? si
d) ¿Está basado en reglas? si

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Si, basado en un esquema de herencia

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si, además de manejo de recursos compartidos en red, como impresoras y directorios

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si con profundidad de 256 bits

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si, basado en herencia

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si, con una profundidad de 256 bits

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Ing. Xavier Jimarez Rodríguez o Ing. Marco Antonio Delgado González

b) ¿Quién autoriza la creación de nuevos perfiles?
Autoridad de le Secretaría administrativa o del área involucrada

c) ¿Se lleva registro de la creación de nuevos perfiles?
Si, en bitácora de base de datos

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
no

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, previo a autorización

c) ¿Cómo se evita el acceso remoto no autorizado?
Bloqueo por medio de firewall, aceeso por certificado ssl.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   - **a)** Completos_x_, diferenciales ___ o incrementales___;
   - **b)** De forma automática __x__ o Manual _____,
   - **c)** Periodicidad con que los realiza: Cada 24 hrs.
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad Respaldo en discos duros
3. Cómo y dónde archiva esos medios,
   Se almacenan en el centro de datos de la secretaría administrativa, dentro de racks.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

El área universitaria se encarga de los respaldos, en específico el departamento de sistemas.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia terminado, está en desarrollo

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-01-PA-01	
(Nombre del sistema)*	REPEVU	
Recurso*	**Descripción***	**Control***
No se cuenta con alguna herramienta de monitoreo		

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-01-PA-01	
(Nombre del sistema)*	REPEVU	
Medida de seguridad*	**Procedimiento***	**Responsable***
No se cuentan con medidas de seguridad en el rubro		

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-01-PA-01	
(Nombre del sistema)*	REPEVU	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No existe información en el rubro		

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-01-PA-01	
(Nombre del sistema)*	REPEVU	
Medida de seguridad*	**Acciones***	**Responsable***
Gestión integral de la seguridad de la información	Comienzar a definir políticas de seguridad, planes y procedimientos para el análisis y gestión de los riesgos en la seguridad de la información.	Ing. Xavier Jimarez Rodriguez Febrero de 2023

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-01-PA-01		
(Nombre del sistema)*	REPEVU		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación en el rubro			

8.2. Programa de difusión de la protección a los datos personales

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-01-PA-01		
(Nombre del sistema)*	REPEVU		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión en el rubro			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-01-PA-01		
(Nombre del sistema)*	REPEVU		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-Revisión mensual del funcionamiento correcto del sistema -Respaldo total del sistema y sus bases de datos	-Se revisa modulo, por modulo por posibles bugs a nivel de desarrollo y a nivel de producción -los respaldos se hacen de manera total mesualmente e incremental anualmente	De 20 a 30 días naturales durante los periodos intersemestrales.	-Se garantiza un acceso correcto a la información -se garantiza el resguardo de datos

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-01-PA-01		
(Nombre del sistema)*	REPEVU		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-mantenimiento preventivo semestral **-**mantenimiento correctivo por evento	-Limpieza de servidores de producción. -Prueba de las líneas de tensión que alimenta a los servidores. -Revisión de cableado estructurado	Un día hábil, el penúltimo día del periodo intersemestral	Evitar sobrecalentamientos en servidores Evitar cortes de energía Evitar cortes o cuelgues de red

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-01-PA-01	
(Nombre del sistema)*	REPEVU	
Proceso*	**Descripción***	**Responsable***
-adquisición de nuevos dispositivos de respaldo -respaldos mensuales	Buscar elementos de almacenamiento como lo son discos duros o nuevas tecnologías. Realizar en tiempo los respaldos necesarios	a) Ing. Xavier Jimarez Rodriguez b) 3 dias habiles

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-01-PA-01	
(Nombre del sistema)*	REPEVU	
Proceso*	**Descripción***	**Responsable***
Proceso basado en el borrado seguro de la circular DGTIC/003/2017	Se puede consultar el procedimiento en la liga: Borrado seguro de información | UNAM-CERT	a) Ing. Xavier Jimarez Rodriguez b) 3 dias habiles

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un protocolo o plan de acción para la cancelación, baja o destrucción de un sistema de tratamiento de datos personales.

Sistema de Servicios Generales SISEG

Sistema que lleva el control de las solicitudes para la realización de servicios generales dentro de la Facultad de Ingeniería.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-02-SG-01
(Nombre del sistema) *	SISEG
Datos personales (sensibles o no) contenidos en el sistema*:	Datos Sensibles Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios.
Responsable*:	Ing.Francisco Xavier Jimaréz Rodríguez
Nombre*:	Ing.Francisco Xavier Jimaréz Rodríguez
Cargo*:	Jefe del departamento de sistemas de la secretaría Administrativa
Funciones*:	Administrar, resguardar, manipular las bases de datos donde se alojan los datos personales, así como garantizar el correcto acceso a dichos datos.
Obligaciones*:	-Designa roles de acceso a usuarios del sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Ing. Marco Antonio Delgado Gonzalez
Cargo*:	Desarrollador en jefe del departamento de sistemas
Funciones*:	-Programar las funciones que el responsable haya aprobado -respaldar las bases de datos que contienen datos personales -garantizar el correcto funcionamiento de los sistemas
Obligaciones*:	Mantener en correcto funcionamiento los sistemas de software de la Secretaría Administrativa, validando su disponibilidad para el uso del personal administrativo, asegurando la integridad de la información que se maneja en los mismos y salvaguardando la confidencialidad de los datos tratados por los sistemas. Realizar respaldos de las bases de datos que utilizan los sistemas.
	Usuarios:

(Nombre del Usuario 1*)	Administrador
Cargo*:	Funcionario
Funciones*:	Registrar solicitudes, aprobarlas, rechazarlas y/o descargar constancias
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos.
(Nombre del Usuario 2*)	Jefe de Unidad
Cargo*:	Funcionarios y personal administrativo
Funciones*:	Aprobar las solicitudes del área correspondiente.
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos.
(Nombre del Usuario 3*)	Jefe de taller
Cargo*:	Funcionarios y personal administrativo
Funciones*:	Coordinar las solicitudes
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos.
(Nombre del Usuario 4*)	Usuario general
Cargo*:	Personal académico y personal administrativo.
Funciones*:	Realizar solicitudes de servicios
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-02-SG-01
(Nombre del sistema *)	SISEG
Tipo de soporte:*	Soporte electrónico
Descripción:*	Base de datos alojada en un servidor local.
Características del lugar donde se resguardan los soportes:*	Site de cómputo ubicado en las instalaciones de la Secretaría Administrativa.

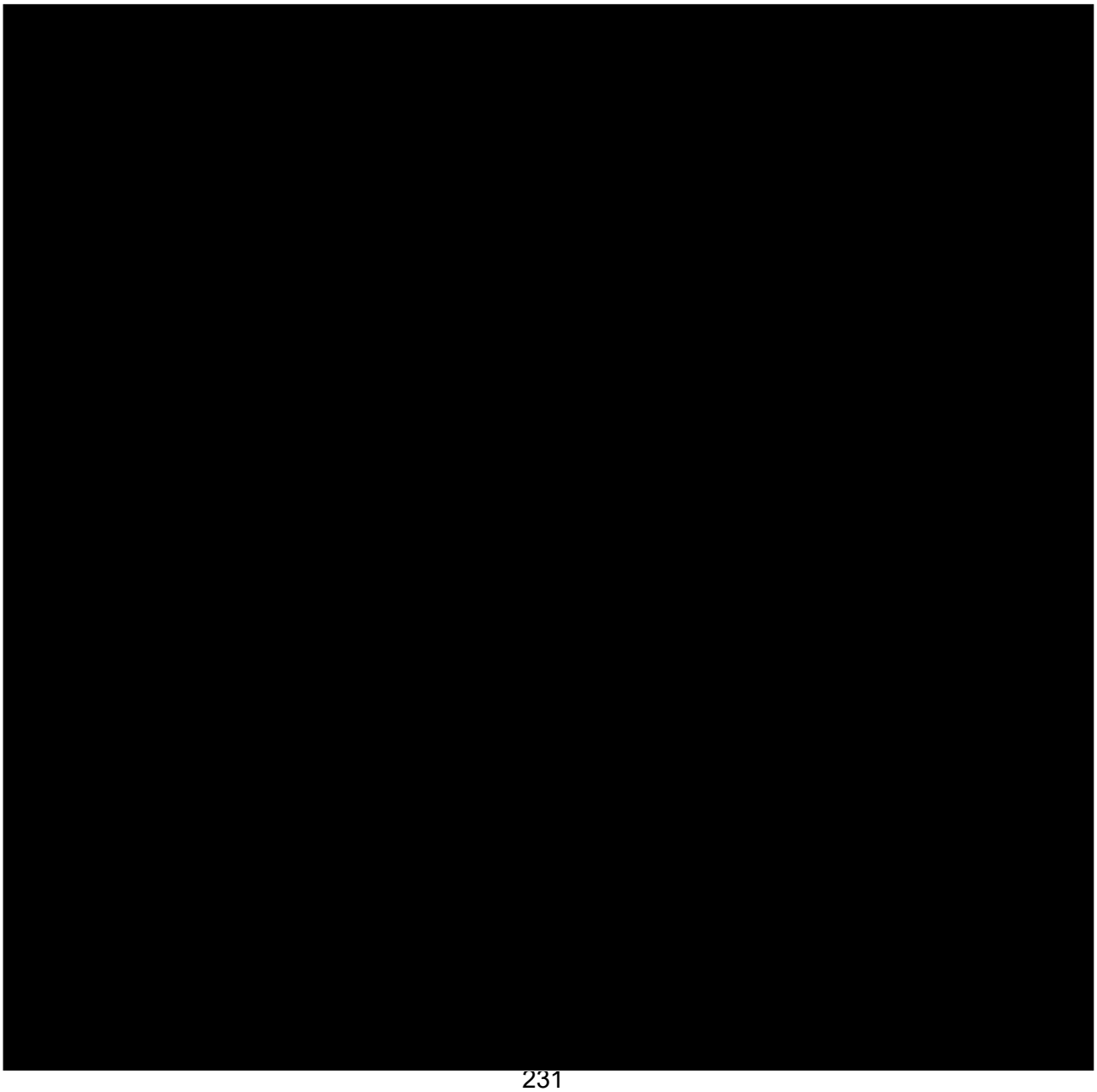
3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 230 a 232.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO



[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-02-SG-01
(Nombre del sistema)*	SISEG
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza envió físico de información
Transferencias mediante el traslado de soportes electrónicos:	La información enviada no es cifrada antes de de ser enviada, pero es cifrada al momento de ser almacenada, con un número de identificación único y un nivel de protección de 128 bits
Transferencias mediante el traslado sobre redes electrónicas:	-se realiza envío de información a través de internet bajo protocolos seguros

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

- **a)** Solamente tienen acceso a la información las áreas involucradas con la inspección del departamento de sistemas
- **b)** Para soportes físicos: N/A
- **c)** Para soportes electrónicos: Fecha, hora, nombre de usuario, dirección ip y tipo de acción (lectura, escritura, borrado o reasignación).

2. Bitácoras en soporte electrónico

3. Se almacena en un servidor por un año
4. Se respalda semanalmente las bitácoras en conjunto con las bases de datos
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas: Personal del Departamento de sistemas, mensualmente o de ser necesario cuando sea requerido
   b) Para el caso de que las bitácoras estén en soporte electrónico: No se analizan con herramientas de software.

IV. REGISTRO DE INCIDENTES:

Se realiza levantamiento de un ticket que se entrega inmediatamente después de ser detectado el incidente, que es recibido por el departamento de sistemas de la SA, que consta de:

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen en un servidor del centro de datos y respaldándola en un servidor de soporte.
   c) Para soportes electrónicos: se recuperan todos los campos que decidan las áreas involucradas y de ser el caso un respaldo previo anterior.
2. El registro se encuentra en un medio digital.
3. Se garantiza el resguardo a través de respaldos semanal
4. Para la autorización de la recuperación de datos, los responsables de área deciden.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Se Accesa a las áreas mediante un punto de acceso con lector biométrico de huellas digitales, como primer filtro, para acceder al centro de datos, previa autorización, un responsable del departamento de sistemas contara con las llaves de la cerradura del centro de datos y estará en todo momento en el lugar hasta que se hayan realizado las acciones necesarias. Se cuenta con un sistema CCTV, que vigila la entrada del centro de datos.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
   Previa autorización de autoridades de la Secretaria Administrativa y previa entrevista
b) ¿Cómo las autentifica?
   Previa entrevista
c) ¿Cómo les autoriza el acceso?
   Previa autorización de una autoridad de la secretaria administrativa.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El centro de datos cuenta con cerraduras y apertura de puerta reducida.

Las llaves de las cerraduras están en manos de el departamento de sistemas de la facultad.

1. ¿Cómo las identifica?
   Previa autorización de autoridades de la Secretaria Administrativa y previa entrevista
2. ¿Cómo las autentifica?
   Previa entrevista
3. ¿Cómo les autoriza el acceso?
   Previa autorización de una autoridad de la secretaria administrativa.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización está dada previa solicitud del o las áreas involucradas mediante aviso por correo electrónico o en el mismo sistema, la frecuencia dependerá de la administración de la UNAM, no hay periodicidad

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los perfiles y sus respectivas contraseñas están dadas por nomenclatura, basadas en roles y reglas, el departamento de sistemas y el área involucrada decidirán como, cuando y para que se da de alta un usuario o no, se da de baja o se actualiza

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? si
- **b)** ¿Es discrecional (matriz de control de acceso)? si
- **c)** ¿Está basado en roles (perfiles) o grupos? si
- **d)** ¿Está basado en reglas? Si

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  Si, basado en un esquema de herencia
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  Si, además de manejo de recursos compartidos en red.
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Si con profundidad de 256 bits

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
  Si, basado en herencia
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

Si, con una profundidad de 256 bits

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Ing. Xavier Jimarez Rodríguez o Ing. Marco Antonio Delgado González

b) ¿Quién autoriza la creación de nuevos perfiles?
Autoridad de le Secretaría administrativa o del área involucrada

c) ¿Se lleva registro de la creación de nuevos perfiles?
Si, en bitácora de base de datos

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
no

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, previo a autorización

c) ¿Cómo se evita el acceso remoto no autorizado?
Bloqueo por medio de firewall, aceeso por certificado ssl.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_x_, diferenciales ___ o incrementales___;
   b) De forma automática __x__ o Manual _____,
   c) Periodicidad con que los realiza: Cada 24 hrs.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad
Respaldo en discos duros

3. Cómo y dónde archiva esos medios,
Se almacenan en el centro de datos de la secretaría administrativa, dentro de racks.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

El área universitaria se encarga de los respaldos, en específico el departamento de sistemas.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia terminado, está en desarrollo

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-02-SG-01

(Nombre del sistema)*	SISEG	
Recurso*	**Descripción***	**Control***
No se cuenta con alguna herramienta de monitoreo		

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-02-SG-01	
(Nombre del sistema)*	SISEG	
Medida de seguridad*	**Procedimiento***	**Responsable***
No se cuentan con medidas de seguridad en el rubro		

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-02-SG-01	
(Nombre del sistema)*	SISEG	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No existe información en el rubro		

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-02-SG-01	
(Nombre del sistema)*	SISEG	
Medida de seguridad*	**Acciones***	**Responsable***
Gestión integral de la seguridad de la información	Comenzar a definir políticas de seguridad, planes y procedimientos para el análisis y gestión de los riesgos en la seguridad de la información.	Ing. Xavier Jimarez Rodríguez Febrero de 2023

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-02-SG-01		
(Nombre del sistema)*	SISEG		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación en el rubro			

8.2 Programa de difusión de la protección a los datos personales

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-02-SG-01		
(Nombre del sistema)*	SISEG		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión en el rubro			

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-02-SG-01		
(Nombre del sistema)*	SISEG		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-Revisión mensual del funcionamiento correcto del sistema -Respaldo total del sistema y sus bases de datos	-Se revisa modulo, por modulo por posibles bugs a nivel de desarrollo y a nivel de producción -los respaldos se hacen de manera total mesualmente e incremental anualmente	De 20 a 30 días naturales durante los periodos intersemestrales.	-Se garantiza un acceso correcto a la información -se garantiza el resguardo de datos

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-02-SG-01		
(Nombre del sistema)*	**SISEG**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-mantenimiento preventivo semestral -mantenimiento correctivo por evento	-Limpieza de servidores de producción. -Prueba de las líneas de tensión que alimenta a los servidores. -Revisión de cableado estructurado	Un día hábil, el penúltimo día del periodo intersemestral	Evitar sobrecalentamientos en servidores Evitar cortes de energía Evitar cortes o cuelgues de red

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-02-SG-01	
(Nombre del sistema)*	SISEG	
Proceso*	**Descripción***	**Responsable***
-adquisición de nuevos dispositivos de respaldo -respaldos mensuales	Buscar elementos de almacenamiento como lo son discos duros o nuevas tecnologías. Realizar en tiempo los respaldos necesarios	a) Ing. Xavier Jimarez Rodriguez b) 3 dias habiles

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-02-SG-01	
(Nombre del sistema)*	SISEG	
Proceso*	**Descripción***	**Responsable***
Proceso basado en el borrado seguro de la circular DGTIC/003/2017	Se puede consultar el procedimiento en la liga: Borrado seguro de información | UNAM-CERT	a) Ing. Xavier Jimarez Rodriguez b) 3 dias habiles

10 PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un protocolo o plan de acción para la cancelación, baja o destrucción de un sistema de tratamiento de datos personales.

Sistema de Préstamo de Equipo Audiovisual SIPEA

Sistema que ayuda a el préstamo de equipo audiovisual, inventario de fotocopiado, engargolado, así como las estadísticas de dichos préstamos a personal académico de la facultad.

Se cuenta con una versión web y una versión de escritorio

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-03-SG-02
(Nombre del sistema) *	SIPEA
Datos personales (sensibles o no) contenidos en el sistema*:	Datos Sensibles Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios.
Responsable*:	Ing.Francisco Xavier Jimaréz Rodríguez
Nombre*:	Ing.Francisco Xavier Jimaréz Rodríguez
Cargo*:	Jefe del departamento de sistemas de la secretaría Administrativa
Funciones*:	Administrar, resguardar, manipular las bases de datos donde se alojan los datos personales, así como garantizar el correcto acceso a dichos datos.
Obligaciones*:	-Designa roles de acceso a usuarios del sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Ing. Marco Antonio Delgado Gonzalez
Cargo*:	Desarrollador en jefe del departamento de sistemas
Funciones*:	-Programar las funciones que el responsable haya aprobado -respaldar las bases de datos que contienen datos personales -garantizar el correcto funcionamiento de los sistemas
Obligaciones*:	Mantener en correcto funcionamiento los sistemas de software de la Secretaría Administrativa, validando su disponibilidad para el uso del personal administrativo, asegurando la integridad de la información que se maneja en los mismos y salvaguardando la confidencialidad de los datos tratados por los sistemas.

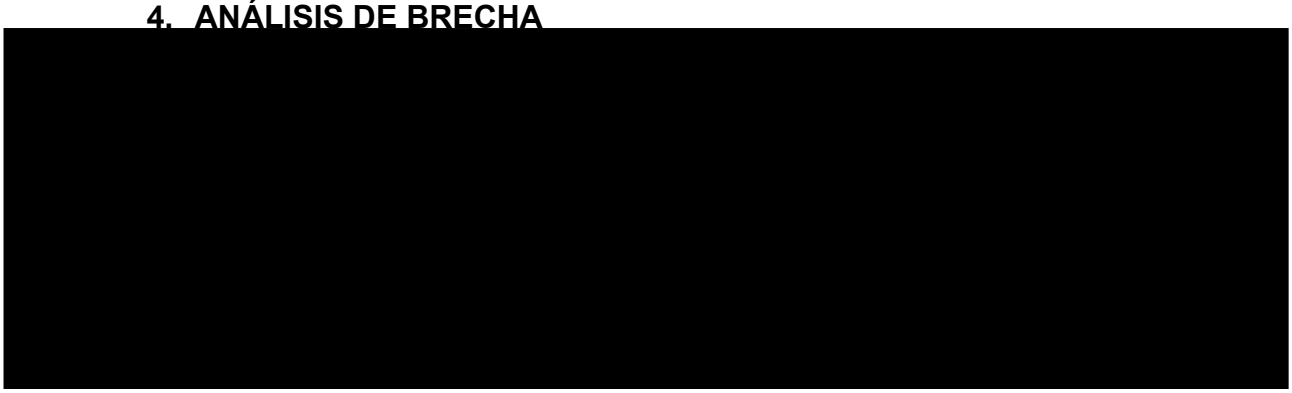
	Realizar respaldos de las bases de datos que utilizan los sistemas.
	Usuarios:
(Nombre del Usuario 1*)	Administrador
Cargo*:	Funcionario jefe de departamento
Funciones*:	Generar reportes y consultar el histórico de servicios.
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos.
(Nombre del Usuario 2*)	Usuario general
Cargo*:	Personal administrativo
Funciones*:	Realizar préstamos y proporcionar servicios ofrecidos por el departamento de Audiovisual.
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único¨*	SA-03-SG-02
(Nombre del sistema *)	SIPEA
Tipo de soporte:*	Soporte electrónico
Descripción:*	Base de datos alojada en un servidor local.
Características del lugar donde se resguardan los soportes:*	Site de cómputo ubicado en las instalaciones de la Secretaría Administrativa.

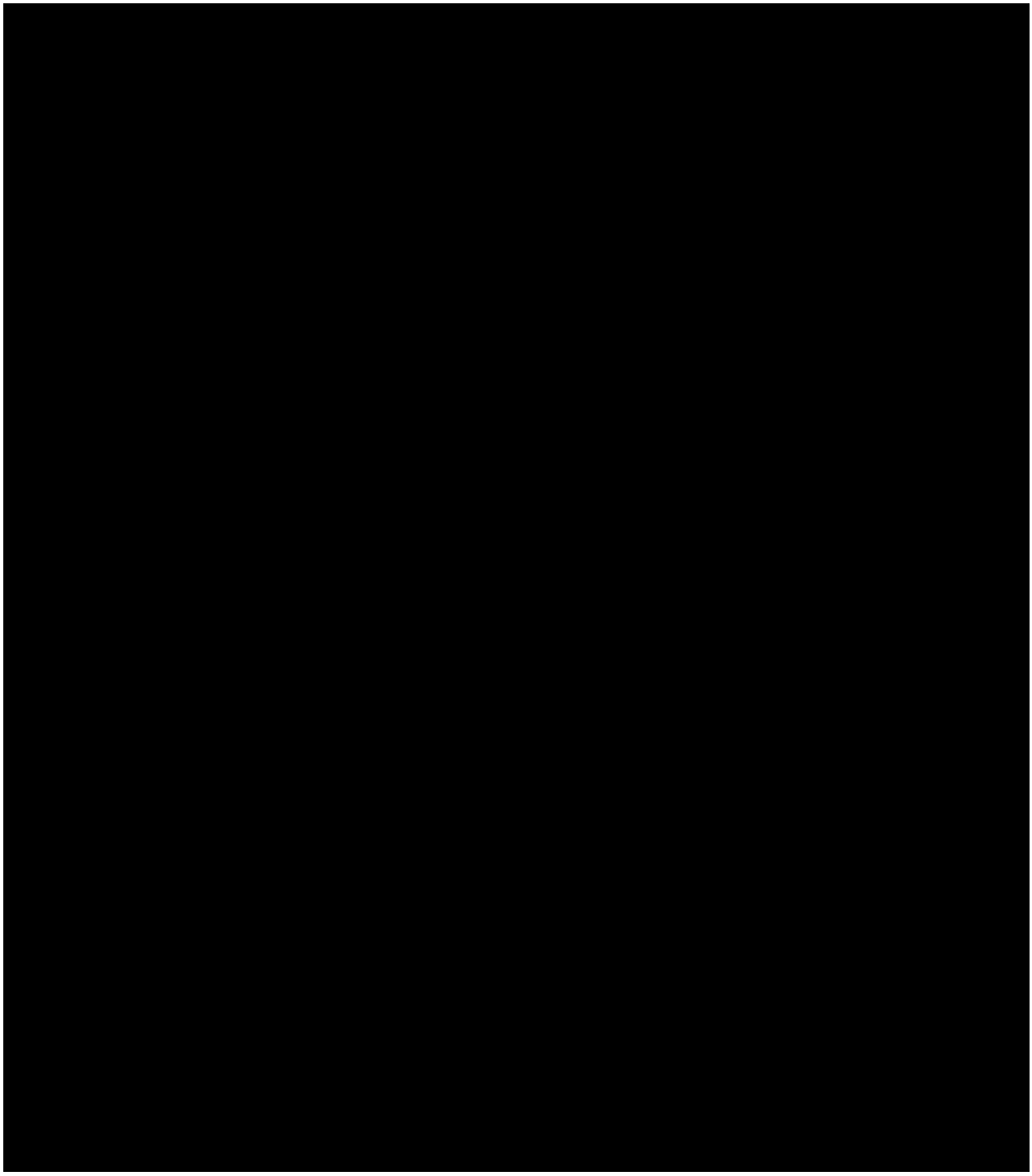
3. ANÁLISIS DE RIESGOS

4. ANÁLISIS DE BRECHA



Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 240 a 241.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-03-SG-02
(Nombre del sistema)*	SIPEA
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza envió físico de información
Transferencias mediante el traslado de soportes electrónicos:	La información enviada no es cifrada antes de ser enviada, pero es cifrada al momento de ser almacenada, con un número de identificación único y un nivel de protección de 128 bits
Transferencias mediante el traslado sobre redes electrónicas:	Se realiza envío de información a través de internet bajo protocolos seguros.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

a) Solamente tienen acceso a la información las áreas involucradas con la inspección del departamento de sistemas
b) Para soportes físicos: N/A
c) Para soportes electrónicos: Fecha, hora, nombre de usuario, dirección ip y tipo de acción (lectura, escritura, borrado o reasignación).

2. Bitácoras en soporte electrónico
3. Se almacena en un servidor por un año
4. Se respalda semanalmente las bitácoras en conjunto con las bases de datos
5. Respecto del análisis de las bitácoras:
    a) Quién es el responsable de analizarlas: Personal del Departamento de sistemas, mensualmente o de ser necesario cuando sea requerido
    b) Para el caso de que las bitácoras estén en soporte electrónico: No se analizan con herramientas de software.

IV. REGISTRO DE INCIDENTES:

Se realiza levantamiento de un ticket que se entrega inmediatamente después de ser detectado

el incidente, que es recibido por el departamento de sistemas de la SA, que consta de:

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen en un servidor del centro de datos y respaldándola en un servidor de soporte.
   c) Para soportes electrónicos: se recuperan todos los campos que decidan las áreas involucradas y de ser el caso un respaldo previo anterior.
2. El registro se encuentra en un medio digital.
3. Se garantiza el resguardo a través de respaldos semanal
4. Para la autorización de la recuperación de datos, los responsables de área decide.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Se Accesa a las áreas mediante un punto de acceso con lector biométrico de huellas digitales, como primer filtro, para acceder al centro de datos, previa autorización, un responsable del departamento de sistemas contara con las llaves de la cerradura del centro de datos y estará en todo momento en el lugar hasta que se hayan realizado las acciones necesarias. Se cuenta con un sistema CCTV, que vigila la entrada del centro de datos.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaria Administrativa y previa entrevista

b) ¿Cómo las autentifica?
Previa entrevista

c) ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la Secretaria Administrativa.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El centro de datos cuenta con cerraduras y apertura limitada.
Las llaves de las cerraduras están en manos de el departamento de sistemas de la facultad.

1. ¿Cómo las identifica?
   Previa autorización de autoridades de la Secretaria Administrativa y previa entrevista
2. ¿Cómo las autentifica?
   Previa entrevista
3. ¿Cómo les autoriza el acceso?
   Previa autorización de una autoridad de la secretaria administrativa.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización está dada previa solicitud del o las áreas involucradas mediante aviso por correo electrónico o en el mismo sistema, la frecuencia dependerá de la administración de la UNAM, no hay periodicidad

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los perfiles y sus respectivas contraseñas están dadas por nomenclatura, basadas en roles y reglas, el departamento de sistemas y el área involucrada decidirán como, cuando y para que se da de alta un usuario o no, se da de baja o se actualiza

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? si
- **b)** ¿Es discrecional (matriz de control de acceso)? si
- **c)** ¿Está basado en roles (perfiles) o grupos? si
- **d)** ¿Está basado en reglas? si

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  Si, basado en un esquema de herencia
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  Si, además de manejo de recursos compartidos en red.
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Si con profundidad de 256 bits

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
  Si, basado en herencia
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Si, con una profundidad de 256 bits

4. Administración de perfiles de usuario y contraseñas:

- **a)** ¿Quién da de alta nuevos perfiles?
  Ing. Xavier Jimarez Rodríguez o Ing. Marco Antonio Delgado González
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
  Autoridad de le Secretaría administrativa o del área involucrada
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?
  Si, en bitácora de base de datos

5. Acceso remoto al sistema de tratamiento de datos personales:

- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
  no

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, previo a autorización

c) ¿Cómo se evita el acceso remoto no autorizado?
Bloqueo por medio de firewall, aceeso por certificado ssl.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos_x_, diferenciales ___ o incrementales___;

b) De forma automática __x__ o Manual _____,

c) Periodicidad con que los realiza: Cada 24 hrs.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad Respaldo en discos duros
3. Cómo y dónde archiva esos medios,

Se almacenan en el centro de datos de la secretaría administrativa, dentro de racks.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

El área universitaria se encarga de los respaldos, en específico el departamento de sistemas.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia terminado, está en desarrollo

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-03-SG-02	
(Nombre del sistema)*	SIPEA	
Recurso*	**Descripción***	**Control***
No se cuenta con alguna herramienta de monitoreo		

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-02-SG-02	
(Nombre del sistema)*	SIPEA	
Medida de seguridad*	**Procedimiento***	**Responsable***
No se cuentan con medidas de seguridad en el rubro		

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-03-SG-02	
(Nombre del sistema)*	SIPEA	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No existe información en el rubro		

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-03-SG-02	
(Nombre del sistema)*	**SIPEA**	
Medida de seguridad*	**Acciones***	**Responsable***
Gestión integral de la seguridad de la información	Comienzar a definir políticas de seguridad, planes y procedimientos para el análisis y gestión de los riesgos en la seguridad de la información.	Ing. Xavier Jimarez Rodriguez Febrero de 2023

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-03-SG-02		
(Nombre del sistema)*	SIPEA		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación en el rubro			

8.2 Programa de difusión de la protección a los datos personales

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-03-SG-02		
(Nombre del sistema)*	SIPEA		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión en el rubro			

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-03-SG-02
(Nombre del sistema)*	SIPEA

Actividad*	Descripción*	Duración*	Cobertura*
-Revisión mensual del funcionamiento correcto del sistema -Respaldo total del sistema y sus bases de datos	-Se revisa modulo, por modulo por posibles bugs a nivel de desarrollo y a nivel de producción -los respaldos se hacen de manera total mesualmente e incremental anualmente	De 20 a 30 días naturales durante los periodos intersemestrales.	-Se garantiza un acceso correcto a la información -se garantiza el resguardo de datos

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-03-SG-02		
(Nombre del sistema)*	SIPEA		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-mantenimiento preventivo semestral -mantenimiento correctivo por evento	-Limpieza de servidores de producción. -Prueba de las líneas de tensión que alimenta a los servidores. -Revisión de cableado estructurado	Un día hábil, el penúltimo día del periodo intersemestral	Evitar sobrecalentamientos en servidores Evitar cortes de energía Evitar cortes o cuelgues de red

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-03-SG-02	
(Nombre del sistema)*	SIPEA	
Proceso*	**Descripción***	**Responsable***
-adquisición de nuevos dispositivos de respaldo -respaldos mensuales	Buscar elementos de almacenamiento como lo son discos duros o nuevas tecnologías. Realizar en tiempo los respaldos necesarios	a) Ing. Xavier Jimarez Rodriguez b) 3 días hábiles

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-03-SG-02
(Nombre del sistema)*	SIPEA

Proceso*	Descripción*	Responsable*
Proceso basado en el borrado seguro de la circular DGTIC/003/2017	Se puede consultar el procedimiento en la liga: Borrado seguro de información | UNAM-CERT	a) Ing. Xavier Jimarez Rodriguez b) 3 días hábiles

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un protocolo o plan de acción para la cancelación, baja o destrucción de un sistema de tratamiento de datos personales.

Sistema de Becas de la Facultad de Ingeniería SIBEFI

Sistema que lleva el control de las solicitudes de beca que realiza el alumnado.

El alumno se registra en el sistema con el fin de obtener un perfil para realizar solicitudes de beca.

El alumno realiza la solicitud de beca llenando el formulario correspondiente y adjuntando los documentos requeridos, con lo cual se le asigna un folio a su solicitud.

Esta solicitud es evaluada por el Departamento de Operación Administrativa y, de ser correcta toda la información, se aprueba la solicitud.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-04-FN-01
(Nombre del sistema) *	SIBEFI
Datos personales (sensibles o no) contenidos en el sistema*:	Datos Sensibles Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios.
Responsable*:	Ing.Francisco Xavier Jimaréz Rodríguez
Nombre*:	Ing.Francisco Xavier Jimaréz Rodríguez
Cargo*:	Jefe del departamento de sistemas de la secretaría Administrativa
Funciones*:	Administrar, resguardar, manipular las bases de datos donde se alojan los datos personales, así como garantizar el correcto acceso a dichos datos.
Obligaciones*:	-Designa roles de acceso a usuarios del sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Ing. Marco Antonio Delgado Gonzalez
Cargo*:	Desarrolador en jefe del departamento de sistemas
Funciones*:	-Programar las funciones que el responsable haya aprobado -respaldar las bases de datos que contienen datos personales -garantizar el correcto funcionamiento de los sistemas
Obligaciones*:	Mantener en correcto funcionamiento los sistemas de software de la Secretaría Administrativa, validando su disponibilidad para el uso del personal administrativo, asegurando la integridad de la información que se maneja

	en los mismos y salvaguardando la confidencialidad de los datos tratados por los sistemas. Realizar respaldos de las bases de datos que utilizan los sistemas.
	Usuarios:
(Nombre del Usuario 1*)	Superadministrador
Cargo*:	Funcionarios, personal académico y personal administrativo
Funciones*:	Registrar solicitudes, aprobarlas, rechazarlas y descargar documentos. Dar de alta administradores y asignarles permisos dentro del sistema.
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos.
(Nombre del Usuario 2*)	Usuario de consulta
Cargo*:	Personal académico y personal administrativo.
Funciones*:	Coordinar solicitudes de beca de los proyectos que le son asignados.
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos.
(Nombre del Usuario 3*)	Evaluador
Cargo*:	Personal administrativo.
Funciones*:	Revisar solicitudes realizadas por los usuarios.
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos.
(Nombre del Usuario 4*)	Usuario general
Cargo*:	Becario
Funciones*:	Realizar solicitudes de beca.
Obligaciones*:	Resguardar los datos personales y usarlos para los fines establecidos

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único¨*	SA-04-FN-01
(Nombre del sistema *)	SIBEFI
Tipo de soporte:*	Soporte electrónico
Descripción:*	Base de datos alojada en un servidor local.
Características del lugar donde se resguardan los soportes:*	Site de cómputo ubicado en las instalaciones de la Secretaría Administrativa.

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las paginas 250 a 252.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-04-FN-01
(Nombre del sistema)*	SIBEFI
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza envió físico de información
Transferencias mediante el traslado de soportes electrónicos:	La información enviada no es cifrada antes de ser enviada, pero es cifrada al momento de ser almacenada, con un número de identificación único y un nivel de protección de 128 bits
Transferencias mediante el traslado sobre redes electrónicas:	-se realiza envío de información a través de internet bajo protocolos seguros

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**

   a) Solamente tienen acceso a la información las áreas involucradas con la inspección del departamento de sistemas
   b) Para soportes físicos: N/A
   c) Para soportes electrónicos: Fecha, hora, nombre de usuario, dirección ip y tipo de acción (lectura, escritura, borrado o reasignación).
2. Bitácoras en soporte electrónico
3. Se almacena en un servidor por un año
4. Se respalda semanalmente las bitácoras en conjunto con las bases de datos
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas: Personal del Departamento de sistemas, mensualmente o de ser necesario cuando sea requerido
   b) Para el caso de que las bitácoras estén en soporte electrónico: No se analizan con herramientas de software.

IV. REGISTRO DE INCIDENTES:

Se realiza levantamiento de un ticket que se entrega inmediatamente después de ser detectado el incidente, que es recibido por el departamento de sistemas de la SA, que consta de:

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen en un servidor del centro de datos y respaldándola en un servidor de soporte.
   c) Para soportes electrónicos: se recuperan todos los campos que decidan las áreas involucradas y de ser el caso un respaldo previo anterior.
2. El registro se encuentra en un medio digital.
3. Se garantiza el resguardo a través de respaldos semanal
4. Para la autorización de la recuperación de datos, los responsables de área deciden.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Se Accesa a las áreas mediante un punto de acceso con lector biométrico de huellas digitales, como primer filtro, para acceder al centro de datos, previa autorización, un responsable del departamento de sistemas contara con las llaves de la cerradura del centro de datos y estará en todo momento en el lugar hasta que se hayan realizado las acciones necesarias. Se cuenta con un sistema CCTV, que vigila la entrada del centro de datos.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista

b) ¿Cómo las autentifica?
Previa entrevista

c) ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la secretaria administrativa.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El centro de datos cuenta con cerraduras y puerta de acceso limitado.
Las llaves de las cerraduras están en manos del departamento de sistemas de la facultad.

1. ¿Cómo las identifica?
   Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista
2. ¿Cómo las autentifica?
   Previa entrevista
3. ¿Cómo les autoriza el acceso?
   Previa autorización de una autoridad de la Secretaría Administrativa.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización está dada previa solicitud del o las áreas involucradas mediante aviso por correo electrónico o en el mismo sistema, la frecuencia dependerá de la administración de la UNAM, no hay periodicidad

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los perfiles y sus respectivas contraseñas están dadas por nomenclatura, basadas en roles y reglas, el departamento de sistemas y el área involucrada decidirán como, cuando y para que se da de alta un usuario o no, se da de baja o se actualiza

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? si
b) ¿Es discrecional (matriz de control de acceso)? si
c) ¿Está basado en roles (perfiles) o grupos? si
d) ¿Está basado en reglas? si

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Si, basado en un esquema de herencia

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si, además de manejo de recursos compartidos en red, como impresoras y directorios

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si, con profundidad de 256 bits

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?

Si, basado en herencia

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si, con una profundidad de 256 bits

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Ing. Xavier Jimarez Rodríguez o Ing. Marco Antonio Delgado González

b) ¿Quién autoriza la creación de nuevos perfiles?
Autoridad de le Secretaría administrativa o del área involucrada

c) ¿Se lleva registro de la creación de nuevos perfiles?
Si, en bitácora de base de datos

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
no

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, previo a autorización

c) ¿Cómo se evita el acceso remoto no autorizado?
Bloqueo por medio de firewall, aceeso por certificado ssl.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos_x_, diferenciales ___ o incrementales___;

b) De forma automática __x__ o Manual _____,

c) Periodicidad con que los realiza: Cada 24 hrs.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad
Respaldo en discos duros

3. Cómo y dónde archiva esos medios,
Se almacenan en el centro de datos de la secretaría administrativa, dentro de racks.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
El área universitaria se encarga de los respaldos, en específico el departamento de sistemas.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia terminado, está en desarrollo

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-04-FN-01	
(Nombre del sistema)*	SIBEFI	
Recurso*	**Descripción***	**Control***
No se cuenta con alguna herramienta de monitoreo		

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-04-FN-01	
(Nombre del sistema)*	SIBEFI	
Medida de seguridad*	**Procedimiento***	**Responsable***
No se cuentan con medidas de seguridad en el rubro		

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-04-FN-01	
(Nombre del sistema)*	SIBEFI	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No existe información en el rubro		

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-04-FN-01	
(Nombre del sistema)*	SIBEFI	
Medida de seguridad*	**Acciones***	**Responsable***
Gestión integral de la seguridad de la información	Comenzar a definir políticas de seguridad, planes y procedimientos para el análisis y gestión de los riesgos en la seguridad de la información.	Ing. Xavier Jimarez Rodriguez Febrero de 2023

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-04-FN-01

(Nombre del sistema)*	SIBEFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación en el rubro			

8.2 Programa de difusión de la protección a los datos personales

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-04-FN-01		
(Nombre del sistema)*	SIBEFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión en el rubro			

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-04-FN-01		
(Nombre del sistema)*	SIBEFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-Revisión mensual del funcionamiento correcto del sistema -Respaldo total del sistema y sus bases de datos	-Se revisa modulo, por modulo por posibles bugs a nivel de desarrollo y a nivel de producción -los respaldos se hacen de manera total mensualmente e incremental anualmente	De 20 a 30 días naturales durante los periodos intersemestrales.	-Se garantiza un acceso correcto a la información -se garantiza el resguardo de datos

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-04-FN-01		
(Nombre del sistema)*	SIBEFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-mantenimiento preventivo semestral -mantenimiento correctivo por evento	-Limpieza de servidores de producción. -Prueba de las líneas de tensión	Un día hábil, el penúltimo día del periodo intersemestral	Evitar sobrecalentamientos en servidores Evitar cortes de energía

	que alimenta a los servidores. -Revisión de cableado estructurado		Evitar cortes o cuelgues de red

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-04-FN-01	
(Nombre del sistema)*	SIBEFI	
Proceso*	**Descripción***	**Responsable***
-adquisición de nuevos dispositivos de respaldo -respaldos mensuales	Buscar elementos de almacenamiento como lo son discos duros o nuevas tecnologías. Realizar en tiempo los respaldos necesarios	a) Ing. Xavier Jimarez Rodriguez b) 3 días hábiles

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-04-FN-01	
(Nombre del sistema)*	SIBEFI	
Proceso*	**Descripción***	**Responsable***
Proceso basado en el borrado seguro de la circular DGTIC/003/2017	Se puede consultar el procedimiento en la liga: Borrado seguro de información | UNAM-CERT	a) Ing. Xavier Jimarez Rodriguez b) 3 días hábiles

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un protocolo o plan de acción para la cancelación, baja o destrucción de un sistema de tratamiento de datos personales.

Sistema de Trámites de Presupuesto SITRAP

El Sistema de Trámites de Presupuesto es un sistema en el que se pueden realizar solicitudes para viáticos, gastos de trabajo de campo o gastos de intercambio por parte de los académicos. Este sistema fue desarrollado para la Coordinación de Procesos Administrativos perteneciente al departamento de Finanzas, los cuales pueden gestionar las solicitudes y realizar las correspondientes aprobaciones o cancelaciones de estas. Las solicitudes, una vez aprobadas, se ingresan a ventanilla, se procesan fuera del sistema y, una vez el cheque llega a la facultad, se le informa al usuario la disponibilidad de este y se registra la entrega correspondiente. Para la administración es posible generar reportes y consultar el histórico de tramites registrados.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-05-FN-02
(Nombre del sistema) *	SITRAP
Datos personales (sensibles o no) contenidos en el sistema*:	Datos Sensibles Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios.
Responsable*:	Ing.Francisco Xavier Jimaréz Rodríguez
Nombre*:	Ing.Francisco Xavier Jimaréz Rodríguez
Cargo*:	Jefe del departamento de sistemas de la secretaría Administrativa
Funciones*:	Administrar, resguardar, manipular las bases de datos donde se alojan los datos personales, así como garantizar el correcto acceso a dichos datos.
Obligaciones*:	-Designa roles de acceso a usuarios del sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Ing. Marco Antonio Delgado Gonzalez
Cargo*:	Desarrollador en jefe del departamento de sistemas
Funciones*:	-Programar las funciones que el responsable haya aprobado -respaldar las bases de datos que contienen datos personales -garantizar el correcto funcionamiento de los sistemas
Obligaciones*:	Mantener en correcto funcionamiento los sistemas de

	software de la Secretaría Administrativa, validando su disponibilidad para el uso del personal administrativo, asegurando la integridad de la información que se maneja en los mismos y salvaguardando la confidencialidad de los datos tratados por los sistemas. Realizar respaldos de las bases de datos que utilizan los sistemas.
	Usuarios:
(Nombre del Usuario 1*)	Administrador
Cargo*:	Funcionarios
Funciones*:	Registrar, aprobar o rechazar solicitudes. Descargar documentos y reportes. Consultar el estatus del trámite.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 2*)	Prácticas Escolares
Cargo*:	Funcionarios y personal administrativo
Funciones*:	Realizar solicitudes.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 3*)	Ventanilla
Cargo*:	Personal administrativo
Funciones*:	Consultar estatus de trámites
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 4*)	Usuario general
Cargo*:	Personal académico y personal administrativo
Funciones*:	Realizar solicitudes.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único¨*	SA-05-FN-02
(Nombre del sistema *)	SITRAP
Tipo de soporte:*	Soporte electrónico
Descripción:*	Base de datos alojada en un servidor local.
Características del lugar donde se resguardan los soportes:*	Site de cómputo ubicado en las instalaciones de la Secretaría Administrativa.

3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

5. PLAN DE TRABAJO

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 261 a 262.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-05-FN-02
(Nombre del sistema)*	SITRAP
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza envió físico de información
Transferencias mediante el traslado de soportes electrónicos:	La información enviada no es cifrada antes de ser enviada, pero es cifrada al momento de ser almacenada, con un número de identificación único y un nivel de protección de 128 bits
Transferencias mediante el traslado sobre redes electrónicas:	Se realiza envío de información a través de internet bajo protocolos seguros

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**
    a) Solamente tienen acceso a la información las áreas involucradas con la inspección del departamento de sistemas
    b) Para soportes físicos: N/A
    c) Para soportes electrónicos: Fecha, hora, nombre de usuario, dirección ip y tipo de acción (lectura, escritura, borrado o reasignación).
2. Bitácoras en soporte electrónico
3. Se almacena en un servidor por un año
4. Se respalda semanalmente las bitácoras en conjunto con las bases de datos
5. Respecto del análisis de las bitácoras:
    a) Quién es el responsable de analizarlas: Personal del Departamento de sistemas, mensualmente o de ser necesario cuando sea requerido
    b) Para el caso de que las bitácoras estén en soporte electrónico: No se analizan con herramientas de software.

IV. REGISTRO DE INCIDENTES:

Se realiza levantamiento de un ticket que se entrega inmediatamente después de ser detectado el incidente, que es recibido por el departamento de sistemas de la SA, que consta de:

1. Los datos que registra:
    a) La persona que resolvió el incidente;
    b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen en un servidor del centro de datos y respaldándola en un servidor de soporte.
    c) Para soportes electrónicos: se recuperan todos los campos que decidan las áreas involucradas y de ser el caso un respaldo previo anterior.
2. El registro se encuentra en un medio digital.
3. Se garantiza el resguardo a través de respaldos semanal
4. Para la autorización de la recuperación de datos, los responsables de área deciden.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Se Accesa a las áreas mediante un punto de acceso con lector biométrico de huellas digitales, como primer filtro, para acceder al centro de datos, previa autorización, un responsable del departamento de sistemas contara con las llaves de la cerradura del centro de datos y estará en todo momento en el lugar hasta que se hayan realizado las acciones necesarias. Se cuenta con un sistema CCTV, que vigila la entrada del centro de datos.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista

b) ¿Cómo las autentifica?
Previa entrevista

c) ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la secretaria administrativa.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El centro de datos cuenta con cerraduras y puerta con acceso limitado.

Las llaves de las cerraduras están en manos del departamento de sistemas de la facultad.

1. ¿Cómo las identifica?

Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista

2. ¿Cómo las autentifica?

Previa entrevista

3. ¿Cómo les autoriza el acceso?

Previa autorización de una autoridad de la secretaria administrativa.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización está dada previa solicitud del o las áreas involucradas mediante aviso por correo electrónico o en el mismo sistema, la frecuencia dependerá de la administración de la UNAM, no hay periodicidad

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los perfiles y sus respectivas contraseñas están dadas por nomenclatura, basadas en roles y reglas, el departamento de sistemas y el área involucrada decidirán como, cuando y para que se da de alta un usuario o no, se da de baja o se actualiza

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? si
- **b)** ¿Es discrecional (matriz de control de acceso)? si
- **c)** ¿Está basado en roles (perfiles) o grupos? si
- **d)** ¿Está basado en reglas? si

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  Si, basado en un esquema de herencia
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  Si, además de manejo de recursos compartidos en red, como impresoras y directorios
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Si con profundidad de 256 bits

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
  Si, basado en herencia

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si, con una profundidad de 256 bits

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
Ing. Xavier Jimarez Rodríguez o Ing. Marco Antonio Delgado González
b) ¿Quién autoriza la creación de nuevos perfiles?
Autoridad de le Secretaría administrativa o del área involucrada
c) ¿Se lleva registro de la creación de nuevos perfiles?
Si, en bitácora de base de datos

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
no
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, previo a autorización
c) ¿Cómo se evita el acceso remoto no autorizado?
Bloqueo por medio de firewall, acceso por certificado ssl.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
a) Completos_x_, diferenciales ___ o incrementales___;
b) De forma automática __x__ o Manual _____,
c) Periodicidad con que los realiza: Cada 24 hrs.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad
Respaldo en discos duros

3. Cómo y dónde archiva esos medios,
Se almacenan en el centro de datos de la secretaría administrativa, dentro de racks.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
El área universitaria se encarga de los respaldos, en específico el departamento de sistemas.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia terminado, está en desarrollo

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-05-FN-02	
(Nombre del sistema)*	SITRAP	
Recurso*	**Descripción***	**Control***
No se cuenta con alguna herramienta de monitoreo		

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-05-FN-02	
(Nombre del sistema)*	SITRAP	
Medida de seguridad*	**Procedimiento***	**Responsable***
No se cuentan con medidas de seguridad en el rubro		

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-05-FN-02	
(Nombre del sistema)*	SITRAP	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No existe información en el rubro		

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-05-FN-02	
(Nombre del sistema)*	**SITRAP**	
Medida de seguridad*	**Acciones***	**Responsable***
Gestión integral de la seguridad de la información	Comenzar a definir políticas de seguridad, planes y procedimientos para el análisis y gestión de los riesgos en la seguridad de la información.	Ing. Xavier Jimarez Rodriguez Febrero de 2023

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-05-FN-02
(Nombre del sistema)*	SITRAP

Actividad*	Descripción*	Duración*	Cobertura*
No se cuenta con un programa de capacitación en el rubro			

8.2 Programa de difusión de la protección a los datos personales

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-05-FN-02		
(Nombre del sistema)*	SITRAP		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión en el rubro			

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-05-FN-02		
(Nombre del sistema)*	SITRAP		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-Revisión mensual del funcionamiento correcto del sistema -Respaldo total del sistema y sus bases de datos	-Se revisa modulo, por modulo por posibles bugs a nivel de desarrollo y a nivel de producción -los respaldos se hacen de manera total mensualmente e incremental anualmente	De 20 a 30 días naturales durante los periodos intersemestrales.	-Se garantiza un acceso correcto a la información -se garantiza el resguardo de datos

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-05-FN-02		
(Nombre del sistema)*	SITRAP		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-mantenimiento preventivo semestral -mantenimiento correctivo por evento	-Limpieza de servidores de producción. -Prueba de las líneas de tensión que alimenta a los servidores.	Un día hábil, el penúltimo día del periodo intersemestral	Evitar sobrecalentamientos en servidores Evitar cortes de energía Evitar cortes o cuelgues de red

	-Revisión de cableado estructurado		

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-05-FN-02	
(Nombre del sistema)*	SITRAP	
Proceso*	**Descripción***	**Responsable***
-adquisición de nuevos dispositivos de respaldo -respaldos mensuales	Buscar elementos de almacenamiento como lo son discos duros o nuevas tecnologías. Realizar en tiempo los respaldos necesarios	a) Ing. Xavier Jimarez Rodriguez b) 3 días hábiles

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-05-FN-02	
(Nombre del sistema)*	SITRAP	
Proceso*	**Descripción***	**Responsable***
Proceso basado en el borrado seguro de la circular DGTIC/003/2017	Se puede consultar el procedimiento en la liga: Borrado seguro de información | UNAM-CERT	a) Ing. Xavier Jimarez Rodriguez b) 3 días hábiles

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

NO se cuenta con un protocolo o plan de acción para la cancelación, baja o destrucción de un sistema de tratamiento de datos personales.

Sistema de Ingresos Extraordinarios y Presupuesto de la Facultad de Ingeniería SIEPFI

El Sistema de Ingresos Extraordinarios y Presupuesto de la Facultad de Ingeniería es un sistema en el que se puede administrar el presupuesto y los ingresos extraordinarios de cada una de las Unidades Responsables dentro de la Facultad de Ingeniería. En dicho sistema, la Coordinación de Procesos Administrativos del Departamento de Finanzas le informa sobre la asignación de presupuesto a cada unidad responsable (los cuales pueden acceder al sistema mediante su propio usuario y realizar la consulta), mostrando el detalle del presupuesto designado para cada partida, así como una descripción de la misma.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-06-FN-03
(Nombre del sistema) *	SIEPFI
Datos personales (sensibles o no) contenidos en el sistema*:	Datos Sensibles Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios.
Responsable*:	Ing. Francisco Xavier Jimaréz Rodríguez
Nombre*:	Ing. Francisco Xavier Jimaréz Rodríguez
Cargo*:	Jefe del departamento de sistemas de la secretaría Administrativa
Funciones*:	Administrar, resguardar, manipular las bases de datos donde se alojan los datos personales, así como garantizar el correcto acceso a dichos datos.
Obligaciones*:	-Designa roles de acceso a usuarios del sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Ing. Marco Antonio Delgado Gonzalez
Cargo*:	Desarrolador en jefe del departamento de sistemas
Funciones*:	-Programar las funciones que el responsable haya aprobado -respaldar las bases de datos que contienen datos personales -garantizar el correcto funcionamiento de los sistemas
Obligaciones*:	Mantener en correcto funcionamiento los sistemas de software de la Secretaría Administrativa, validando su disponibilidad para el uso del personal administrativo, asegurando la integridad de la información que se maneja en los mismos y salvaguardando la confidencialidad de los datos tratados por los sistemas. Realizar respaldos de las bases de datos que utilizan los sistemas.

	Usuarios:
(Nombre del Usuario 1*)	Administrador
Cargo*:	Funcionarios, personal académico y personal administrativo
Funciones*:	Manejo de presupuesto
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 2*)	Jefe de Unidad Responsable
Cargo*:	Funcionarios, personal académico y personal administrativo
Funciones*:	Autorizar los gastos de los líderes de proyecto
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 3*)	Líder de proyecto
Cargo*:	Personal académico y personal administrativo
Funciones*:	Solicitar presupuesto
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 4*)	Sistemas
Cargo*:	Funcionario
Funciones*:	Consulta de información y presupuesto. Generación de reportes.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único¨*	SA-06-FN-03
(Nombre del sistema *)	SIEPFI
Descripción:*	Base de datos alojada en un servidor local.
Características del lugar donde se resguardan los soportes:*	Site de cómputo ubicado en las instalaciones de la Secretaría Administrativa.

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 270 a 272.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaria Administrativa Facultad de Ingeniería	
Identificador único*	SA-06-FN-03
(Nombre del sistema)*	SIEPFI
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza envió físico de información
Transferencias mediante el traslado de soportes electrónicos:	La información enviada no es cifrada antes de ser enviada, pero es cifrada al momento de ser almacenada, con un número de identificación único y un nivel de protección de 128 bits
Transferencias mediante el traslado sobre redes electrónicas:	Se realiza envío de información a través de internet bajo protocolos seguros.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

a) Solamente tienen acceso a la información las áreas involucradas con la inspección del departamento de sistemas

b) Para soportes físicos: N/A

c) Para soportes electrónicos: Fecha, hora, nombre de usuario, dirección ip y tipo de acción (lectura, escritura, borrado o reasignación).

2. Bitácoras en soporte electrónico

3. Se almacena en un servidor por un año

4. Se respalda semanalmente las bitácoras en conjunto con las bases de datos

5. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas: Personal del Departamento de sistemas, mensualmente o de ser necesario cuando sea requerido

b) Para el caso de que las bitácoras estén en soporte electrónico: No se analizan con herramientas de software.

IV. REGISTRO DE INCIDENTES:

Se realiza levantamiento de un ticket que se entrega inmediatamente después de ser detectado el incidente, que es recibido por el departamento de sistemas de la SA, que consta de:

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen en un servidor del centro de datos y respaldándola en un servidor de soporte.
   c) Para soportes electrónicos: se recuperan todos los campos que decidan las áreas involucradas y de ser el caso un respaldo previo anterior.
2. El registro se encuentra en un medio digital.
3. Se garantiza el resguardo a través de respaldos semanal
4. Para la autorización de la recuperación de datos, los responsables de área deciden.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Se Accesa a las áreas mediante un punto de acceso con lector biométrico de huellas digitales, como primer filtro, para acceder al centro de datos, previa autorización, un responsable del departamento de sistemas contara con las llaves de la cerradura del centro de datos y estará en todo momento en el lugar hasta que se hayan realizado las acciones necesarias. Se cuenta con un sistema CCTV, que vigila la entrada del centro de datos.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
   Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista
b) ¿Cómo las autentifica?
   Previa entrevista
c) ¿Cómo les autoriza el acceso?
   Previa autorización de una autoridad de la Secretaría Administrativa.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El centro de datos cuenta con cerraduras y apertura de puerta limitada.
Las llaves de las cerraduras están en manos del departamento de sistemas de la facultad.

1. ¿Cómo las identifica?
   Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista
2. ¿Cómo las autentifica?
   Previa entrevista
3. ¿Cómo les autoriza el acceso?
   Previa autorización de una autoridad de la secretaria administrativa.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización está dada previa solicitud del o las áreas involucradas mediante aviso por correo electrónico o en el mismo sistema, la frecuencia dependerá de la administración de la UNAM, no hay periodicidad.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los perfiles y sus respectivas contraseñas están dadas por nomenclatura, basadas en roles y reglas, el departamento de sistemas y el área involucrada decidirán como, cuando y para que se da de alta un usuario o no, se da de baja o se actualiza.

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? si
- **b)** ¿Es discrecional (matriz de control de acceso)? si
- **c)** ¿Está basado en roles (perfiles) o grupos? si
- **d)** ¿Está basado en reglas? si

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  Si, basado en un esquema de herencia
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  Si, además de manejo de recursos compartidos en red.
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Si, con profundidad de 256 bits

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
  Si, basado en herencia
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Si, con una profundidad de 256 bits

4. Administración de perfiles de usuario y contraseñas:

- **a)** ¿Quién da de alta nuevos perfiles?
  Ing. Xavier Jimarez Rodríguez o Ing. Marco Antonio Delgado González
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
  Autoridad de le Secretaría administrativa o del área involucrada
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?
  Si, en bitácora de base de datos

5. Acceso remoto al sistema de tratamiento de datos personales:

- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
  no
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
  Si, previo a autorización

c) ¿Cómo se evita el acceso remoto no autorizado?
Bloqueo por medio de firewall, acceso por certificado ssl.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   - **a)** Completos_x_, diferenciales ___ o incrementales___;
   - **b)** De forma automática __x__ o Manual _____,
   - **c)** Periodicidad con que los realiza: Cada 24 hrs.
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad
   Respaldo en discos duros
3. Cómo y dónde archiva esos medios,
   Se almacenan en el centro de datos de la secretaría administrativa, dentro de racks.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   El área universitaria se encarga de los respaldos, en específico el departamento de sistemas.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia terminado, está en desarrollo

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-06-FN-03	
(Nombre del sistema)*	SIEPFI	
Recurso*	**Descripción***	**Control***
No se cuenta con alguna herramienta de monitoreo		

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-06-FN-03	
(Nombre del sistema)*	SIEPFI	
Medida de seguridad*	**Procedimiento***	**Responsable***
No se cuentan con medidas de seguridad en el rubro		

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-06-FN-03	
(Nombre del sistema)*	SIEPFI	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No existe información en el rubro		

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-06-FN-03	
(Nombre del sistema)*	SIEPFI	
Medida de seguridad*	**Acciones***	**Responsable***
Gestión integral de la seguridad de la información	Comienzar a definir políticas de seguridad, planes y procedimientos para el análisis y gestión de los riesgos en la seguridad de la información.	Ing. Xavier Jimarez Rodriguez Febrero de 2023

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-06-FN-03		
(Nombre del sistema)*	SIEPFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación en el rubro			

8.2 Programa de difusión de la protección a los datos personales

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-06-FN-03		
(Nombre del sistema)*	SIEPFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión en el rubro			

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-06-FN-03		
(Nombre del sistema)*	SIEPFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-Revisión mensual del funcionamiento correcto del sistema -Respaldo total del sistema y sus bases de datos	-Se revisa modulo, por modulo por posibles bugs a nivel de desarrollo y a nivel de producción -los respaldos se hacen de manera total mensualmente e incremental anualmente	De 20 a 30 días naturales durante los periodos intersemestrales.	-Se garantiza un acceso correcto a la información -se garantiza el resguardo de datos

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaria Administrativa Facultad de Ingeniería			
Identificador único*	SA-06-FN-03		
(Nombre del sistema)*	**SIEPFI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-mantenimiento preventivo semestral -mantenimiento correctivo por evento	-Limpieza de servidores de producción. -Prueba de las líneas de tensión que alimenta a los servidores. -Revisión de cableado estructurado	Un día hábil, el penúltimo día del periodo intersemestral	Evitar sobrecalentamientos en servidores Evitar cortes de energía Evitar cortes o cuelgues de red

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-06-FN-03	
(Nombre del sistema)*	SIEPFI	
Proceso*	**Descripción***	**Responsable***
-adquisición de nuevos dispositivos de respaldo -respaldos mensuales	Buscar elementos de almacenamiento como lo	a) Ing. Xavier Jimarez Rodriguez

	son discos duros o nuevas tecnologías. Realizar en tiempo los respaldos necesarios	b) 3 días hábiles

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaria Administrativa Facultad de Ingeniería		
Identificador único*	SA-06-FN-03	
(Nombre del sistema)*	SIEPFI	
Proceso*	**Descripción***	**Responsable***
Proceso basado en el borrado seguro de la circular DGTIC/003/2017	Se puede consultar el procedimiento en la liga: Borrado seguro de información | UNAM-CERT	a) Ing. Xavier Jimarez Rodriguez b) 3 dias habiles

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un protocolo o plan de acción para la cancelación, baja o destrucción de un sistema de tratamiento de datos personales.

Sistema de Vale de Salida de Almacén SIVALE

El Sistema de Vale de Salida de Almacén es un sistema desarrollado para la administración de entradas y salidas de productos del almacén de la Facultad de Ingeniería. En dicho sistema es posible solicitar algún producto requerido por el usuario, con lo cual se genera un vale que, posteriormente, es canjeado en el área de Almacén por el producto correspondiente. Para la Coordinación de Bienes y Suministros (administrador del sistema), es posible obtener la visibilidad del inventario de productos que posee, así como realizar la captura correspondiente cuando haya algún ingreso de producto al Almacén.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-07-BYS-01
(Nombre del sistema) *	SIVALE
Datos personales (sensibles o no) contenidos en el sistema*:	El sistema trabaja con datos de identificación, datos laborales y datos académicos, tales como: • Nombre del trabajador • RFC del trabajador • Número de trabajador del profesor • Correo institucional • Departamento al que el empleado está adscrito • Lugar de trabajo
Responsable*:	Departamento de Sistemas
Nombre*:	Ing. Xavier Jimarez Rodríguez
Cargo*:	Jefe de Departamento de Sistemas de la Secretaría Administrativa
Funciones*:	Administrar, resguardar, manipular las bases de datos donde se alojan los datos personales, así como garantizar el correcto acceso a dichos datos.
Obligaciones*:	• Designa roles de acceso a usuarios del sistema con privilegios administrativos. • Decidir sobre la incorporación de nuevas funcionalidades en el sistema. • Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Marco Antonio Delgado González
Cargo*:	Desarrollador en jefe del Departamento de Sistemas de la Secretaría Administrativa
Funciones*:	Desarrollo y mantenimiento de los diferentes sistemas de software para la Secretaría Administrativa que ayuden en la mejora, optimización y automatización de sus procesos.

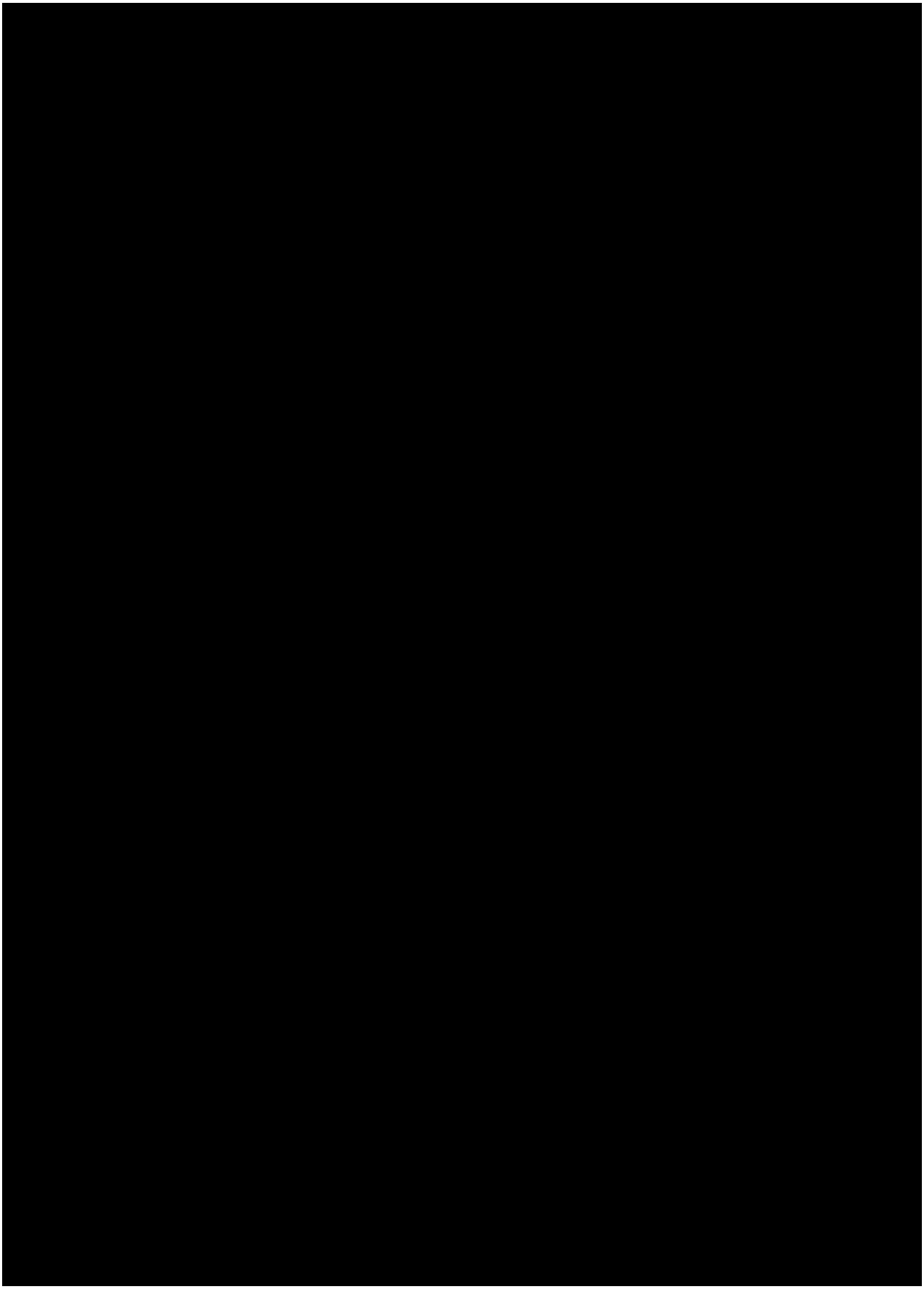
Obligaciones*:	Mantener en correcto funcionamiento los sistemas de software de la Secretaría Administrativa, validando su disponibilidad para el uso del personal administrativo, asegurando la integridad de la información que se maneja en los mismos y salvaguardando la confidencialidad de los datos tratados por los sistemas. Realizar respaldos de las bases de datos que utilizan los sistemas.
	Usuarios:
(Nombre del Usuario 1*)	Administrador
Cargo*:	Funcionario
Funciones*:	Generación de reportes y adquisiciones del almacén. Consulta de histórico.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 2*)	Almacenista
Cargo*:	Personal administrativo
Funciones*:	Acceder al inventario y añadir registros del almacén.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 3*)	Usuario general
Cargo*:	Funcionarios, personal académico y personal administrativo
Funciones*:	Solicitud de productos del almacén.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único¨*	SA-07-BYS-01
(Nombre del sistema *)	SIVALE
Tipo de soporte:*	El sistema se encuentra en soporte físico y electrónico
Descripción:*	Base de datos alojada en un servidor local
Características del lugar donde se resguardan los soportes:*	Site de cómputo ubicado en las instalaciones de la Secretaría Administrativa.

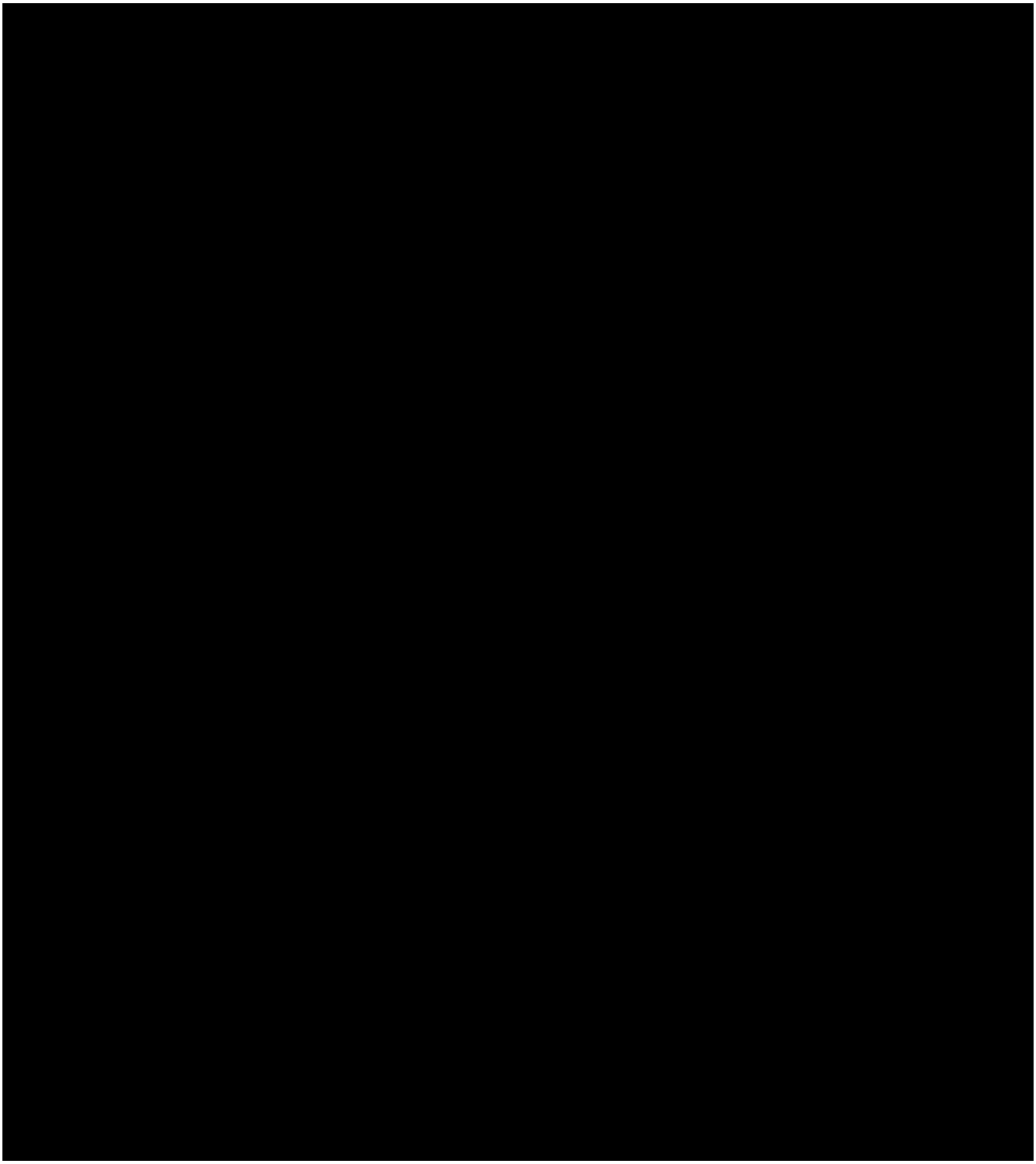
3. ANÁLISIS DE RIESGOS

[redacted]



4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-07-BYS-01
(Nombre del sistema)*	SIVALE
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza envío físico de información.
Transferencias mediante el traslado de soportes electrónicos:	La información, al ser enviada no es cifrada, sin embargo al almacenarse en base de datos se realiza mediante un cifrado MD5.
Transferencias mediante el traslado sobre redes electrónicas:	Se realiza el traslado de información sobre la red utilizando los protocolos seguros.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**

   a) Solamente tiene acceso a la información personal el Departamento de sistemas debido a que es de control interno.
   b) Para soportes físicos: No se cuenta con soportes físicos que traten datos personales.
   c) Para soportes electrónicos: Fecha, hora, nombre de usuario, dirección IP y tipo de acción realizada.
2. Bitácoras en soporte electrónico
3. Se almacena en el servidor por un año
4. Se respaldan semanalmente las bitácoras en conjunto con el resto de la base de datos
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas: el personal del Departamento de Sistemas de la Secretaría Administrativa.
   b) Para el caso de que las bitácoras estén en soporte electrónico: No se analizan con herramientas de software

IV. REGISTRO DE INCIDENTES:

Se realiza levantamiento de un ticket que se entrega inmediatamente después de ser detectado el incidente, que es recibido por el departamento de sistemas de la SA, que consta de:

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen en un servidor del centro de datos y respaldándola en un servidor de soporte.

c) Para soportes electrónicos: se recuperan todos los campos que decidan las áreas involucradas y de ser el caso un respaldo previo anterior.

2. El registro se encuentra en un medio digital.

3. Se garantiza el resguardo a través de respaldos semanal

4. Para la autorización de la recuperación de datos, los responsables de área deciden.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Se accede a las áreas mediante un punto de acceso con lector biométrico de huellas digitales, como primer filtro, para acceder al centro de datos, previa autorización, un responsable del departamento de sistemas contara con las llaves de la cerradura del centro de datos y estará en todo momento en el lugar hasta que se hayan realizado las acciones necesarias. Se cuenta con un sistema CCTV, que vigila la entrada del centro de datos.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista

b) ¿Cómo las autentifica?
Según lo acordado en previa entrevista

c) ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la Secretaría Administrativa.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El centro de datos cuenta cerraduras y puerta con apertura limitada.

Las llaves de las cerraduras están en manos del departamento de sistemas de la facultad. Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista
2. ¿Cómo las autentifica?
Según lo acordado en previa entrevista
3. ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la Secretaría Administrativa.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización está dada previa solicitud del o las áreas involucradas mediante aviso por correo electrónico o en el mismo sistema, la frecuencia dependerá de la administración de la UNAM, no hay periodicidad

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los perfiles y sus respectivas contraseñas están dadas por nomenclatura, basadas en roles y reglas, el departamento de sistemas y el área involucrada decidirán como, cuando y para que se da de alta un usuario o no, se da de baja o se actualiza.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? SÍ
b) ¿Es discrecional (matriz de control de acceso)? SÍ
c) ¿Está basado en roles (perfiles) o grupos? SÍ
d) ¿Está basado en reglas? SÍ

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí, basado en un esquema de herencia
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí, además de manejo de recursos compartidos en red, como impresoras y directorios
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí, con una profundidad de 256 bits.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí, basado en un esquema de herencia
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí, con una profundidad de 256 bits.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Ing. Xavier Jimarez Rodríguez o Ing. Marco Antonio Delgado González
b) ¿Quién autoriza la creación de nuevos perfiles?
Autoridad de le Secretaría administrativa o del área involucrada
c) ¿Se lleva registro de la creación de nuevos perfiles?
Sí, en bitácora de base de datos

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí, previo a autorización
c) ¿Cómo se evita el acceso remoto no autorizado?
Bloqueo por medio firewall, acceso por certificado SSL.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   - **a)** Completos_X_, diferenciales ___ o incrementales___;
   - **b)** De forma automática __X__ o Manual _____,
   - **c)** Periodicidad con que los realiza: Cada 24 hrs.
2. El tipo de medios que utiliza para almacenar las copias de seguridad: discos duros.
3. Cómo y dónde archiva esos medios: en un servidor local y en un disco duro externo.
4. Quién es el responsable de realizar estas operaciones.
   El área universitaria se encarga de los respaldos, en específico el departamento de sistemas.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia terminado, está en desarrollo.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-07-BYS-01	
(Nombre del sistema)*	SIVALE	
Recurso*	**Descripción***	**Control***
No se utilizan herramientas para el monitoreo.	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-07-BYS-01	
(Nombre del sistema)*	SIVALE	
Medida de seguridad*	**Procedimiento***	**Responsable***
No se cuenta con medidas en este rubro	N/A	N/A

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-07-BYS-01	
(Nombre del sistema)*	SIVALE	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No existe información en el rubro.	N/A	N/A

7.4 Acciones para la corrección y actualización de las medidas de seguridad

7.5 Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-07-BYS-01	
(Nombre del sistema)*	SIVALE	
Medida de seguridad*	**Acciones***	**Responsable***
Gestión integral de la seguridad de la información	Comenzar a definir políticas de seguridad, planes y procedimientos para el análisis y gestión de los riesgos en la seguridad de la información.	Ing. Xavier Jimarez Rodríguez Febrero de 2023

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-07-BYS-01		
(Nombre del sistema)*	SIVALE		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación en el rubro	N/A	N/A	N/A

8.2 Programa de difusión de la protección a los datos personales

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-07-BYS-01		
(Nombre del sistema)*	SIVALE		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión en el rubro	N/A	N/A	N/A

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-07-BYS-01		
(Nombre del sistema)*	SIVALE		
Actividad*	**Descripción***	**Duración***	**Cobertura***
• Revisión mensual del funcionamiento correcto del sistema	• Se revisa modulo, por modulo por posibles bugs a nivel de desarrollo y a	De 20 a 30 días naturales durante los periodos intersemestrales.	• Se garantiza un acceso correcto a la información

• Respaldo total del sistema y sus bases de datos	nivel de producción • Los respaldos se hacen de manera total mensualmente e incremental anualmente		• Se garantiza el resguardo de datos

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-07-BYS-01		
(Nombre del sistema)*	SIVALE		
Actividad*	**Descripción***	**Duración***	**Cobertura***
• Mantenimiento preventivo semestral • Mantenimiento correctivo por evento	• Limpieza de servidores de producción. • Prueba de las líneas de tensión que alimenta a los servidores. • Revisión de cableado estructurado	Un día hábil, el penúltimo día del periodo intersemestral	• Evitar sobrecalentamientos en servidores • Evitar cortes de energía • Evitar cortes o cuelgues de red

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-07-BYS-01	
(Nombre del sistema)*	SIVALE	
Proceso*	**Descripción***	**Responsable***
• Adquisición de nuevos dispositivos de respaldo • Respaldos mensuales	Buscar elementos de almacenamiento como lo son discos duros o nuevas tecnologías. Realizar en tiempo los respaldos necesarios	a) Ing. Xavier Jimarez Rodríguez b) 3 días hábiles

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-07-BYS-01	
(Nombre del sistema)*	SIVALE	
Proceso*	**Descripción***	**Responsable***
Proceso basado en el borrado seguro de la circular DGTIC/003/2017	Se puede consultar el procedimiento en la liga: Borrado seguro de información | UNAM-CERT	a) Ing. Xavier Jimarez Rodriguez b) 3 dias habiles

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un protocolo o plan de acción para la cancelación, baja o destrucción de un sistema de tratamiento de datos personales.

Matriz de Indicadores de Resultados MIR

La Matriz de Indicadores de Resultados es un Sistema que lleva el control de los indicadores de resultados programados y los coteja contra los realizados por las diferentes áreas de la Facultad de Ingeniería. Este sistema fue desarrollado para la Coordinación de Asignación y Control Presupuestal y del Sistema de Gestión de la Calidad, el cual es una herramienta que le permite evaluar el desempeño de las diferentes áreas de la Facultad de Ingeniería.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

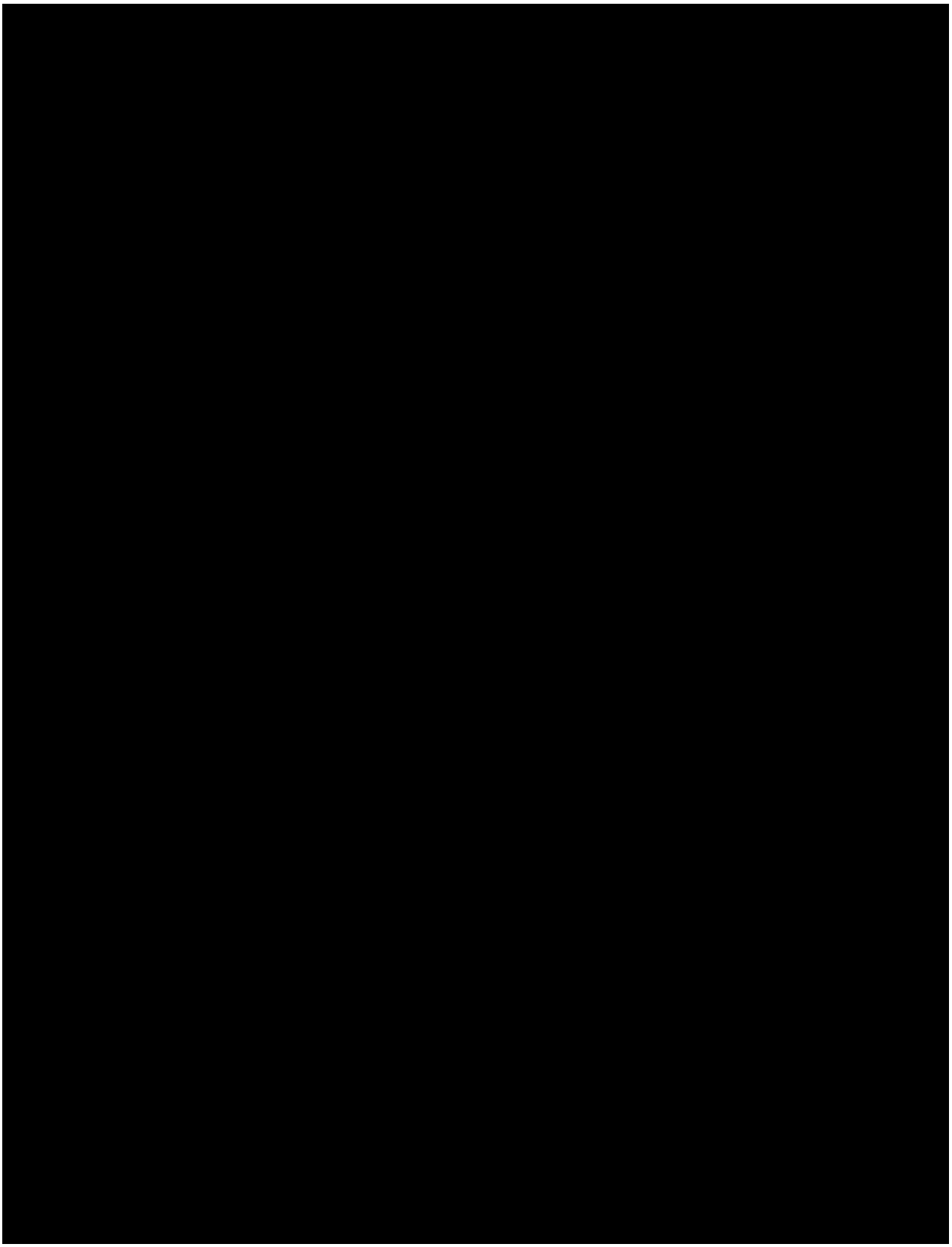
Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-08-ACPYGC-01
(Nombre del sistema) *	MIR
Datos personales (sensibles o no) contenidos en el sistema*:	El sistema trabaja con datos de identificación, datos laborales y datos académicos, tales como: • Nombre del trabajador • RFC del trabajador • Número de trabajador del profesor • Correo institucional • Departamento al que el empleado está adscrito • Lugar de trabajo
Responsable*:	Departamento de Sistemas
Nombre*:	Ing. Xavier Jimarez Rodríguez
Cargo*:	Jefe de Departamento de Sistemas de la Secretaría Administrativa
Funciones*:	Administrar, resguardar, manipular las bases de datos donde se alojan los datos personales, así como garantizar el correcto acceso a dichos datos.
Obligaciones*:	• Designa roles de acceso a usuarios del sistema con privilegios administrativos. • Decidir sobre la incorporación de nuevas funcionalidades en el sistema. • Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Marco Antonio Delgado González
Cargo*:	Desarrollador en jefe del Departamento de Sistemas de la Secretaría Administrativa
Funciones*:	Desarrollo y mantenimiento de los diferentes sistemas de software para la Secretaría Administrativa que ayuden en la mejora, optimización y automatización de sus procesos.
Obligaciones*:	Mantener en correcto funcionamiento los sistemas de

	software de la Secretaría Administrativa, validando su disponibilidad para el uso del personal administrativo, asegurando la integridad de la información que se maneja en los mismos y salvaguardando la confidencialidad de los datos tratados por los sistemas. Realizar respaldos de las bases de datos que utilizan los sistemas.
	Usuarios:
(Nombre del Usuario 1*)	Administrador
Cargo*:	Funcionarios y académicos
Funciones*:	Consulta y registro de información. Generación de reportes. Control de periodos de captura de información.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 2*)	Jefe de unidad
Cargo*:	Académicos
Funciones*:	Coordina y consulta la información de su unidad
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 3*)	Sistemas
Cargo*:	Funcionario
Funciones*:	Consulta y registro de información. Control de periodos de captura de información.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 4*)	Usuario general
Cargo*:	Personal académico y personal administrativo
Funciones*:	Captura de información
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único¨*	SA-08-ACPYGC-01
(Nombre del sistema *)	MIR
Tipo de soporte:*	El sistema se encuentra en soporte físico y electrónico
Descripción:*	Base de datos alojada en un servidor local.
Características del lugar donde se resguardan los soportes:*	Site de cómputo ubicado en las instalaciones de la Secretaría Administrativa.

3. ANÁLISIS DE RIESGOS



Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 293 a 295.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-08-ACPYGC-01
(Nombre del sistema)*	MIR
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza envío físico de información.
Transferencias mediante el traslado de soportes electrónicos:	La información, al ser enviada no es cifrada, sin embargo al almacenarse en base de datos se realiza mediante un cifrado MD5.

Transferencias mediante el traslado sobre redes electrónicas:	Se realiza el traslado de información sobre la red utilizando protocolos seguros.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**
   - **a)** Solamente tiene acceso a la información personal el Departamento de sistemas debido a que es de control interno.
   - **b)** Para soportes físicos: No se cuenta con soportes físicos que traten datos personales.
   - **c)** Para soportes electrónicos: Fecha, hora, nombre de usuario, dirección IP y tipo de acción realizada.
2. Bitácoras en soporte electrónico
3. Se almacena en el servidor por un año
4. Se respaldan semanalmente las bitácoras en conjunto con el resto de la base de datos
5. Respecto del análisis de las bitácoras:
   - **a)** Quién es el responsable de analizarlas: el personal del Departamento de Sistemas de la Secretaría Administrativa.
   - **b)** Para el caso de que las bitácoras estén en soporte electrónico: No se analizan con herramientas de software

IV. REGISTRO DE INCIDENTES:

Se realiza levantamiento de un ticket que se entrega inmediatamente después de ser detectado el incidente, que es recibido por el departamento de sistemas de la SA, que consta de:

1. Los datos que registra:
   - **a)** La persona que resolvió el incidente;
   - **b)** El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen en un servidor del centro de datos y respaldándola en un servidor de soporte.
   - **c)** Para soportes electrónicos: se recuperan todos los campos que decidan las áreas involucradas y de ser el caso un respaldo previo anterior.
2. El registro se encuentra en un medio digital.
3. Se garantiza el resguardo a través de respaldos semanal
4. Para la autorización de la recuperación de datos, los responsables de área deciden.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Se accede a las áreas mediante un punto de acceso con lector biométrico de huellas digitales, como primer filtro, para acceder al centro de datos, previa autorización, un responsable del departamento de sistemas contara con las llaves de la cerradura del centro

de datos y estará en todo momento en el lugar hasta que se hayan realizado las acciones necesarias. Se cuenta con un sistema CCTV, que vigila la entrada del centro de datos.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista
b) ¿Cómo las autentifica?
Según lo acordado en previa entrevista
c) ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la Secretaría Administrativa.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El centro de datos cuenta con cerraduras y puerta con acceso limitado

Las llaves de las cerraduras están en manos del departamento de sistemas de la facultad.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista
2. ¿Cómo las autentifica?
Según lo acordado en previa entrevista
3. ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la Secretaría Administrativa.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización está dada previa solicitud del o las áreas involucradas mediante aviso por correo electrónico o en el mismo sistema, la frecuencia dependerá de la administración de la UNAM, no hay periodicidad

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los perfiles y sus respectivas contraseñas están dadas por nomenclatura, basadas en roles y reglas, el departamento de sistemas y el área involucrada decidirán como, cuando y para que se da de alta un usuario o no, se da de baja o se actualiza.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? SÍ
b) ¿Es discrecional (matriz de control de acceso)? SÍ
c) ¿Está basado en roles (perfiles) o grupos? SÍ
d) ¿Está basado en reglas? SÍ

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí, basado en un esquema de herencia

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí, además de manejo de recursos compartidos en red.

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí, con una profundidad de 256 bits.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí, basado en un esquema de herencia

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí, con una profundidad de 256 bits.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Ing. Xavier Jimarez Rodríguez o Ing. Marco Antonio Delgado González

b) ¿Quién autoriza la creación de nuevos perfiles?
Autoridad de le Secretaría Administrativa o del área involucrada

c) ¿Se lleva registro de la creación de nuevos perfiles?
Sí, en bitácora de base de datos

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí, previo a autorización

c) ¿Cómo se evita el acceso remoto no autorizado?
Bloqueo por medio firewall, acceso por certificado SSL.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

c) Completos_X_, diferenciales ___ o incrementales___;

d) De forma automática __X__ o Manual _____,

e) Periodicidad con que los realiza: Cada 24 hrs.

2. El tipo de medios: discos duros.

3. Cómo y dónde archiva esos medios: en un servidor local y en un disco duro externo.

4. Quién es el responsable de realizar estas operaciones.
El área universitaria se encarga de los respaldos, en específico el departamento de sistemas.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia terminado, está en desarrollo.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-08-ACPYGC-01	
(Nombre del sistema)*	MIR	
Recurso*	**Descripción***	**Control***
No se utilizan herramientas para el monitoreo.	N/A	N/A

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-08-ACPYGC-01	
(Nombre del sistema)*	MIR	
Medida de seguridad*	**Procedimiento***	**Responsable***
No se cuenta con medidas en este rubro	N/A	N/A

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-08-ACPYGC-01	
(Nombre del sistema)*	MIR	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No existe información en el rubro.	N/A	N/A

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-08-ACPYGC-01	
(Nombre del sistema)*	MIR	
Medida de seguridad*	**Acciones***	**Responsable***
Gestión integral de la seguridad de la información	Comenzar a definir políticas de seguridad, planes y procedimientos para el análisis y gestión de los riesgos en la seguridad de la información.	Ing. Xavier Jimarez Rodríguez Febrero de 2023

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-08-ACPYGC-01		
(Nombre del sistema)*	MIR		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación en el rubro	N/A	N/A	N/A

8.2. Programa de difusión de la protección a los datos personales

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-08-ACPYGC-01		
(Nombre del sistema)*	MIR		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión en el rubro	N/A	N/A	N/A

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-08-ACPYGC-01		
(Nombre del sistema)*	MIR		
Actividad*	**Descripción***	**Duración***	**Cobertura***
• Revisión mensual del funcionamiento correcto del sistema • Respaldo total del sistema y sus bases de datos	• Se revisa modulo, por modulo por posibles bugs a nivel de desarrollo y a nivel de producción • Los respaldos se hacen de manera total mensualmente e incremental anualmente	De 20 a 30 días naturales durante los periodos intersemestrales.	• Se garantiza un acceso correcto a la información • Se garantiza el resguardo de datos

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-08-ACPYGC-01		
(Nombre del sistema)*	MIR		
Actividad*	**Descripción***	**Duración***	**Cobertura***
• Mantenimiento preventivo semestral • Mantenimiento correctivo por evento	• Limpieza de servidores de producción. • Prueba de las líneas de tensión que alimenta a los servidores. • Revisión de cableado estructurado	Un día hábil, el penúltimo día del periodo intersemestral	• Evitar sobrecalentamientos en servidores • Evitar cortes de energía • Evitar cortes o cuelgues de red

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-08-ACPYGC-01	
(Nombre del sistema)*	MIR	
Proceso*	**Descripción***	**Responsable***
• Adquisición de nuevos dispositivos de respaldo • Respaldos mensuales	Buscar elementos de almacenamiento como lo son discos duros o nuevas tecnologías. Realizar en tiempo los respaldos necesarios	a) Ing. Xavier Jimarez Rodríguez b) 3 días hábiles

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-08-ACPYGC-01
(Nombre del sistema)*	MIR

Proceso*	Descripción*	Responsable*
Proceso basado en el borrado seguro de la circular DGTIC/003/2017	Se puede consultar el procedimiento en la liga: Borrado seguro de información | UNAM-CERT	a) Ing. Xavier Jimarez Rodriguez b) 3 dias habiles

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un protocolo o plan de acción para la cancelación, baja o destrucción de un sistema de tratamiento de datos personales.

Sistema de Soporte Técnico SIST

El Sistema de Soporte Técnico es un sistema de control interno desarrollado para el propio Departamento de Sistemas de la Secretaría Administrativa en el que se lleva el control de información correspondiente a los Usuarios y Equipos que existen en la Secretaría Administrativa.

A su vez, es posible que los usuarios soliciten el servicio de soporte técnico por alguna incidencia que presenten, tal como fallas con el internet, sospecha de virus, problemas con paquetería de Office, problemas de impresión, con el monitor, mouse o teclado de su equipo, así como alguna falla con un software, accesos, asesorías, etc. Para que el Departamento de Sistemas pueda atenderlas.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-09-SIS-01
(Nombre del sistema) *	SIST
Datos personales (sensibles o no) contenidos en el sistema*:	El sistema trabaja con datos de identificación, datos laborales y datos académicos, tales como: • Nombre del trabajador • RFC del trabajador • Número de trabajador del profesor • Correo institucional • Departamento al que el empleado está adscrito • Lugar de trabajo • Equipo de trabajo • Cuenta de acceso a equipo de trabajo • Contraseña de acceso a equipo de trabajo
Responsable*:	Departamento de Sistemas
Nombre*:	Ing. Xavier Jimarez Rodríguez
Cargo*:	Jefe de Departamento de Sistemas de la Secretaría Administrativa
Funciones*:	Administrar, resguardar, manipular las bases de datos donde se alojan los datos personales, así como garantizar el correcto acceso a dichos datos.
Obligaciones*:	• Designa roles de acceso a usuarios del sistema con privilegios administrativos. • Decidir sobre la incorporación de nuevas funcionalidades en el sistema. • Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Marco Antonio Delgado González

Cargo*:	Desarrollador en jefe del Departamento de Sistemas de la Secretaría Administrativa
Funciones*:	Desarrollo y mantenimiento de los diferentes sistemas de software para la Secretaría Administrativa que ayuden en la mejora, optimización y automatización de sus procesos.
Obligaciones*:	Mantener en correcto funcionamiento los sistemas de software de la Secretaría Administrativa, validando su disponibilidad para el uso del personal administrativo, asegurando la integridad de la información que se maneja en los mismos y salvaguardando la confidencialidad de los datos tratados por los sistemas. Realizar respaldos de las bases de datos que utilizan los sistemas.
	Usuarios:
(Nombre del Usuario 1*)	Administrador
Cargo*:	Funcionarios, personal académico y personal administrativo
Funciones*:	Acceso a la información de usuarios y equipos. Revisión de solicitudes de soporte técnico.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 2*)	Usuario general
Cargo*:	Funcionarios, personal académico y personal administrativo
Funciones*:	Solicitud de servicios

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único¨*	SA-09-SIS-01
(Nombre del sistema *)	SIST
Tipo de soporte:*	El sistema se encuentra en soporte físico y electrónico
Descripción*	Base de datos alojada en un servidor local
Características del lugar donde se resguardan los soporte:*	Site de cómputo ubicado en las instalaciones de la Secretaría Administrativa.

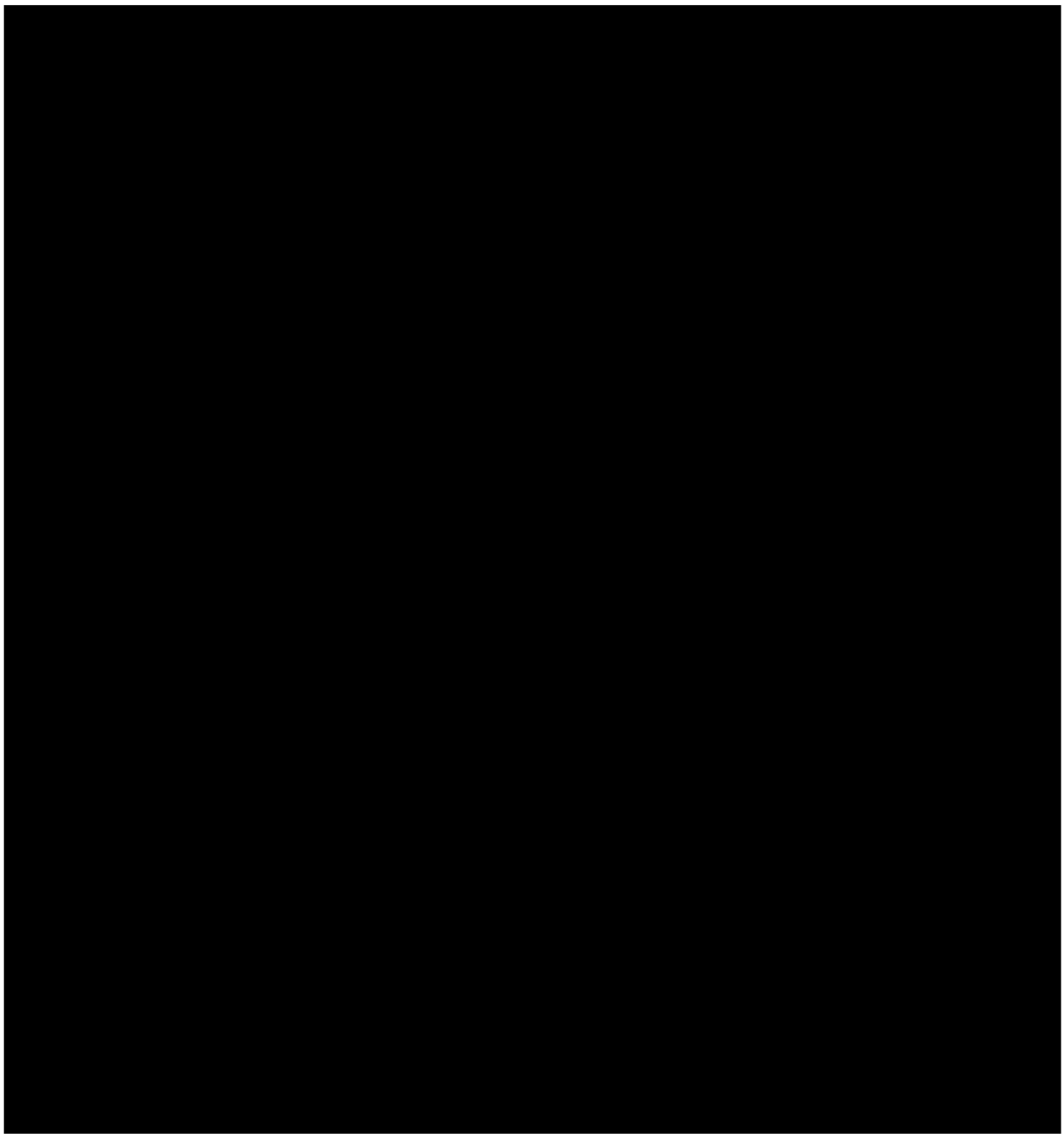
3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 305 a 307.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-09-SIS-01
(Nombre del sistema)*	SIST
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza envío físico de información.

Transferencias mediante el traslado de soportes electrónicos:	La información, al ser enviada no es cifrada, sin embargo, al almacenarse en base de datos se realiza mediante un cifrado MD5.
Transferencias mediante el traslado sobre redes electrónicas:	Se realiza el traslado de información sobre la red utilizando protocolos seguros.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**
   - **a)** Solamente tiene acceso a la información personal el Departamento de sistemas debido a que es de control interno.
   - **b)** Para soportes físicos: No se cuenta con soportes físicos que traten datos personales.
   - **c)** Para soportes electrónicos: Fecha, hora, nombre de usuario, dirección IP y tipo de acción realizada.
2. Bitácoras en soporte electrónico
3. Se almacena en el servidor por un año
4. Se respaldan semanalmente las bitácoras en conjunto con el resto de la base de datos
5. Respecto del análisis de las bitácoras:
   - **a)** Quién es el responsable de analizarlas: el personal del Departamento de Sistemas de la Secretaría Administrativa.
   - **b)** Para el caso de que las bitácoras estén en soporte electrónico: No se analizan con herramientas de software

IV. REGISTRO DE INCIDENTES:

Se realiza levantamiento de un ticket que se entrega inmediatamente después de ser detectado el incidente, que es recibido por el departamento de sistemas de la SA, que consta de:

1. Los datos que registra:
   - **a)** La persona que resolvió el incidente;
   - **b)** El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen en un servidor del centro de datos y respaldándola en un servidor de soporte.
   - **c)** Para soportes electrónicos: se recuperan todos los campos que decidan las áreas involucradas y de ser el caso un respaldo previo anterior.
2. El registro se encuentra en un medio digital.
3. Se garantiza el resguardo a través de respaldos semanal
4. Para la autorización de la recuperación de datos, los responsables de área deciden.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Se accede a las áreas mediante un punto de acceso con lector biométrico de huellas digitales, como primer filtro, para acceder al centro de datos, previa autorización, un responsable del departamento de sistemas contara con las llaves de la cerradura del centro de datos y estará en todo momento en el lugar hasta que se hayan realizado las acciones necesarias. Se cuenta con un sistema CCTV, que vigila la entrada del centro de datos.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista
b) ¿Cómo las autentifica?
Según lo acordado en previa entrevista
c) ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la Secretaría Administrativa.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El centro de datos cuenta con cerraduras y puerta de apertura limitada.

Las llaves de las cerraduras están en manos del departamento de sistemas de la facultad.

Para las personas que acceden a dichos espacios interiores:

a) ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista
b) ¿Cómo las autentifica?
Según lo acordado en previa entrevista
c) ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la Secretaría Administrativa.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización está dada previa solicitud del o las áreas involucradas mediante aviso por correo electrónico o en el mismo sistema, la frecuencia dependerá de la administración de la UNAM, no hay periodicidad

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los perfiles y sus respectivas contraseñas están dadas por nomenclatura, basadas en roles y reglas, el departamento de sistemas y el área involucrada decidirán como, cuando y para que se da de alta un usuario o no, se da de baja o se actualiza.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? SÍ
b) ¿Es discrecional (matriz de control de acceso)? SÍ

c) ¿Está basado en roles (perfiles) o grupos? SÍ
d) ¿Está basado en reglas? SÍ

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí, basado en un esquema de herencia

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí, además de manejo de recursos compartidos en red.

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí, con una profundidad de 256 bits.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí, basado en un esquema de herencia

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí, con una profundidad de 256 bits.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Ing. Xavier Jimarez Rodríguez o Ing. Marco Antonio Delgado González

b) ¿Quién autoriza la creación de nuevos perfiles?
Autoridad de le Secretaría administrativa o del área involucrada

c) ¿Se lleva registro de la creación de nuevos perfiles?
Sí, en bitácora de base de datos

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí, previo a autorización

c) ¿Cómo se evita el acceso remoto no autorizado?
Bloqueo por medio firewall, acceso por certificado SSL.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos_X_, diferenciales ___ o incrementales___;

b) De forma automática __X__ o Manual _____,

c) Periodicidad con que los realiza: Cada 24 hrs.

2. El tipo de medios: discos duros.

3. Cómo y dónde archiva esos medios: en un servidor local y en un disco duro externo.

4. Quién es el responsable de realizar estas operaciones.

El área universitaria se encarga de los respaldos, en específico el departamento de sistemas.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia terminado, está en desarrollo.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-09-SIS-01	
(Nombre del sistema)*	SIST	
Recurso*	**Descripción***	**Control***
No se utilizan herramientas para el monitoreo.	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-09-SIS-01	
(Nombre del sistema)*	SIST	
Medida de seguridad*	**Procedimiento***	**Responsable***
No se cuenta con medidas en este rubro	N/A	N/A

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-09-SIS-01	
(Nombre del sistema)*	SIST	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No existe información en el rubro.	N/A	N/A

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-09-SIS-01	
(Nombre del sistema)*	SIST	
Medida de seguridad*	**Acciones***	**Responsable***
Gestión integral de la seguridad de la información	Comenzar a definir políticas de seguridad, planes y procedimientos para el análisis y gestión de los riesgos en la seguridad de la información.	Ing. Xavier Jimarez Rodríguez Febrero de 2023

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-09-SIS-01		
(Nombre del sistema)*	SIST		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación en el rubro	N/A	N/A	N/A

8.2 Programa de difusión de la protección a los datos personales

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-09-SIS-01		
(Nombre del sistema)*	SIST		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión en el rubro	N/A	N/A	N/A

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-09-SIS-01		
(Nombre del sistema)*	SIST		
Actividad*	**Descripción***	**Duración***	**Cobertura***
• Revisión mensual del funcionamiento correcto del sistema • Respaldo total del sistema y sus bases de datos	• Se revisa modulo, por modulo por posibles bugs a nivel de desarrollo y a nivel de producción • Los respaldos se hacen de manera total mensualmente e incremental anualmente	De 20 a 30 días naturales durante los periodos intersemestrales.	• Se garantiza un acceso correcto a la información • Se garantiza el resguardo de datos

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-09-SIS-01		
(Nombre del sistema)*	SIST		
Actividad*	**Descripción***	**Duración***	**Cobertura***
• Mantenimiento preventivo semestral • Mantenimiento correctivo por evento	• Limpieza de servidores de producción. • Prueba de las líneas de tensión que alimenta a los servidores. • Revisión de cableado estructurado	Un día hábil, el penúltimo día del periodo intersemestral	• Evitar sobrecalentamientos en servidores • Evitar cortes de energía • Evitar cortes o cuelgues de red

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-09-SIS-01	
(Nombre del sistema)*	SIST	
Proceso*	**Descripción***	**Responsable***
• Adquisición de nuevos dispositivos de respaldo • Respaldos mensuales	Buscar elementos de almacenamiento como lo son discos duros o nuevas tecnologías. Realizar en tiempo los respaldos necesarios	a) Ing. Xavier Jimarez Rodríguez b) 3 días hábiles

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-09-SIS-01	
(Nombre del sistema)*	SIST	
Proceso*	**Descripción***	**Responsable***
Proceso basado en el borrado seguro de la circular DGTIC/003/2017	Se puede consultar el procedimiento en la liga: Borrado seguro de información | UNAM-CERT	a) Ing. Xavier Jimarez Rodriguez b) 3 dias habiles

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un protocolo o plan de acción para la cancelación, baja o destrucción de un sistema de tratamiento de datos personales.

Sistema de Control de Acceso a Estacionamientos SICAE

El Sistema de Control de Acceso a Estacionamientos es un sistema para llevar el control de usuarios que tienen permitido acceder a los diferentes estacionamientos, gestionando los días y el horario en el que pueden hacerlo. En este sistema se registra la información del usuario que solicita acceso al estacionamiento, tanto de su nombramiento en la Facultad, como del automóvil que va a registrar, así como el registro de la TAG colocada en el automóvil para otorgarle el acceso. Para asignar los permisos de acceso para el usuario se consultan los horarios de clase del profesor y, con ello, es posible limitar dicho acceso para los estacionamientos, en los días y en el horario que le corresponde.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-10-SIS-02
(Nombre del sistema) *	SICAE
Datos personales (sensibles o no) contenidos en el sistema*:	El sistema trabaja con datos de identificación, datos laborales y datos académicos, tales como: • Nombre del trabajador • RFC del trabajador • Número de trabajador del profesor • Correo personal • Correo institucional • Departamento al que el empleado está adscrito • Lugar de trabajo • Horario de trabajo • Placas de automóvil • Tarjeta de circulación • Credencial de trabajador
Responsable*:	Departamento de Sistemas
Nombre*:	Ing. Xavier Jimarez Rodríguez
Cargo*:	Jefe de Departamento de Sistemas de la Secretaría Administrativa
Funciones*:	Administrar, resguardar, manipular las bases de datos donde se alojan los datos personales, así como garantizar el correcto acceso a dichos datos.
Obligaciones*:	• Designa roles de acceso a usuarios del sistema con privilegios administrativos. • Decidir sobre la incorporación de nuevas funcionalidades en el sistema. • Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Marco Antonio Delgado González

Cargo*:	Desarrollador en jefe del Departamento de Sistemas de la Secretaría Administrativa
Funciones*:	Desarrollo y mantenimiento de los diferentes sistemas de software para la Secretaría Administrativa que ayuden en la mejora, optimización y automatización de sus procesos.
Obligaciones*:	Mantener en correcto funcionamiento los sistemas de software de la Secretaría Administrativa, validando su disponibilidad para el uso del personal administrativo, asegurando la integridad de la información que se maneja en los mismos y salvaguardando la confidencialidad de los datos tratados por los sistemas. Realizar respaldos de las bases de datos que utilizan los sistemas.
	Usuarios:
(Nombre del Usuario 1*)	Administrador
Cargo*:	Funcionarios, personal académico y personal administrativo
Funciones*:	Registro y consulta de información.
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.

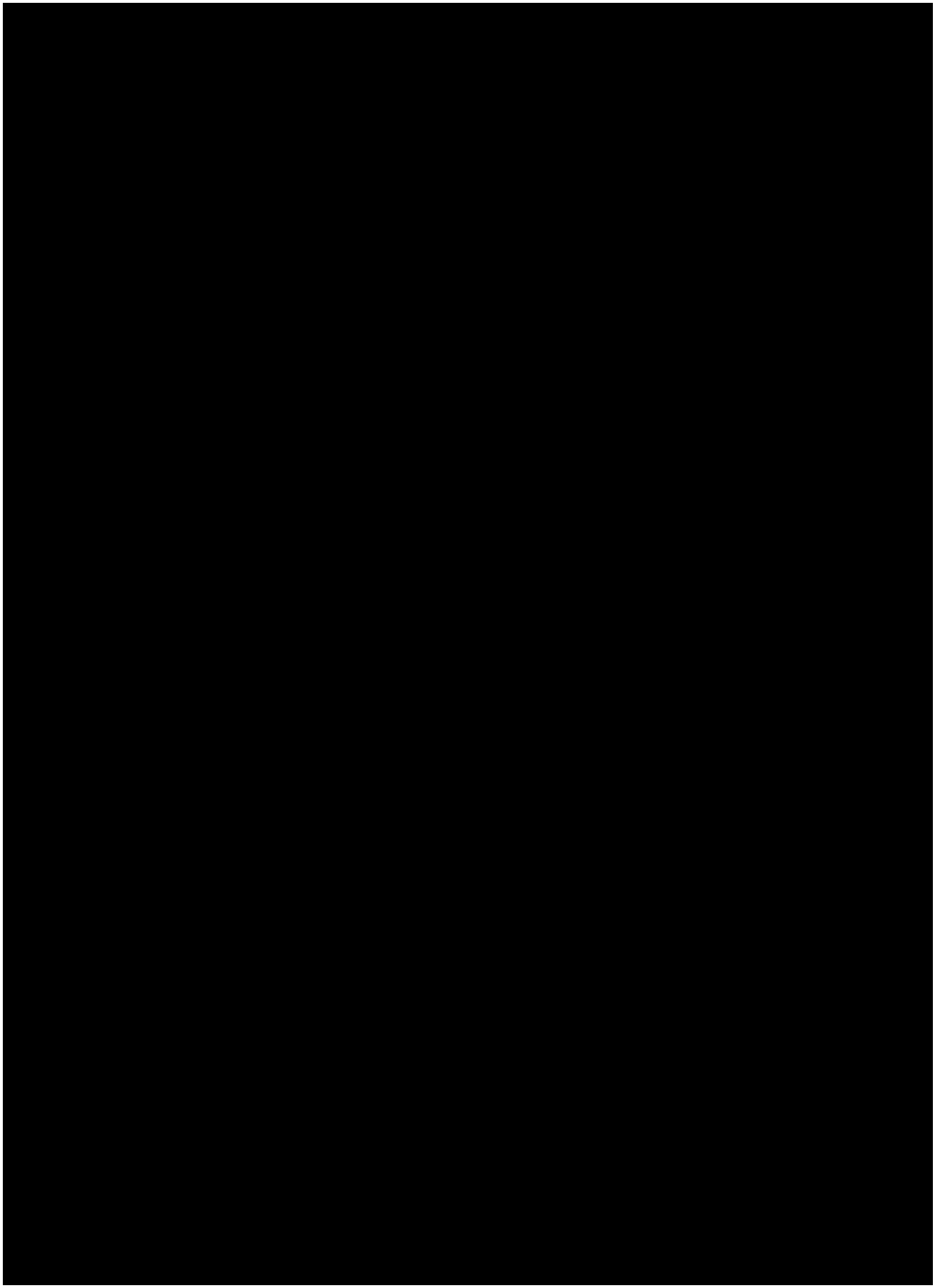
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único¨*	SA-10-SIS-02
(Nombre del sistema *)	SICAE
Tipo de soporte:*	El sistema se encuentra en soporte físico y electrónico
Descripción:*	Base de datos alojada en un servidor local.
Características del lugar donde se resguardan los soportes:*	Site de cómputo ubicado en las instalaciones de la Secretaría Administrativa.

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 316 a 319.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.



4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-10-SIS-02
(Nombre del sistema)*	SICAE
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza envío físico de información.
Transferencias mediante el traslado de soportes electrónicos:	La información, al ser enviada no es cifrada, sin embargo, al almacenarse en base de datos se realiza mediante un cifrado de las contraseñas e información sensible mediante el algoritmo MD5.

Transferencias mediante el traslado sobre redes electrónicas:	Se realiza el traslado de información sobre la red utilizando protocolos seguros.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

a) Solamente tiene acceso a la información personal el Departamento de sistemas debido a que es de control interno.
b) Para soportes físicos: No se cuenta con soportes físicos que traten datos personales.
c) Para soportes electrónicos: Fecha, hora, nombre de usuario, dirección IP y tipo de acción realizada.

2. Bitácoras en soporte electrónico
3. Se almacena en el servidor por un año
4. Se respaldan semanalmente las bitácoras en conjunto con el resto de la base de datos
5. Respecto del análisis de las bitácoras:
a) Quién es el responsable de analizarlas: el personal del Departamento de Sistemas de la Secretaría Administrativa.
b) Para el caso de que las bitácoras estén en soporte electrónico: No se analizan con herramientas de software

IV. REGISTRO DE INCIDENTES:

Se realiza levantamiento de un ticket que se entrega inmediatamente después de ser detectado el incidente, que es recibido por el departamento de sistemas de la SA, que consta de:

1. Los datos que registra:
a) La persona que resolvió el incidente;
b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen en un servidor del centro de datos y respaldándola en un servidor de soporte.
c) Para soportes electrónicos: se recuperan todos los campos que decidan las áreas involucradas y de ser el caso un respaldo previo anterior.

2. El registro se encuentra en un medio digital.
3. Se garantiza el resguardo a través de respaldos semanal
4. Para la autorización de la recuperación de datos, los responsables de área deciden.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Se accede a las áreas mediante un punto de acceso con lector biométrico de huellas digitales, como primer filtro, para acceder al centro de datos, previa autorización, un responsable del departamento de sistemas contara con las llaves de la cerradura del centro

de datos y estará en todo momento en el lugar hasta que se hayan realizado las acciones necesarias. Se cuenta con un sistema CCTV, que vigila la entrada del centro de datos.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista
b) ¿Cómo las autentifica?
Según lo acordado en previa entrevista
c) ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la Secretaría Administrativa.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El centro de datos cuenta cerraduras y puerta con acceso limitado.

Las llaves de las cerraduras están en manos del departamento de sistemas de la facultad. Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista
2. ¿Cómo las autentifica?
Según lo acordado en previa entrevista
3. ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la Secretaría Administrativa.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización está dada previa solicitud del o las áreas involucradas mediante aviso por correo electrónico o en el mismo sistema, la frecuencia dependerá de la administración de la UNAM, no hay periodicidad

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los perfiles y sus respectivas contraseñas están dadas por nomenclatura, basadas en roles y reglas, el departamento de sistemas y el área involucrada decidirán como, cuando y para que se da de alta un usuario o no, se da de baja o se actualiza.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? SÍ
b) ¿Es discrecional (matriz de control de acceso)? SÍ
c) ¿Está basado en roles (perfiles) o grupos? SÍ
d) ¿Está basado en reglas? SÍ

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí, basado en un esquema de herencia

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí, además de manejo de recursos compartidos en red.

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí, con una profundidad de 256 bits.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí, basado en un esquema de herencia

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí, con una profundidad de 256 bits.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Ing. Xavier Jimarez Rodríguez o Ing. Marco Antonio Delgado González

b) ¿Quién autoriza la creación de nuevos perfiles?
Autoridad de le Secretaría administrativa o del área involucrada

c) ¿Se lleva registro de la creación de nuevos perfiles?
Sí, en bitácora de base de datos

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí, previo a autorización

c) ¿Cómo se evita el acceso remoto no autorizado?
Bloqueo por medio firewall, acceso por certificado SSL.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   - **a)** Completos_X_, diferenciales ___ o incrementales___;
   - **b)** De forma automática __X__ o Manual _____,
   - **c)** Periodicidad con que los realiza: Cada 24 hrs.
2. El tipo de medios: discos duros.
3. Cómo y dónde archiva esos medios: en un servidor local y en un disco duro externo.
4. Quién es el responsable de realizar estas operaciones.
   El área universitaria se encarga de los respaldos, en específico el departamento de sistemas.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia terminado, está en desarrollo.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-10-SIS-02	
(Nombre del sistema)*	SICAE	
Recurso*	**Descripción***	**Control***
No se utilizan herramientas para el monitoreo.	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-10-SIS-02	
(Nombre del sistema)*	SICAE	
Medida de seguridad*	**Procedimiento***	**Responsable***
No se cuenta con medidas en este rubro	N/A	N/A

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-10-SIS-02	
(Nombre del sistema)*	SICAE	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No existe información en el rubro.	N/A	N/A

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-10-SIS-02	
(Nombre del sistema)*	SICAE	
Medida de seguridad*	**Acciones***	**Responsable***
Gestión integral de la seguridad de la información	Comenzar a definir políticas de seguridad, planes y procedimientos para el análisis y gestión de los riesgos en la seguridad de la información.	Ing. Xavier Jimarez Rodríguez Febrero de 2023

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-10-SIS-02		
(Nombre del sistema)*	SICAE		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación en el rubro	N/A	N/A	N/A

8.2 Programa de difusión de la protección a los datos personales

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-10-SIS-02		
(Nombre del sistema)*	SICAE		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión en el rubro	N/A	N/A	N/A

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-10-SIS-02		
(Nombre del sistema)*	SICAE		
Actividad*	**Descripción***	**Duración***	**Cobertura***
• Revisión mensual del funcionamiento correcto del sistema • Respaldo total del sistema y sus bases de datos	• Se revisa modulo, por modulo por posibles bugs a nivel de desarrollo y a nivel de producción • Los respaldos se hacen de manera total mensualmente e incremental anualmente	De 20 a 30 días naturales durante los periodos intersemestrales.	• Se garantiza un acceso correcto a la información • Se garantiza el resguardo de datos

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-10-SIS-02		
(Nombre del sistema)*	SICAE		
Actividad*	**Descripción***	**Duración***	**Cobertura***
• Mantenimiento preventivo semestral • Mantenimiento correctivo por evento	• Limpieza de servidores de producción. • Prueba de las líneas de tensión que alimenta a los servidores. • Revisión de cableado estructurado	Un día hábil, el penúltimo día del periodo intersemestral	• Evitar sobrecalentamientos en servidores • Evitar cortes de energía • Evitar cortes o cuelgues de red

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-10-SIS-02	
(Nombre del sistema)*	SICAE	
Proceso*	**Descripción***	**Responsable***
• Adquisición de nuevos dispositivos de respaldo • Respaldos mensuales	Buscar elementos de almacenamiento como lo son discos duros o nuevas tecnologías. Realizar en tiempo los respaldos necesarios	a) Ing. Xavier Jimarez Rodríguez b) 3 días hábiles

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-10-SIS-02
(Nombre del sistema)*	SICAE

Proceso*	Descripción*	Responsable*
Proceso basado en el borrado seguro de la circular DGTIC/003/2017	Se puede consultar el procedimiento en la liga: Borrado seguro de información | UNAM-CERT	a) Ing. Xavier Jimarez Rodriguez b) 3 dias habiles

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un protocolo o plan de acción para la cancelación, baja o destrucción de un sistema de tratamiento de datos personales.

Sistema de Control de Acceso y Asistencia de la Facultad de Ingeniería SICAAFI

El Sistema de Control de Acceso y Asistencia de la Facultad de Ingeniería es un sistema de control interno en el que es posible administrar el acceso biométrico a salones que le correspondan a la Secretaría Administrativa. En dicho sistema es posible registrar la información sobre los horarios de clase y accesos a salones dentro de la Facultad de Ingeniería, así como generar reportes de incidencias ocurridas en las diferentes aulas, dentro de un periodo de tiempo determinado.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-11-SIS-03
(Nombre del sistema) *	SICAAFI
Datos personales (sensibles o no) contenidos en el sistema*:	El sistema trabaja con datos de identificación, datos laborales y datos académicos, tales como: • Nombre del trabajador • RFC del trabajador • Número de trabajador del profesor • Correo institucional • Departamento al que el empleado está adscrito • Lugar de trabajo
Responsable*:	Departamento de Sistemas
Nombre*:	Ing. Xavier Jimarez Rodríguez
Cargo*:	Jefe de Departamento de Sistemas de la Secretaría Administrativa
Funciones*:	Administrar, resguardar, manipular las bases de datos donde se alojan los datos personales, así como garantizar el correcto acceso a dichos datos.
Obligaciones*:	• Designa roles de acceso a usuarios del sistema con privilegios administrativos. • Decidir sobre la incorporación de nuevas funcionalidades en el sistema. • Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Marco Antonio Delgado González
Cargo*:	Desarrollador en jefe del Departamento de Sistemas de la Secretaría Administrativa
Funciones*:	Desarrollo y mantenimiento de los diferentes sistemas de software para la Secretaría Administrativa que ayuden en la mejora, optimización y automatización de sus procesos.

Obligaciones*:	Mantener en correcto funcionamiento los sistemas de software de la Secretaría Administrativa, validando su disponibilidad para el uso del personal administrativo, asegurando la integridad de la información que se maneja en los mismos y salvaguardando la confidencialidad de los datos tratados por los sistemas. Realizar respaldos de las bases de datos que utilizan los sistemas.
	Usuarios:
(Nombre del Usuario 1*)	Administrador
Cargo*:	Funcionarios
Funciones*:	Acceso a toda la información
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 2*)	Control Estacionamiento
Cargo*:	Personal administrativo
Funciones*:	Acceso a la información relativa a estacionamientos
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.
(Nombre del Usuario 3*)	Consulta Biométricos
Cargo*:	Funcionarios y personal académico
Funciones*:	Consulta de información sobre horarios de clases y biométricos
Obligaciones*:	Resguardar los datos personales y usarla para los fines establecidos.

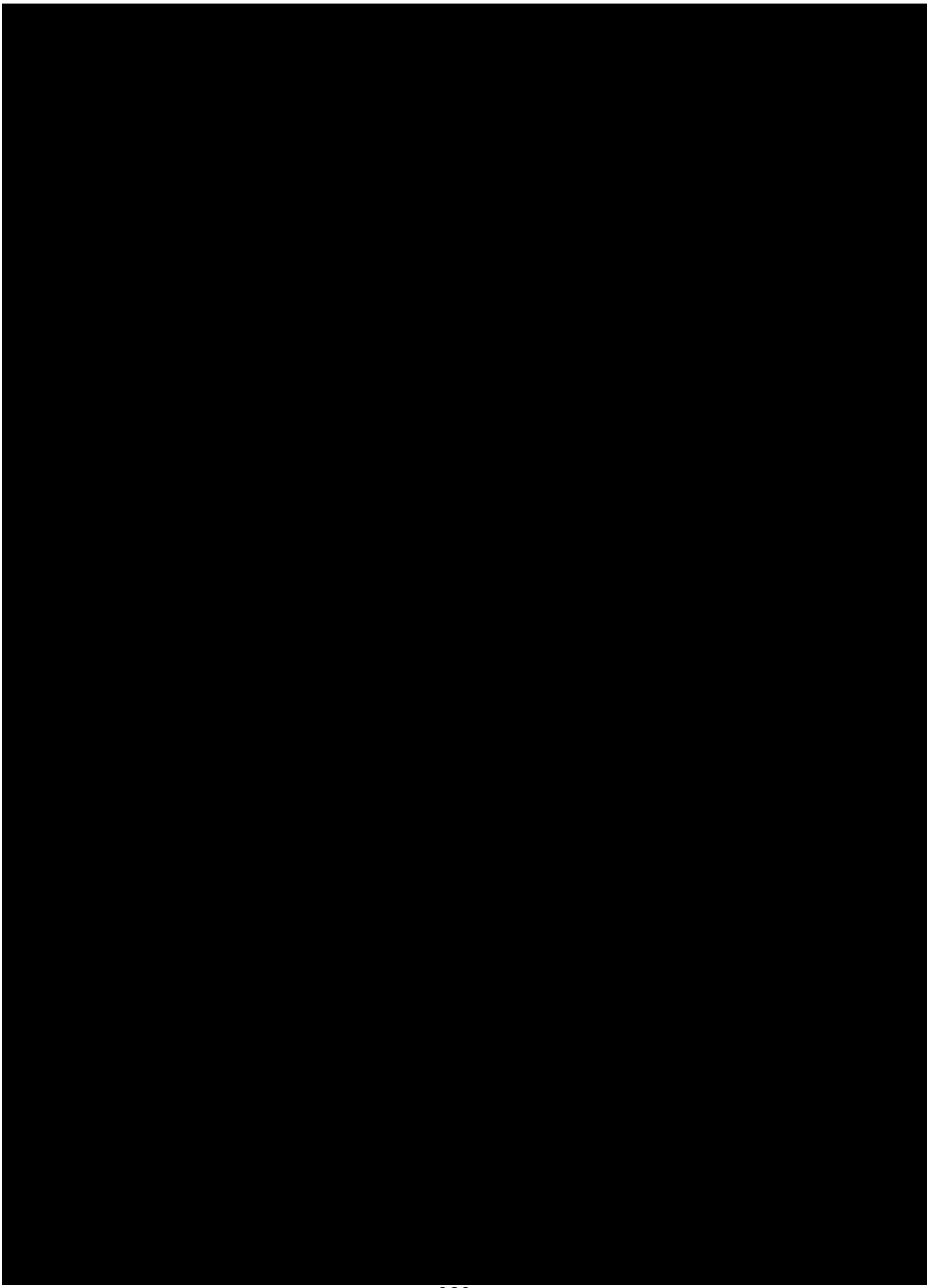
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único¨*	SA-11-SIS-03
(Nombre del sistema *)	SICAAFI
Tipo de soporte:*	El sistema se encuentra en soporte físico y electrónico
Descripción:*	Base de datos alojada en un servidor local.
Características del lugar donde se resguardan los soportes:*	Site de cómputo ubicado en las instalaciones de la Secretaría Administrativa.

3. ANÁLISIS DE RIESGOS

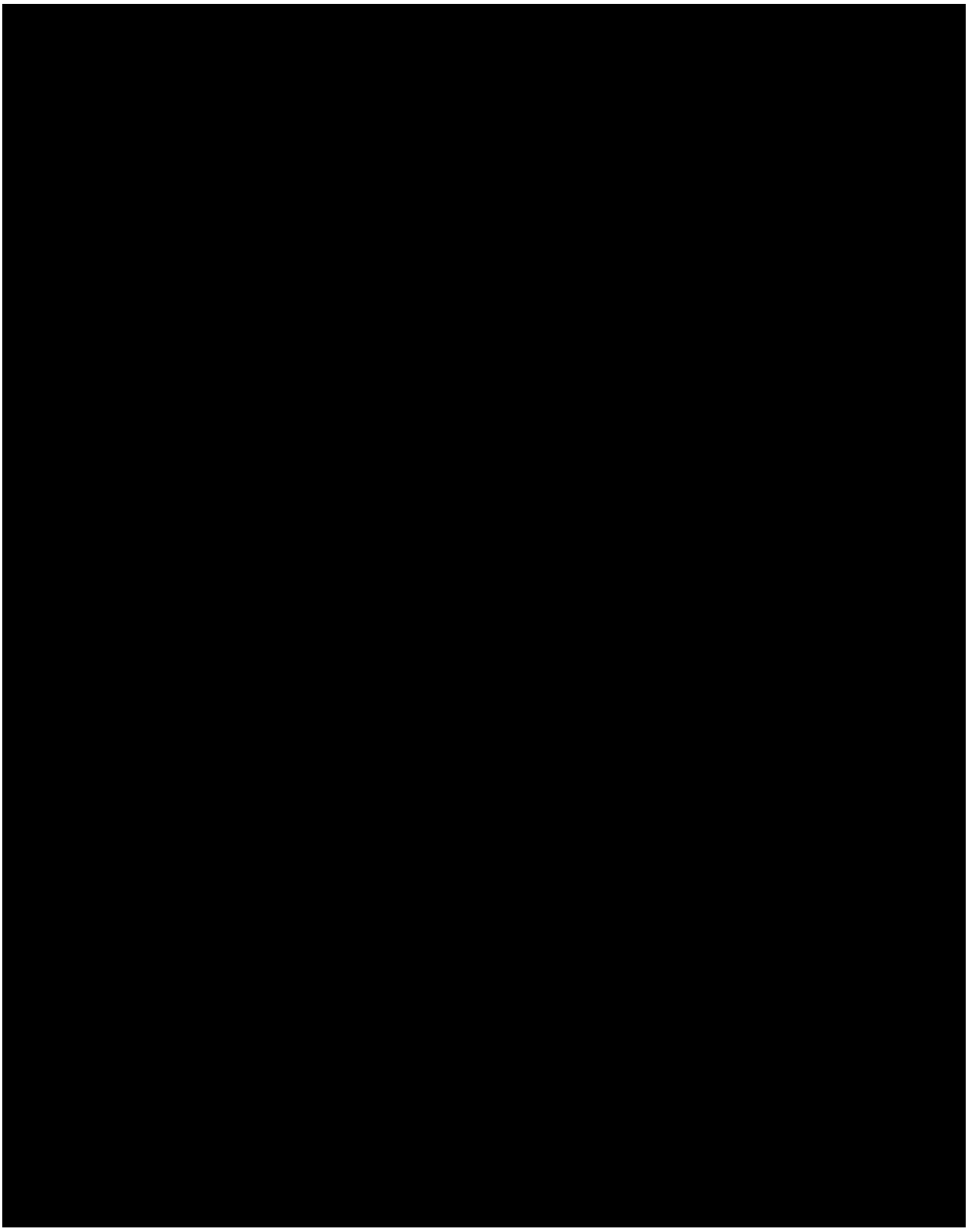
[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 328 a 331.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.



4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-11-SIS-03
(Nombre del sistema)*	SICAAFI
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza envío físico de información.
Transferencias mediante el traslado de soportes electrónicos:	La información, al ser enviada no es cifrada, sin embargo al almacenarse en base de datos se realiza mediante un cifrado MD5.
Transferencias mediante el traslado sobre redes electrónicas:	Se realiza el traslado de información sobre la red utilizando protocolos seguros.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

N/A

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

- **a)** Solamente tiene acceso a la información personal el Departamento de sistemas debido a que es de control interno.
- **b)** Para soportes físicos: No se cuenta con soportes físicos que traten datos personales.
- **c)** Para soportes electrónicos: Fecha, hora, nombre de usuario, dirección IP y tipo de acción realizada.

2. Bitácoras en soporte electrónico
3. Se almacena en el servidor por un año
4. Se respaldan semanalmente las bitácoras en conjunto con el resto de la base de datos
5. Respecto del análisis de las bitácoras:

- **a)** Quién es el responsable de analizarlas: el personal del Departamento de Sistemas de la Secretaría Administrativa.
- **b)** Para el caso de que las bitácoras estén en soporte electrónico: No se analizan con herramientas de software

IV. REGISTRO DE INCIDENTES:

Se realiza levantamiento de un ticket que se entrega inmediatamente después de ser detectado el incidente, que es recibido por el departamento de sistemas de la SA, que consta de:

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen en un servidor del centro de datos y respaldándola en un servidor de soporte.
   c) Para soportes electrónicos: se recuperan todos los campos que decidan las áreas involucradas y de ser el caso un respaldo previo anterior.
2. El registro se encuentra en un medio digital.
3. Se garantiza el resguardo a través de respaldos semanal
4. Para la autorización de la recuperación de datos, los responsables de área deciden.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Se accede a las áreas mediante un punto de acceso con lector biométrico de huellas digitales, como primer filtro, para acceder al centro de datos, previa autorización, un responsable del departamento de sistemas contara con las llaves de la cerradura del centro de datos y estará en todo momento en el lugar hasta que se hayan realizado las acciones necesarias. Se cuenta con un sistema CCTV, que vigila la entrada del centro de datos.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista

b) ¿Cómo las autentifica?
Según lo acordado en previa entrevista

c) ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la Secretaría Administrativa.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El centro de datos cuenta con cerraduras y apertura de puertas limitada.

Las llaves de las cerraduras están en manos del departamento de sistemas de la facultad. Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
Previa autorización de autoridades de la Secretaría Administrativa y previa entrevista

2. ¿Cómo las autentifica?
Según lo acordado en previa entrevista

3. ¿Cómo les autoriza el acceso?
Previa autorización de una autoridad de la Secretaría Administrativa.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización está dada previa solicitud del o las áreas involucradas mediante aviso por correo electrónico o en el mismo sistema, la frecuencia dependerá de la administración de la UNAM, no hay periodicidad

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los perfiles y sus respectivas contraseñas están dadas por nomenclatura, basadas en roles y reglas, el departamento de sistemas y el área involucrada decidirán como, cuando y para que se da de alta un usuario o no, se da de baja o se actualiza.

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? SÍ
- **b)** ¿Es discrecional (matriz de control de acceso)? SÍ
- **c)** ¿Está basado en roles (perfiles) o grupos? SÍ
- **d)** ¿Está basado en reglas? SÍ

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  Sí, basado en un esquema de herencia
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  Sí, además de manejo de recursos compartidos en red, como impresoras y directorios
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Sí, con una profundidad de 256 bits.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
  Sí, basado en un esquema de herencia
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Sí, con una profundidad de 256 bits.

4. Administración de perfiles de usuario y contraseñas:

- **a)** ¿Quién da de alta nuevos perfiles?
  Ing. Xavier Jimarez Rodríguez o Ing. Marco Antonio Delgado González
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
  Autoridad de le Secretaría administrativa o del área involucrada
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?
  Sí, en bitácora de base de datos

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan

para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí, previo a autorización

c) ¿Cómo se evita el acceso remoto no autorizado?
Bloqueo por medio firewall, acceso por certificado SSL.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   - **a)** Completos_X_, diferenciales ___ o incrementales___;
   - **b)** De forma automática __X__ o Manual _____,
   - **c)** Periodicidad con que los realiza: Cada 24 hrs.
2. El tipo de medios: discos duros.
3. Cómo y dónde archiva esos medios: en un servidor local y en un disco duro externo.
4. Quién es el responsable de realizar estas operaciones.
   El área universitaria se encarga de los respaldos, en específico el departamento de sistemas.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia terminado, está en desarrollo.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-11-SIS-03	
(Nombre del sistema)*	SICAAFI	
Recurso*	**Descripción***	**Control***
No se utilizan herramientas para el monitoreo.	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-11-SIS-03	
(Nombre del sistema)*	SICAAFI	
Medida de seguridad*	**Procedimiento***	**Responsable***
No se cuenta con medidas en este rubro	N/A	N/A

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-11-SIS-03	
(Nombre del sistema)*	SICAAFI	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No existe información en el rubro.	N/A	N/A

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-11-SIS-03	
(Nombre del sistema)*	SICAAFI	
Medida de seguridad*	**Acciones***	**Responsable***
Gestión integral de la seguridad de la información	Comenzar a definir políticas de seguridad, planes y procedimientos para el análisis y gestión de los riesgos en la seguridad de la información.	Ing. Xavier Jimarez Rodríguez Febrero de 2023

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-11-SIS-03		
(Nombre del sistema)*	SICAAFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación en el rubro	N/A	N/A	N/A

8.2 Programa de difusión de la protección a los datos personales

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-11-SIS-03		
(Nombre del sistema)*	SICAAFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión en el rubro	N/A	N/A	N/A

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Administrativa de la Facultad de Ingeniería	
Identificador único*	SA-11-SIS-03

(Nombre del sistema)*	SICAAFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
• Revisión mensual del funcionamiento correcto del sistema • Respaldo total del sistema y sus bases de datos	• Se revisa modulo, por modulo por posibles bugs a nivel de desarrollo y a nivel de producción • Los respaldos se hacen de manera total mensualmente e incremental anualmente	De 20 a 30 días naturales durante los periodos intersemestrales.	• Se garantiza un acceso correcto a la información • Se garantiza el resguardo de datos

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Administrativa de la Facultad de Ingeniería			
Identificador único*	SA-11-SIS-03		
(Nombre del sistema)*	SICAAFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
• Mantenimiento preventivo semestral • Mantenimiento correctivo por evento	• Limpieza de servidores de producción. • Prueba de las líneas de tensión que alimenta a los servidores. • Revisión de cableado estructurado	Un día hábil, el penúltimo día del periodo intersemestral	• Evitar sobrecalentamientos en servidores • Evitar cortes de energía • Evitar cortes o cuelgues de red

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-11-SIS-03	
(Nombre del sistema)*	SICAAFI	
Proceso*	**Descripción***	**Responsable***

• Adquisición de nuevos dispositivos de respaldo • Respaldos mensuales	Buscar elementos de almacenamiento como lo son discos duros o nuevas tecnologías. Realizar en tiempo los respaldos necesarios	a) Ing. Xavier Jimarez Rodríguez b) 3 días hábiles

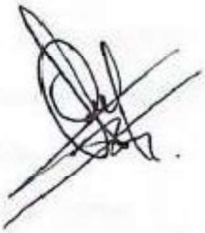
9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría Administrativa de la Facultad de Ingeniería		
Identificador único*	SA-11-SIS-03	
(Nombre del sistema)*	SICAAFI	
Proceso*	**Descripción***	**Responsable***
Proceso basado en el borrado seguro de la circular DGTIC/003/2017	Se puede consultar el procedimiento en la liga: Borrado seguro de información | UNAM-CERT	a) Ing. Xavier Jimarez Rodriguez b) 3 dias habiles

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un protocolo o plan de acción para la cancelación, baja o destrucción de un sistema de tratamiento de datos personales.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Ing. Marco Antonio Delgado González. Desarrollador en jefe del Departamento de Sistemas de la Secretaría Administrativa. marco.delgado@safi.unam.mx 55-61370954	
Revisó:	Ing. Francisco Xavier Jimaréz Rodríguez. Jefe del departamento de Sistemas de la Secretaría Administrativa xavier.jimarez@safi.unam.mx 55-34393774	
Autorizó:	Ing. Luis Jimenez Escobar Secretario Administrativo, Facultad de Ingeniería luis.jimenez@safi.unam.mx 55-56220867	
Fecha de aprobación:	29/08/2022	
Fecha de actualización:		

SECREATRÍA DE SERVICIOS ACADÉMICOS

ANEXO I: DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

ÍNDICE

SECRETARÍA DE SERVICIOS ACADÉMICOS

La Secretaría de Servicios Académicos (SSA) de la Facultad de Ingeniería coordina la planeación y ejecución de los apoyos académicos que se brindan a los estudiantes de la entidad en lo relativo a los servicios de administración escolar (Inscripción, reinscripción, titulación, servicio social y emisión de constancias diversas), bolsa de trabajo, programas deportivos y recreativos, agrupaciones estudiantiles e impresión de materiales didácticos.

Asimismo, resguarda las bases institucionales relacionadas con la trayectoria académica de estudiantes y egresados de la Facultad, así como el desarrollo de aplicaciones para la actualización y uso de información, además, genera reportes estadísticos para apoyar la toma de decisiones de la entidad.

La Secretaría de Servicios Académicos, es reconocida por la calidad de los servicios que brinda a la comunidad estudiantil de la Facultad, distinguiéndose por su trato cordial, cooperativo, digno, eficaz y eficiente, así como por su esquema de mejora continua, siendo un referente en la planeación académica de la entidad.

Dentro de su estructura organizacional la SSA cuenta con las siguientes áreas:

- Unidad de Servicios de Cómputo Administrativo (USECAD)
- Coordinación de Administración Escolar (CAE)
- Departamento de Apoyo a la Comunidad (DAC)
- Departamento de Publicaciones (DEP)
- Secretaría Técnica

Para el desarrollo de sus actividades, la SSA cuenta con los siguientes sistemas de información que involucran datos personales:

- Sistema Escolar TI
- Sistema de Inscripción de la Facultad de Ingeniería (SIINFI)
- Sistema de Titulación (STFI)
- Sistema de Servicios Escolares (SSEFI)

Sistema Escolar TI

El sistema Escolar TI es una herramienta de apoyo a las áreas docentes y administrativas para la gestión de la información de diversos procesos, tales como: Inscripción, Reinscripción, Registro de Exámenes Extraordinarios, Programación de Horarios; asimismo permite la generación y consulta de diversos reportes, entre ellos: datos académicos y personales de alumnos y personal académico.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos	
Identificador único*	SSA-01-USECAD-01
(Nombre del sistema)*	Sistema Escolar TI
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, domicilio particular (calle, colonia, alcaldía o municipio, estado, código postal), teléfono (particular, celular y/o laboral), correo electrónico, RFC (personal académico), CURP (personal académico y alumno), nacionalidad, fecha de nacimiento, edad, contacto de emergencia (nombre, parentesco y teléfono), escolaridad máxima, sexo, número de trabajador de personal académico (UNAM) o número de cuenta (alumnos y exalumnos UNAM).
Responsable*:	USECAD – FACULTAD DE INGENIERÍA
Nombre*:	**M. I. AURELIO SÁNCHEZ VACA**
Cargo*:	**COORDINADOR**
Funciones*:	Coordinar las actividades que se realizan en la USECAD.
Obligaciones*:	Mantener, actualizar y resguardar los sistemas que opera la USECAD cuidando en todo momento la integridad de la información contenida en ellos.
	Encargados:
(Nombre del Encargado 1*)	**Ing. Lenin Guevara López**
Cargo*:	Jefe del Departamento de Procesamiento de Datos.
Funciones*:	Administración y mantenimiento del Sistema Escolar TI.
Obligaciones*:	Sistematizar los Procesos de Inscripción, Reinscripción y Registro de Exámenes Extraordinarios.
(Nombre del Encargado 2*)	**Ing. Leonel Benjamín Pineda Pineda**
Cargo*:	Jefe del Departamento de Análisis de Datos.
Funciones*:	Generar reportes estadísticos útiles para la toma de decisiones de las áreas académicas y autoridades de la Facultad.
Obligaciones*:	Gestionar el acceso de los usuarios al sistema y vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Usuarios:
(Perfil del Usuario 1*)	Áreas académicas y autoridades.
Cargo*:	Director, Secretarios, Jefes de División, Secretarios Académicos, Coordinadores de Carrera y Jefes de

	Departamento.
Funciones*:	Consulta, captura de información y generación de reportes.
Obligaciones*:	Registrar, validar y analizar la información necesaria para la toma de decisiones.
(Perfil del Usuario 2*)	Personal de apoyo para Secretarios Académicos.
Cargo*:	Asistentes secretariales y/o ayudantes.
Funciones*:	Apoyar en el registro de la información.
Obligaciones*:	Registrar la información necesaria para la toma de decisiones.

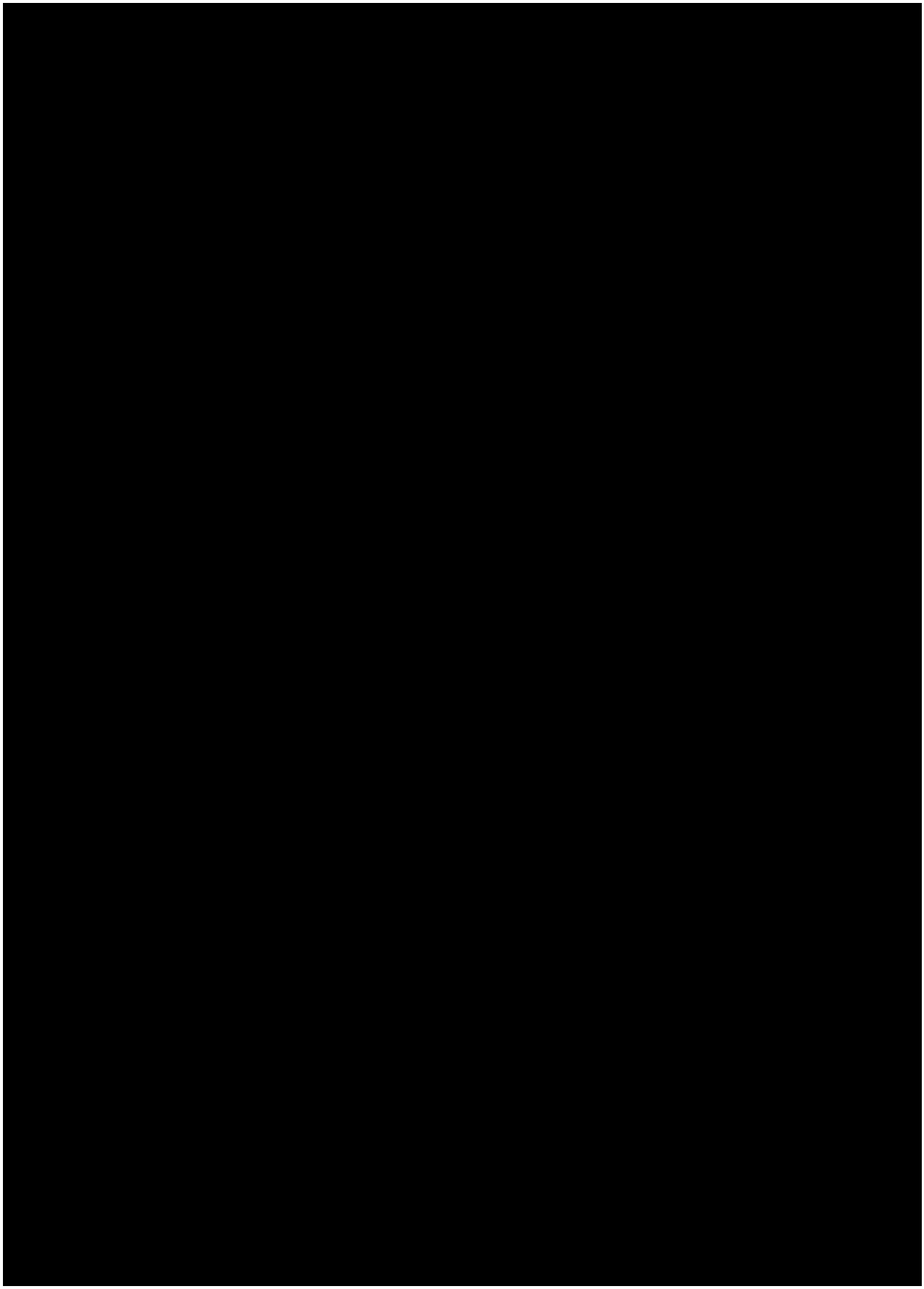
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos	
Identificador único¨*	SSA-01-USECAD-01
(Nombre del sistema)*	Sistema Escolar TI
Tipo de soporte: *	Electrónico.
Descripción: *	Base de datos
Características del lugar donde se resguardan los soportes: *	Centro de datos de la USECAD.

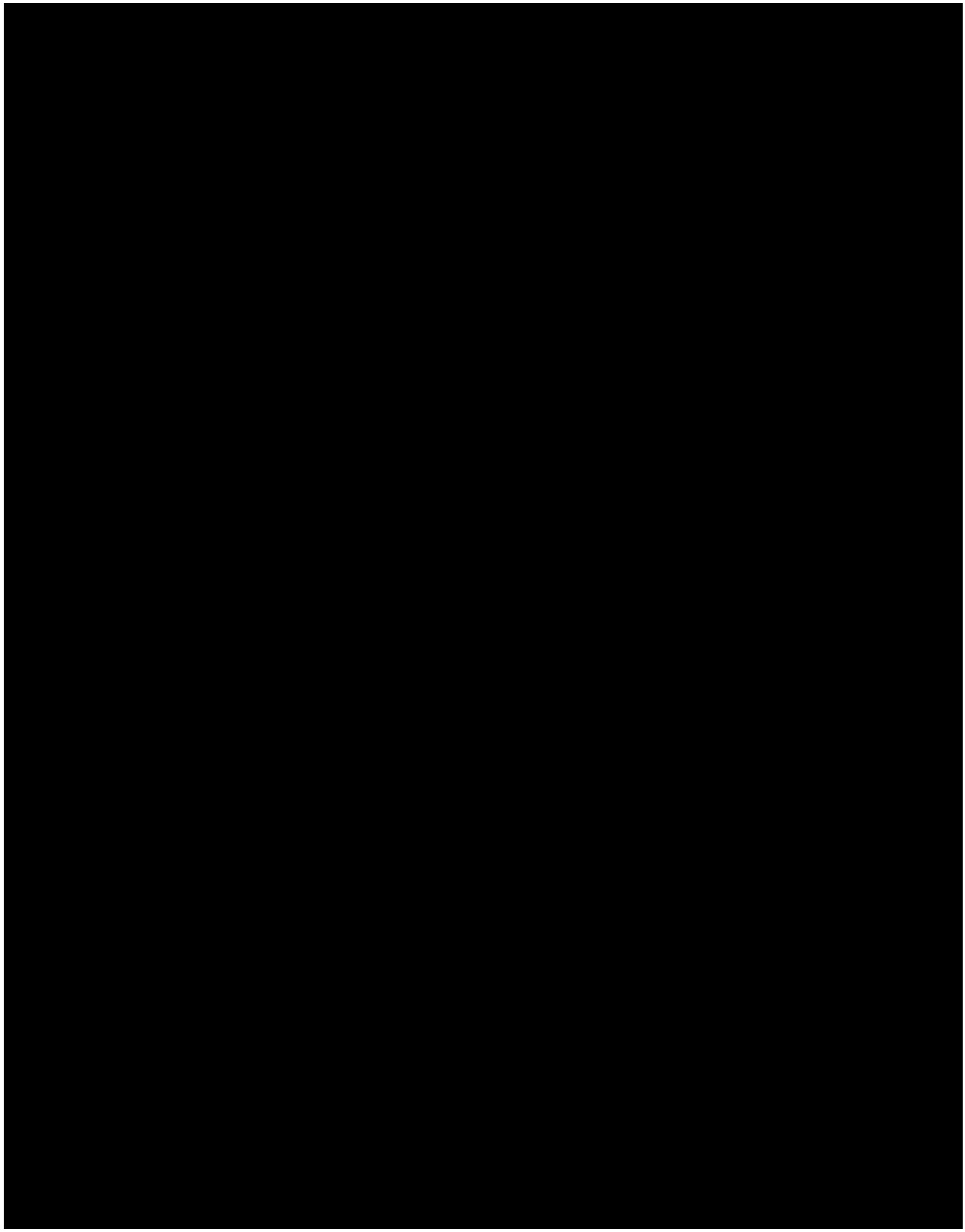
3. ANÁLISIS DE RIESGOS

[redacted]

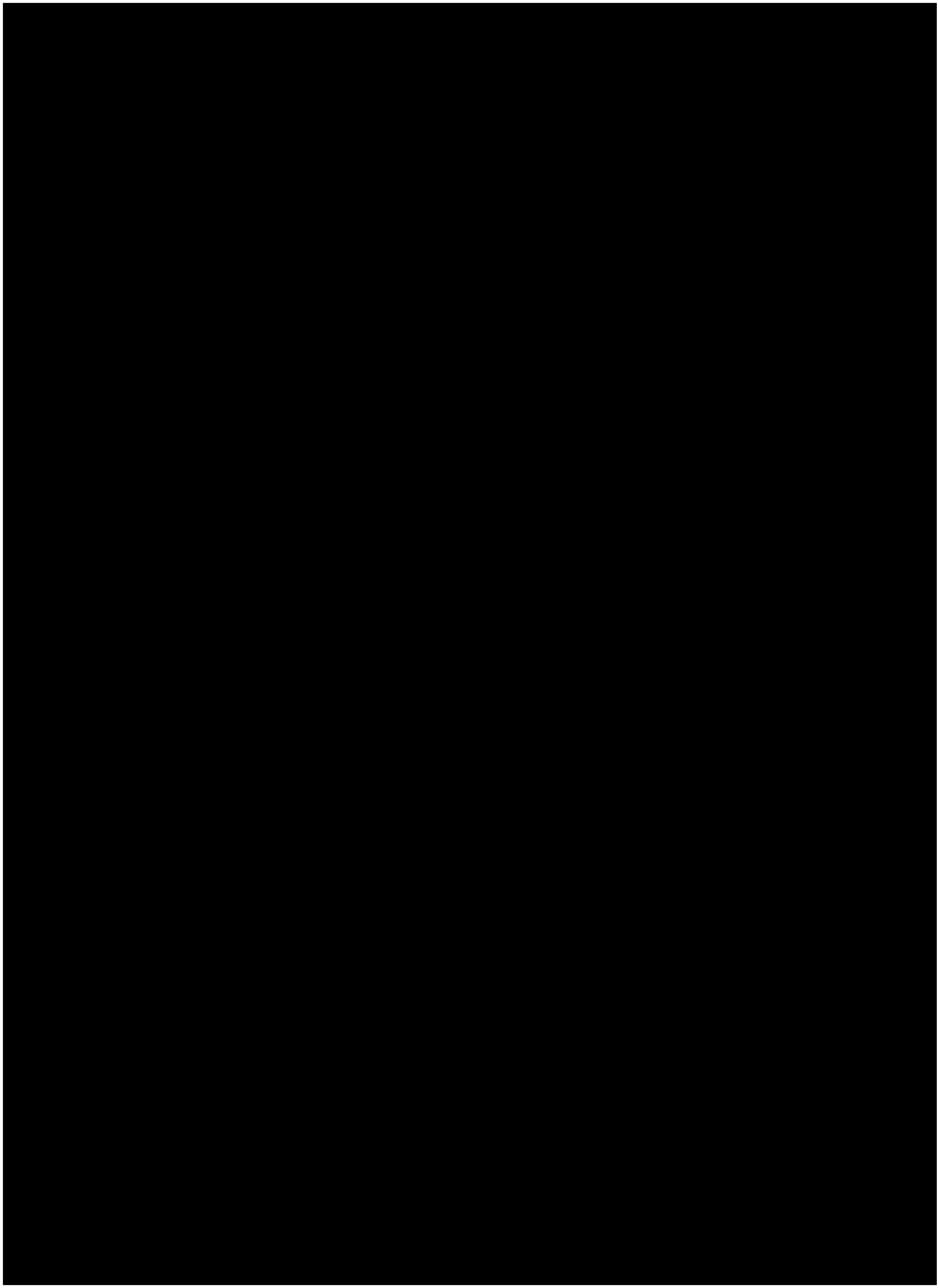
Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 343 a 346.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.



4. ANÁLISIS DE BRECHA



5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I.TRANSFERENCIAS DE DATOS PERSONALES

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos	
Identificador único*	SSA-01-USECAD-01
(Nombre del sistema)*	Sistema Escolar TI
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	Reportes generados por el Sistema tales como: lista de asistencia de alumnos, horarios de clase, matrícula escolar, egresados, encuestas y trayectorias generacionales.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado de redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema Escolar TI no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

III.BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en una ubicación determinada del sistema en el servidor.

IV. REGISTRO DE INCIDENTES:

En el caso de que se presente un incidente relativo al mal uso de la información, se realizará un seguimiento a través de bitácoras en donde se almacena la actividad y acceso al sistema de los usuarios, el cual nos permitirá elaborar un historial de los incidentes.

Por otro lado, en caso de que ocurra un incidente con nuestra base de datos se cuenta con un respaldo de la información elaborado en el tiempo programado para cada proceso.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:
¿Cómo las identifica?
Deberá ser personal adscrito a la USECAD.
¿Cómo las autentifica?
Identificación visual.
¿Cómo les autoriza el acceso?
Identificación visual y acceso con llave para cerradura mecánica.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:
¿Cómo las identifica?
Únicamente el responsable del área puede ingresar a dicho espacio.
¿Cómo las autentifica?
Identificación visual.
¿Cómo les autoriza el acceso?
El responsable del área es el único que cuenta con la autorización para ingresar.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se realizan por medio de interfaces en donde el propio usuario actualiza su información.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso: **Está basado en roles y perfiles**.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  No.
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  No.
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  No.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
  Si.
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Sólo las contraseñas.

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles?
  El Jefe del Departamento de Análisis de Datos.
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
  El Coordinador de USECAD.
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?
  Si, se cuenta incluso con el registro histórico de los perfiles creados y asignados.

5. Acceso remoto al sistema de tratamiento de datos personales:
- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
  Si.
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
  Si.
- **c)** ¿Cómo se evita el acceso remoto no autorizado?
  El acceso remoto al sistema se realiza mediante conexiones VPN habilitadas para los usuarios.
  Implementación de captcha en el inicio de sesión del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X_, diferenciales ___ o incrementales___;
   b) De forma automática __X__ o Manual __X___,
   c) Periodicidad con que los realiza: De acuerdo con el calendario de procesos de cada semestre definido por la Facultad, al finalizar cada uno de ellos se realiza el respaldo correspondiente.
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Discos duros internos y externos
3. Cómo y dónde archiva esos medios: Servidores y equipos de la Unidad
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   El Jefe de Área de Infraestructura en Tecnologías de Información.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

I. Herramientas y recursos para monitoreo de la protección de datos personales

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos		
Identificador único*	SSA-01-USECAD-01	
(Nombre del sistema)*	Sistema Escolar TI	
Recurso*	**Descripción***	**Control***
Herramientas automatizadas.	Se hace uso de herramientas de integración continua.	Se realiza una revisión posterior a cada actualización al sistema. Responsables: Coordinador de la Unidad de Servicios de Cómputo Administrativos. Jefe del Departamento de Procesamiento de Datos. Licencia: asignada para el usuario y de código abierto.

Bitácora del sistema.	Revisión aleatoria.	Se realiza una revisión en horario aleatorio, para validar algún comportamiento inusual. Responsables: Coordinador de la Unidad de Servicios de Cómputo Administrativos. Jefe del Departamento de Procesamiento de Datos.

II. Procedimiento para la revisión de las medidas de seguridad

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos		
Identificador único*	SSA-01-USECAD-01	
(Nombre del sistema)*	Sistema Escolar TI	
Medida de seguridad*	**Procedimiento***	**Responsable***
Plan de respaldos de información.	Revisión y validación del historial de respaldos del sistema.	Jefe del Área de Infraestructura en Tecnologías de Información. La duración de la revisión es un día hábil.
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del firewall y de la base de datos.	Jefe del Área de Infraestructura en Tecnologías de Información. La duración de la revisión es indefinida.
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	Jefe del Área de Infraestructura en Tecnologías de Información. La duración de la revisión es indefinida.

III. Resultados de la evaluación y pruebas a las medidas de seguridad

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos	
Identificador único*	SSA-01-USECAD-01

(Nombre del sistema)*	Sistema Escolar TI	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Plan de respaldos de información.	Se cuenta con respaldos actualizados de la información del sistema.	Jefe del Área de Infraestructura en Tecnologías de Información.
Instalar y mantener actualizado el software antimalware.	El software opera conforme a lo esperado.	Jefe del Área de Infraestructura en Tecnologías de Información.
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Jefe del Área de Infraestructura en Tecnologías de Información.

IV. Acciones para la corrección y actualización de las medidas de seguridad

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos		
Identificador único*	SSA-01-USECAD-01	
(Nombre del sistema)*	Sistema Escolar TI	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL.	Realizar la renovación periódica del certificado SSL para el dominio donde se encuentra el sistema.	Jefe del Área de Infraestructura en Tecnologías de Información.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

I. Programa de a los usuarios del sistema

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos			
Identificador único*	SSA-01-USECAD-01		
(Nombre del sistema)*	Sistema Escolar TI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Se está implementando un programa de capacitación integral	Se encuentran en elaboración los	Indefinido.	Personal administrativo y de apoyo de la Unidad, y

para el manejo del sistema.	manuales de usuario.		responsables de las áreas académicas.

II. Programa de difusión de la protección a los datos personales

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos			
Identificador único*	SSA-01-USECAD-01		
(Nombre del sistema)*	Sistema Escolar TI		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se cuenta con un programa de difusión de la protección de datos personales.

9. MEJORA CONTINUA

I. Actualización y mantenimiento de sistemas de información

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos			
Identificador único*	SSA-01-USECAD-01		
(Nombre del sistema)*	Sistema Escolar TI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización y mantenimiento del Servidor.	Actualizar el sistema operativo del host.	Tiempo indefinido.	Mejorar el rendimiento y protección del sistema.
Mejora continua con base en nuevos requerimientos.	Implementación de nuevas funcionalidades.	Constante.	Mejorar la atención a usuarios.

II. Actualización y mantenimiento de equipo de cómputo

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos			
Identificador único*	SSA-01-USECAD-01		
(Nombre del sistema)*	Sistema Escolar TI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Adquisición de nuevos equipos***.	Reemplazo de equipos descontinuados.	Cuando se presenta una incidencia.	Insuficiente por falta de recursos económicos.
Mantenimiento de equipos.	Reemplazo o integración de componentes de hardware.	Cuando se presenta una incidencia.	Insuficiente por falta de recursos económicos.

*****No se asignan recursos de manera regular para la actualización del equipo de cómputo.**

III. Procesos para la conservación, preservación y respaldos de información

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos		
Identificador único*	SSA-01-USECAD-01	
(Nombre del sistema)*	Sistema Escolar TI	
Proceso*	**Descripción***	**Responsable***
Respaldo de archivos de la base de datos.	Elaboración de copias de seguridad del sistema.	Jefe del Área de Infraestructura en Tecnologías de Información. Tiempo estimado 1 día.
Montaje de respaldo en un ambiente de QA.	Carga de los archivos en ambientes controlados para la elaboración de pruebas.	Jefe del Área de Infraestructura en Tecnologías de Información. Tiempo estimado 1 día.

IV. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos		
Identificador único*	SSA-01-USECAD-01	
(Nombre del sistema)*	Sistema Escolar TI	
Proceso*	**Descripción***	**Responsable***

No se cuenta con proceso de borrado seguro. No se han desechado los equipos que han alojado este sistema.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del Sistema Escolar TI.

Sistema de Inscripción de la Facultad de Ingeniería (SIINFI).

El SIINFI es una herramienta de apoyo para el personal docente y alumnado de la Facultad de Ingeniería, para los procesos de cada semestre de Inscripción, Reinscripción, muestra de manera ordenada y cronológica los pasos a seguir para la Reinscripción, actualización de datos personales del usuario, genera lista de asistencia para los profesores, brinda atención a alumnos de Intercambio y de otras Facultades, cuenta con una sección de consulta de avance de los alumnos para cada uno de los profesores que fungen como Tutores, muestra históricos de grupo con sus respectivas evaluaciones.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos	
Identificador único*	SSA-02-USECAD-02
(Nombre del sistema)*	SIINFI
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, domicilio particular (calle, colonia, alcaldía o municipio, estado, código postal), teléfono (particular, celular y/o laboral), correo electrónico, RFC (personal académico), CURP (personal académico y alumno), nacionalidad, fecha de nacimiento, edad, contacto de emergencia (nombre, parentesco y teléfono), sexo, número de trabajador de personal académico (UNAM) o número de cuenta (alumnos).
Responsable*:	USECAD – FACULTAD DE INGENIERÍA
Nombre*:	**M. I. AURELIO SÁNCHEZ VACA**
Cargo*:	**COORDINADOR**
Funciones*:	Coordinar las actividades que se realizan en la USECAD.
Obligaciones*:	Mantener, actualizar y resguardar los sistemas que opera la USECAD cuidando en todo momento la integridad de la información contenida en ellos.
	Encargados:
(Nombre del Encargado 1*)	**Ing. Lenin Guevara López**
Cargo*:	Jefe del Departamento de Procesamiento de Datos.
Funciones*:	Administración y mantenimiento del Sistema Escolar TI.
Obligaciones*:	Sistematizar los Procesos de Inscripción, Reinscripción y Actualización de Datos Personales.
(Nombre del Encargado 2*)	**Ing. Leonel Benjamín Pineda Pineda**
Cargo*:	Jefe del Departamento de Análisis de Datos.
Funciones*:	Integración entre los sistemas de USECAD y La Secretaría de Apoyo a la Docencia (SAD).
Obligaciones*:	Mantener estrecha comunicación con la SAD.
	Usuarios:
(Perfil del Usuario 1*)	Comunidad estudiantil.
Cargo*:	Alumnos.
Funciones*:	Captura y consulta de información.

Obligaciones*:	Generación y descarga de su comprobante de Inscripción y Horario. Mantener sus datos personales actualizados.
(Perfil del Usuario 2*)	Comunidad docente.
Cargo*:	Profesores.
Funciones*:	Revisar sus resultados de evaluación docente. Seguimiento del avance de los tutorados asignados.
Obligaciones*:	Generar su lista de asistencia, mantener sus datos de contacto actualizados y descargar la Guía del Profesor.

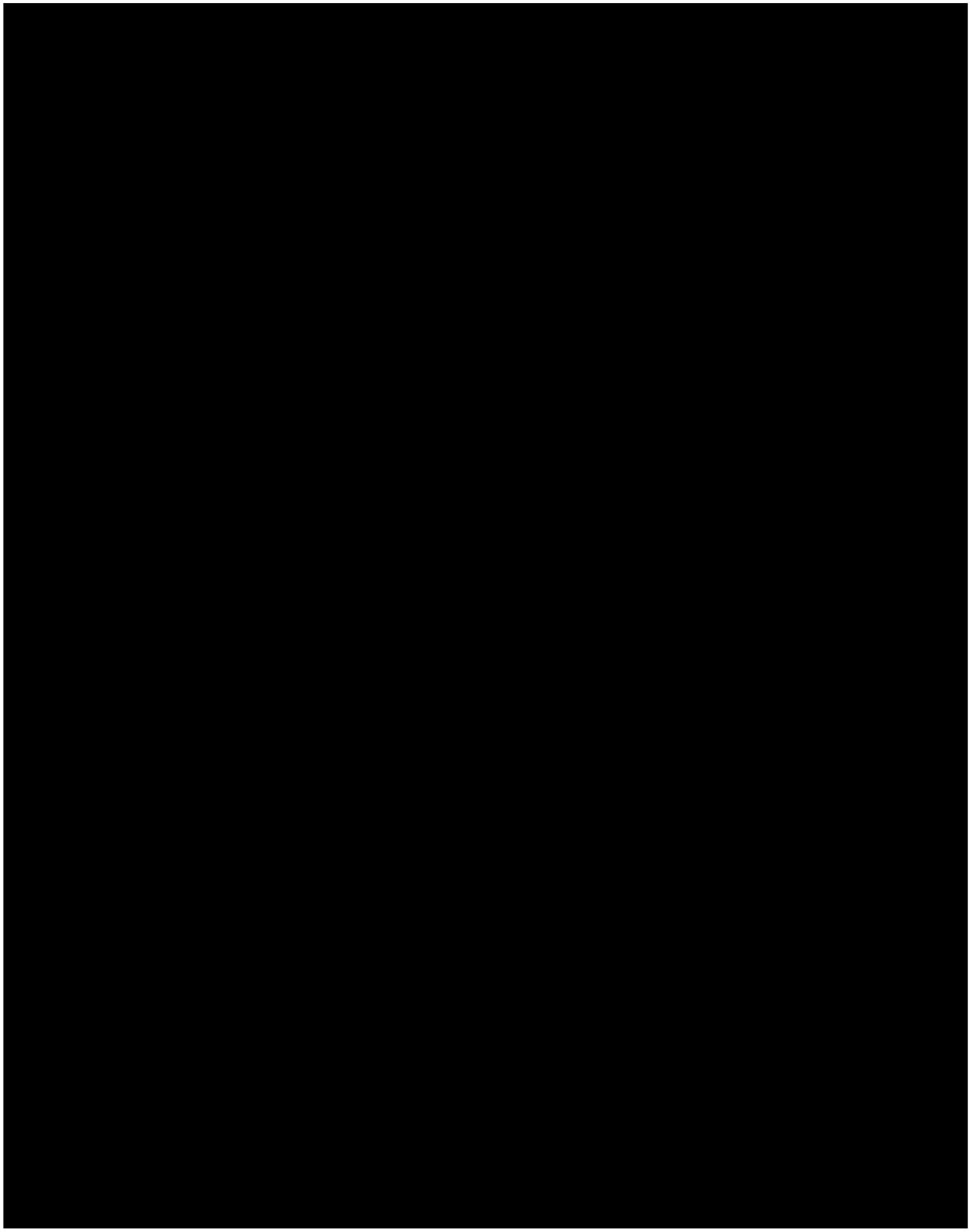
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

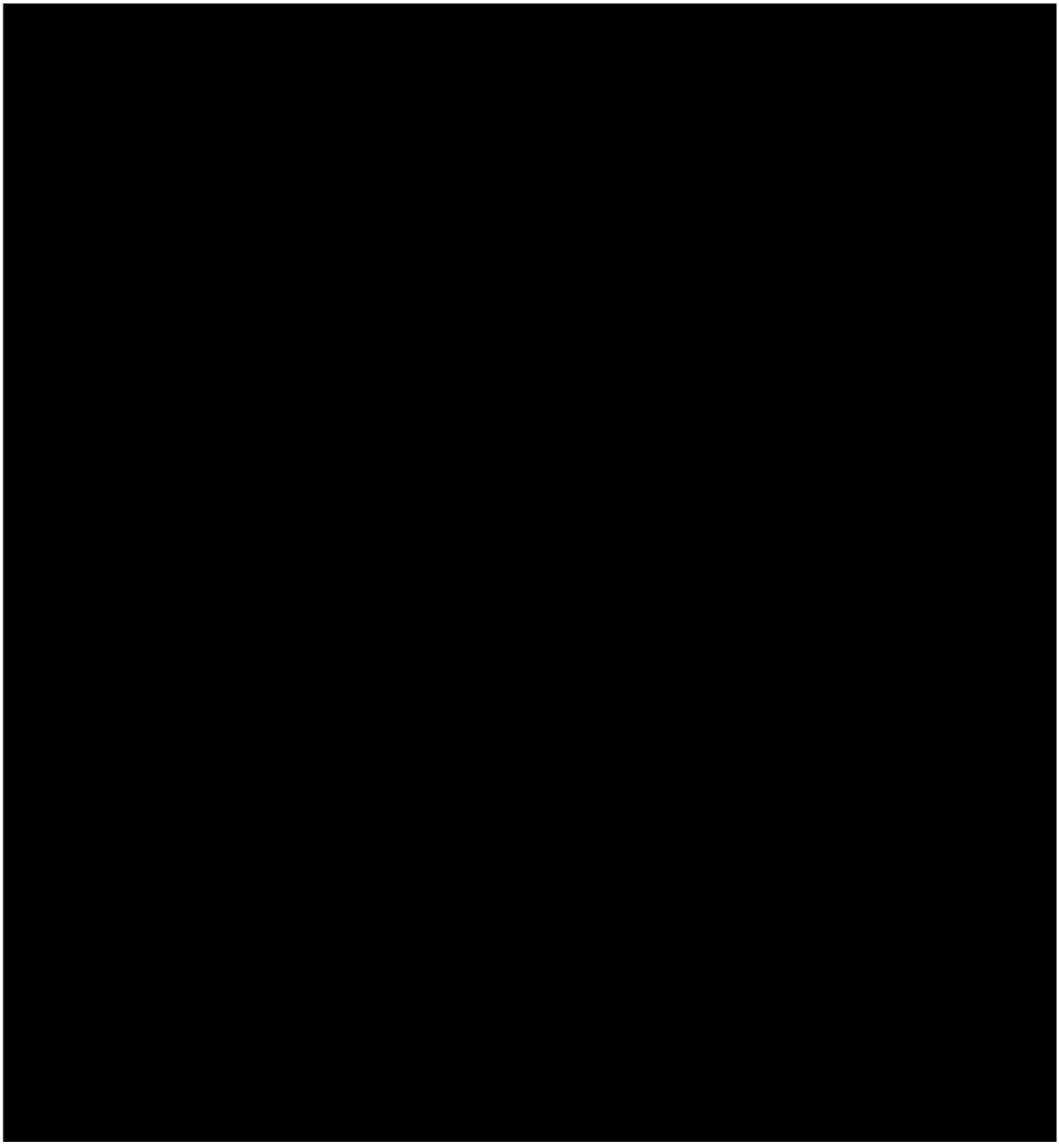
Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos	
Identificador único¨*	SSA-02-USECAD-02
(Nombre del sistema)*	SIINFI
Tipo de soporte: *	Electrónico.
Descripción: *	Base de datos.
Características del lugar donde se resguardan los soportes: *	Centro de datos de la USECAD.

3. ANÁLISIS DE RIESGOS

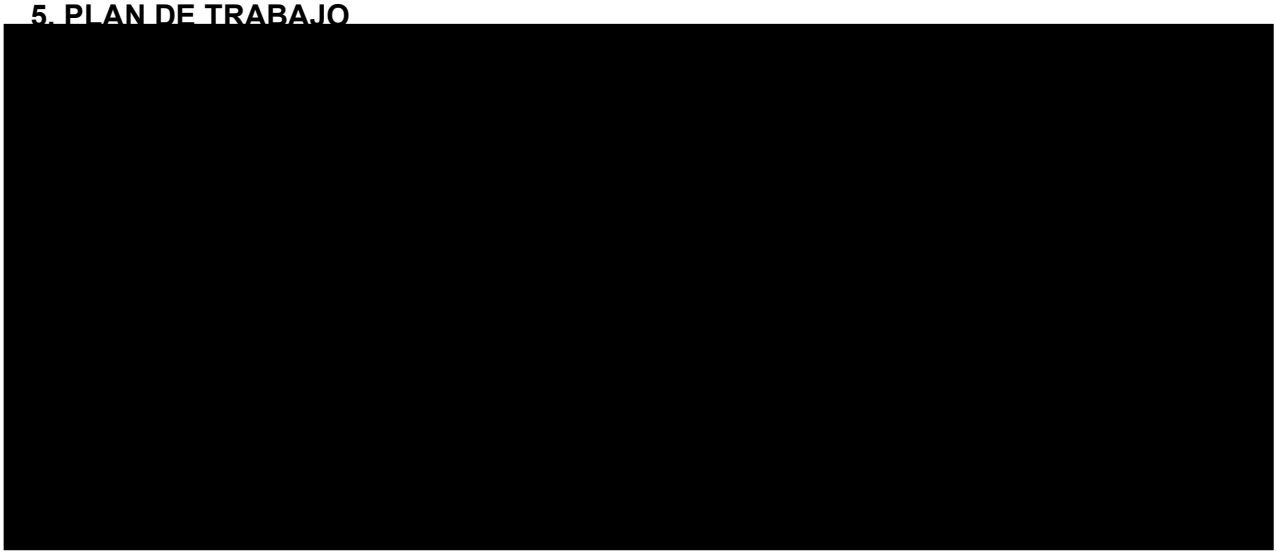
[redacted]

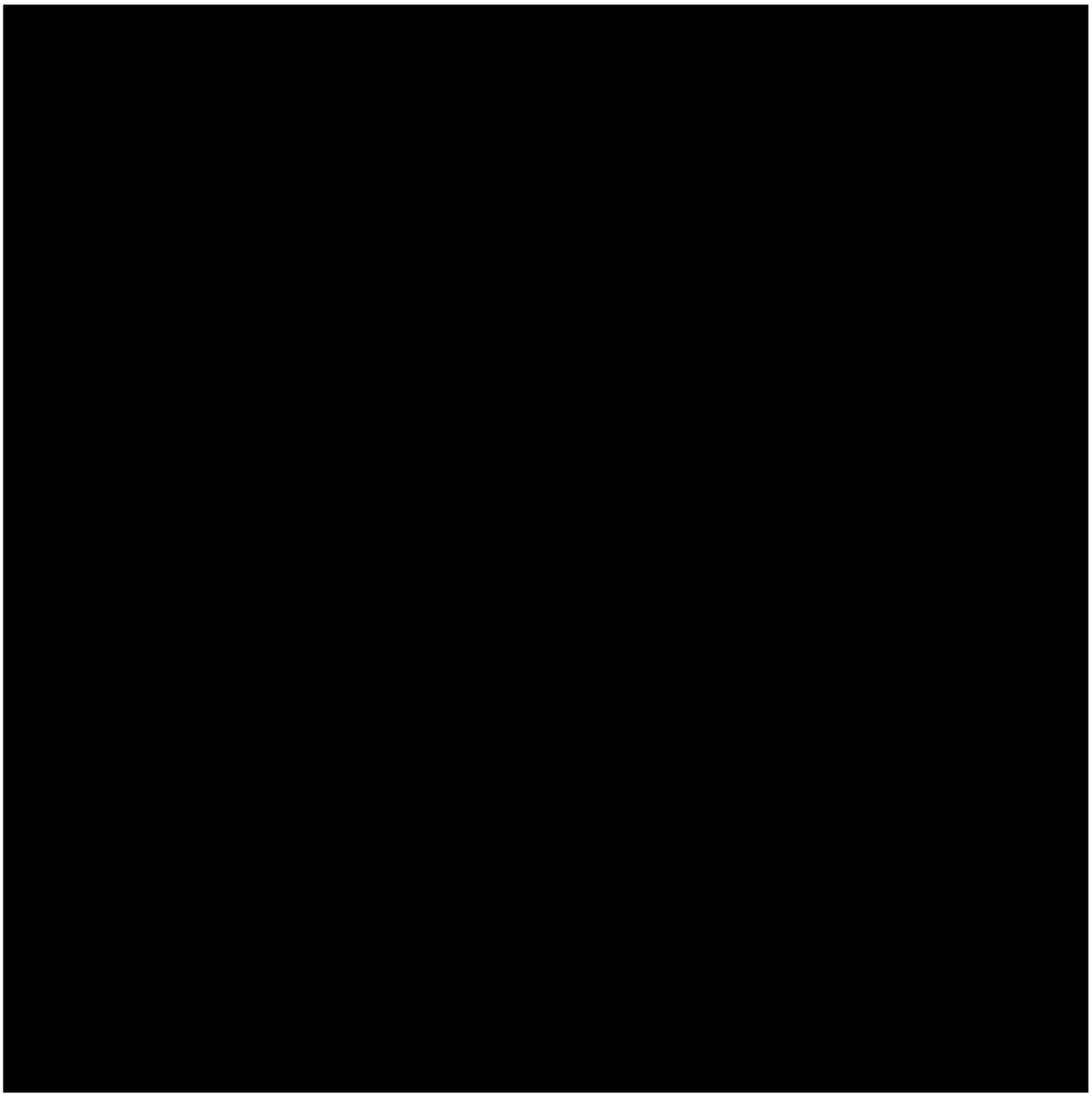
Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las paginas 355 a 358.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.





5. PLAN DE TRABAJO





6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos	
Identificador único*	SSA-02-USECAD-02
(Nombre del sistema)*	SIINFI
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.

Transferencias mediante el traslado de soportes electrónicos:	Reportes generados por el Sistema tales como: lista de asistencia de alumnos, horarios de clase, resultados de encuestas previamente evaluados y trayectorias generacionales.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado de redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El SIINFI no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en una ubicación determinada del sistema en el servidor.

IV. REGISTRO DE INCIDENTES

En el caso de que se presente un incidente relativo al mal uso de la información, se realizará un seguimiento a través de bitácoras en donde se almacena la actividad y acceso al sistema de los usuarios, el cual nos permitirá elaborar un historial de los incidentes.

Por otro lado, en caso de que ocurra un incidente con nuestra base de datos se cuenta con un respaldo de la información elaborado en el tiempo programado para cada proceso

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

¿Cómo las identifica?

Deberá ser personal adscrito a la USECAD.

¿Cómo las autentifica?

Identificación visual.

¿Cómo les autoriza el acceso?

Identificación visual y acceso con llave para cerradura mecánica.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

¿Cómo las identifica?

Únicamente el responsable del área puede ingresar a dicho espacio.

¿Cómo las autentifica?

Identificación visual.

¿Cómo les autoriza el acceso?

El responsable del área es el único que cuenta con la autorización para ingresar.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se realizan por medio de interfaces en donde el propio usuario actualiza su información.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes): **Está basado en roles y perfiles.**

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  No.
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  No.
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  No.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
  Si.
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Sólo las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

- **a)** ¿Quién da de alta nuevos perfiles?
  El Jefe del Departamento de Procesamiento de Datos.
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
  El Coordinador de USECAD.
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?
  Si, se cuenta incluso con el registro histórico de los perfiles creados y asignados.

5. Acceso remoto al sistema de tratamiento de datos personales:

- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
  Si.
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
  Si.
- **c)** ¿Cómo se evita el acceso remoto no autorizado?
  El acceso remoto al sistema se realiza mediante conexiones VPN habilitadas para los usuarios.
  Implementación de captcha en el inicio de sesión del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   - **a)** Completos_X_, diferenciales ___ o incrementales___;
   - **b)** De forma automática __X__ o Manual __X___,
   - **c)** Periodicidad con que los realiza: De acuerdo con el calendario de procesos de cada semestre definido por la Facultad, al finalizar cada uno de ellos se realiza el respaldo correspondiente.
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:

Discos duros internos y externos

3. Cómo y dónde archiva esos medios: Servidores y equipos de la Unidad
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El Jefe del Área de Infraestructura en Tecnologías de Información.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia.

Se cuenta con algunas medidas de seguridad, pero no se tiene desarrollado el instrumentado por completo de un plan de contingencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

I. Herramientas y recursos para monitoreo de la protección de datos personales

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos		
Identificador único*	SSA-02-USECAD-02	
(Nombre del sistema)*	SIINFI	
Recurso*	**Descripción***	**Control***
Herramientas automatizadas.	Se hace uso de herramientas de integración continua.	Se realiza una revisión posterior a cada actualización al sistema. Responsable: Coordinador de la Unidad de Servicios de Cómputo Administrativos. Jefe del Departamento de Procesamiento de Datos. Licencia: asignada para el usuario y de código abierto.
Bitácora del sistema.	Revisión aleatoria.	Se realiza una revisión en horario aleatorio, para validar algún comportamiento inusual. Responsables: Coordinador de la Unidad de Servicios de Cómputo Administrativos.

		Jefe del Departamento de Procesamiento de Datos.

II. Procedimiento para la revisión de las medidas de seguridad

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos		
Identificador único*	SSA-02-USECAD-02	
(Nombre del sistema)*	SIINFI	
Medida de seguridad*	**Procedimiento***	**Responsable***
Plan de respaldos de información.	Revisión y validación del historial de respaldos del sistema.	Jefe del Área de Infraestructura en Tecnologías de Información. La duración de la revisión es un día hábil.
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del firewall y de la base de datos.	Jefe del Área de Infraestructura en Tecnologías de Información. La duración de la revisión es indefinida.
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	Jefe del Área de Infraestructura en Tecnologías de Información. La duración de la revisión es indefinida.

III. Resultados de la evaluación y pruebas a las medidas de seguridad

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos		
Identificador único*	SSA-02-USECAD-02	
(Nombre del sistema)*	SIINFI	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Plan de respaldos de información.	Se cuenta con respaldos actualizados de la información del sistema.	Jefe del Área de Infraestructura en Tecnologías de Información.

Instalar y mantener actualizado el software antimalware.	El software opera conforme a lo esperado.	Jefe del Área de Infraestructura en Tecnologías de Información.
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Jefe del Área de Infraestructura en Tecnologías de Información.

IV. Acciones para la corrección y actualización de las medidas de seguridad

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos		
Identificador único*	SSA-02-USECAD-02	
(Nombre del sistema)*	SIINFI	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL.	Realizar la renovación periódica del certificado SSL para el dominio donde se encuentra el sistema.	Jefe del Área de Infraestructura en Tecnologías de Información.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

I. Programa de a los usuarios del sistema

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos			
Identificador único*	SSA-02-USECAD-02		
(Nombre del sistema)*	SIINFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Se está implementando un programa de capacitación integral para el manejo del sistema.	Se encuentran en elaboración los manuales de usuario.	Indefinido.	Personal administrativo y de apoyo de la Unidad, y responsables de las áreas académicas.

II. Programa de difusión de la protección a los datos personales

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos			
Identificador único*	SSA-02-USECAD-02		
(Nombre del sistema)*	SIINFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se cuenta con un programa de difusión de la protección de datos personales.

9. MEJORA CONTINUA

I. Actualización y mantenimiento de sistemas de información

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos			
Identificador único*	SSA-02-USECAD-02		
(Nombre del sistema)*	SIINFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mejora continua con base en nuevos requerimientos y apoyándonos en las nuevas tecnologías.	Actualizar el sistema operativo del host.	Tiempo indefinido.	Mejorar el rendimiento en el sistema.

II. Actualización y mantenimiento de equipo de cómputo

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos			
Identificador único*	SSA-02-USECAD-02		
(Nombre del sistema)*	SIINFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se han asignado recursos para la actualización del equipo de cómputo.

III. Procesos para la conservación, preservación y respaldos de información

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos		
Identificador único*	SSA-02-USECAD-02	
(Nombre del sistema)*	SIINFI	
Proceso*	**Descripción***	**Responsable***
Respaldo de archivos de la base de datos.	Elaboración de copias de seguridad del sistema.	Jefe del Área de Infraestructura en Tecnologías de Información.

		Tiempo estimado 1 día.
Montaje de respaldo en los ambientes de desarrollo.	Carga de los archivos en ambientes controlados para la elaboración de pruebas y nuevos desarrollos.	Jefe del Área de Infraestructura en Tecnologías de Información. Tiempo estimado 1 día.

IV. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos		
Identificador único*	SSA-02-USECAD-02	
(Nombre del sistema)*	SIINFI	
Proceso*	**Descripción***	**Responsable***
Formateo de unidades de almacenamiento masivo y desecho de equipo en el área correspondiente.	Se borra a bajo nivel los discos duros y se envía la baja a la entidad correspondiente.	Jefe del Área de Infraestructura en Tecnologías de Información.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del SIINFI.

Sistema de Titulación (STFI)

El STFI automatiza el proceso de titulación de los egresados de la Facultad de Ingeniería, permitiendo administrar los eventos de titulación, tanto Exámenes Profesionales (EP), así como de las Ceremonias de Recepción Profesional (CRP). El Sistema permite registrar a todo egresado que cumpla con los requisitos de egreso y titulación necesarios para llevar a cabo un evento de titulación, permite realizar el evento de titulación y llevar el control del expediente de titulación que se transfiere a la DGAE, institución encargada de la emisión de los títulos profesionales.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos	
Identificador único*	SSA-03-CAE-01
(Nombre del sistema)*	Sistema de Titulación
Datos personales (sensibles o no) contenidos en el sistema*:	-Para todos los usuarios del sistema: Nombre completo, correo electrónico, teléfono. -Para los egresado: número de cuenta, RFC, CURP, sexo, domicilio (colonia, estado, alcaldía, ciudad, código postal), teléfono celular, nacionalidad, fecha de nacimiento, lugar de nacimiento, carrera, año de ingreso a la Facultad de Ingeniería, año de egreso a la Facultad de Ingeniería, promedio, modalidad de titulación, título de trabajo escrito (EP), nombre de diplomado o cursos seleccionado(CRP), fecha de titulación, hora del evento de titulación, recinto donde se llevó a cabo el evento, integrantes del Jurado/Comité que participaron en el evento de titulación, resultado del evento de titulación, fecha de envío de expediente de titulación a la DGAE, datos laborales(nombre de la empresa donde laboran, cargo, teléfono de la empresa, correo electrónico laboral). -Para los académicos que han participado en titulación: grado académico, RFC, CURP, no. de trabajador UNAM, nombramiento, división de adscripción, especialidad, datos laborales (nombre de la empresa donde laboran, cargo, teléfono de la empresa, correo electrónico laboral).
Responsable*:	CAE – FACULTAD DE INGENIERÍA
Nombre*:	**ING. JESÚS VALLEJO GONZÁLEZ**
Cargo*:	**COORDINADOR**
Funciones*:	Coordinar las actividades que se realizan en la CAE.
Obligaciones*:	Mantener, actualizar y resguardar los sistemas que opera la CAE cuidando en todo momento la integridad de la información contenida en ellos.
	Encargados:
(Nombre del Encargado 1*)	**Ing. María Fernanda Hernández Delgadillo**
Cargo*:	Administradora del Sistema de Titulación
Funciones*:	Administración y mantenimiento del Sistema de Titulación.

Obligaciones*:	Sistematizar los Procesos de Inscripción, Reinscripción y Registro de Exámenes Extraordinarios.
	Usuarios:
(Perfil del Usuario 1*)	Dr. Carlos Agustín Escalante Sandoval
Cargo*:	Director de la Facultad de Ingeniería
Funciones*:	Generar reportes de titulación.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 2*)	M.I. Miguel Figueroa Bustos
Cargo*:	Secretario de Servicios Académicos
Funciones*:	Generar reportes de titulación.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 3*)	Dr. Edmundo Gabriel Rocha Cozatl
Cargo*:	Jefe del Departamento de Ingeniería Mecatrónica
Funciones*:	Generar reportes de titulación.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 4*)	Myrna Cruz Olmedo
Cargo*:	Secretaría Técnica
Funciones*:	Generar reportes de titulación.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 5*)	Lic. Angélica Gutiérrez Vázquez
Cargo*:	Coordinadora de Titulación y Servicio Social de la División de Ingeniería Eléctrica
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 6*)	M.I. Antonio Zepeda Sánchez
Cargo*:	Coordinador de la Carrera de Ingeniería Mecánica
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 7*)	Ing. Claudia Ivette González Hernández
Cargo*:	Coordinadora de Seminarios y Titulación de la División de Ingeniería Mecánica e Industrial
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 8*)	M.I. Claudia Gabriela Delgado Ávila
Cargo*:	Secretaria Técnica de la División De Ingeniería Civil y Geomática
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.

Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 9*)	M.C. David Escobedo Zenil
Cargo*:	Jefe del Departamento de Ingeniería geofísica
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 10*)	M.I. Berenice Anell Martínez Cabañas
Cargo*:	Coordinadora de la Carrera de Ingeniería Petrolera
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 11*)	Dr. Enrique Alejandro González Torres
Cargo*:	Jefe de la División de Ingeniería de Ciencias de la Tierra
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 12*)	M.I. Isabel Domínguez Trejo
Cargo*:	Coordinadora de la Carrera de Ingeniería Geológica
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 13*)	Ing. Soledad Viridiana Guzmán Herrera
Cargo*:	Coordinadora de la Carrera de Ingeniería de Minas y Metalurgia
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 14*)	Ing. Thalía Alfonsina Reyes Pimentel
Cargo*:	Coordinadora de la Carrera de Ingeniería Geofísica
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 15*)	Gabriela Arriaga Rivas
Cargo*:	Personal de apoyo al área de titulación.
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 16*)	Isela Jannet Popoca Rodríguez
Cargo*:	Personal de apoyo al área de titulación.
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su

	modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 17*)	Josefina Sánchez Sosa
Cargo*:	Registrar en el Sistema de Titulación la entrega del expediente de titulación por parte de los egresados a la coordinación de Administración Escolar.
Funciones*:	Registrar en el Sistema de Titulación a los egresados con su modalidad de titulación, especificaciones, integrantes del Jurado/Comité, así como generación de formatos.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 18*)	Marco Antonio Ramírez Villagómez
Cargo*:	Personal de apoyo al área de titulación de la Coordinación de Administración Escolar.
Funciones*:	Registrar datos académicos de los egresados registrados en el Sistema de Titulación.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 19*)	Silvia Martínez Vivanco
Cargo*:	Personal de apoyo al área de titulación de la Coordinación de Administración Escolar.
Funciones*:	Registrar en el Sistema de Titulación la entrega del expediente de titulación por parte de los egresados a la coordinación de Administración Escolar.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 20*)	Silvia del Carmen Rosales Sánchez
Cargo*:	Personal de apoyo al área de titulación de la Coordinación de Administración Escolar.
Funciones*:	Indicar cuando se realizó el envío del expediente de titulación de los egresados a la DGAE.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 21*)	Planta de alumnos
Cargo*:	Egresado
Funciones*:	Actualizar datos personales y de contacto, descargar constancias de interés propio.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 22*)	Planta de académicos que hayan participado en eventos de titulación
Cargo*:	Personal de apoyo al área de titulación de la Coordinación de Administración Escolar.
Funciones*:	Actualizar datos personales y de contacto, descargar constancias de interés propio.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.

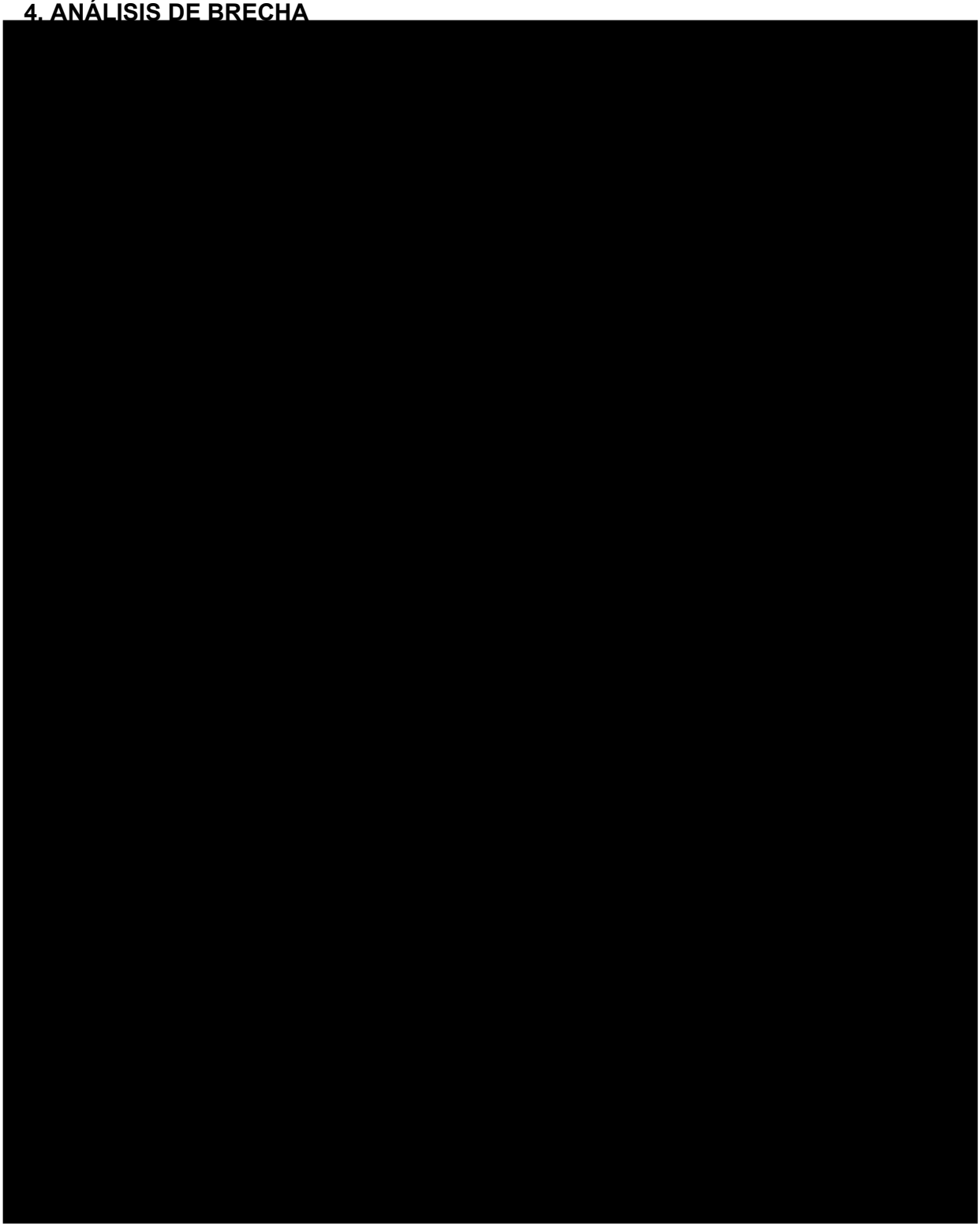
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos	
Identificador único*	SSA-03-CAE-01
(Nombre del sistema)*	Sistema de Titulación
Tipo de soporte: *	Electrónico.
Descripción: *	Base de datos.
Características del lugar donde se resguardan los soportes: *	Cuarto de telecomunicaciones.

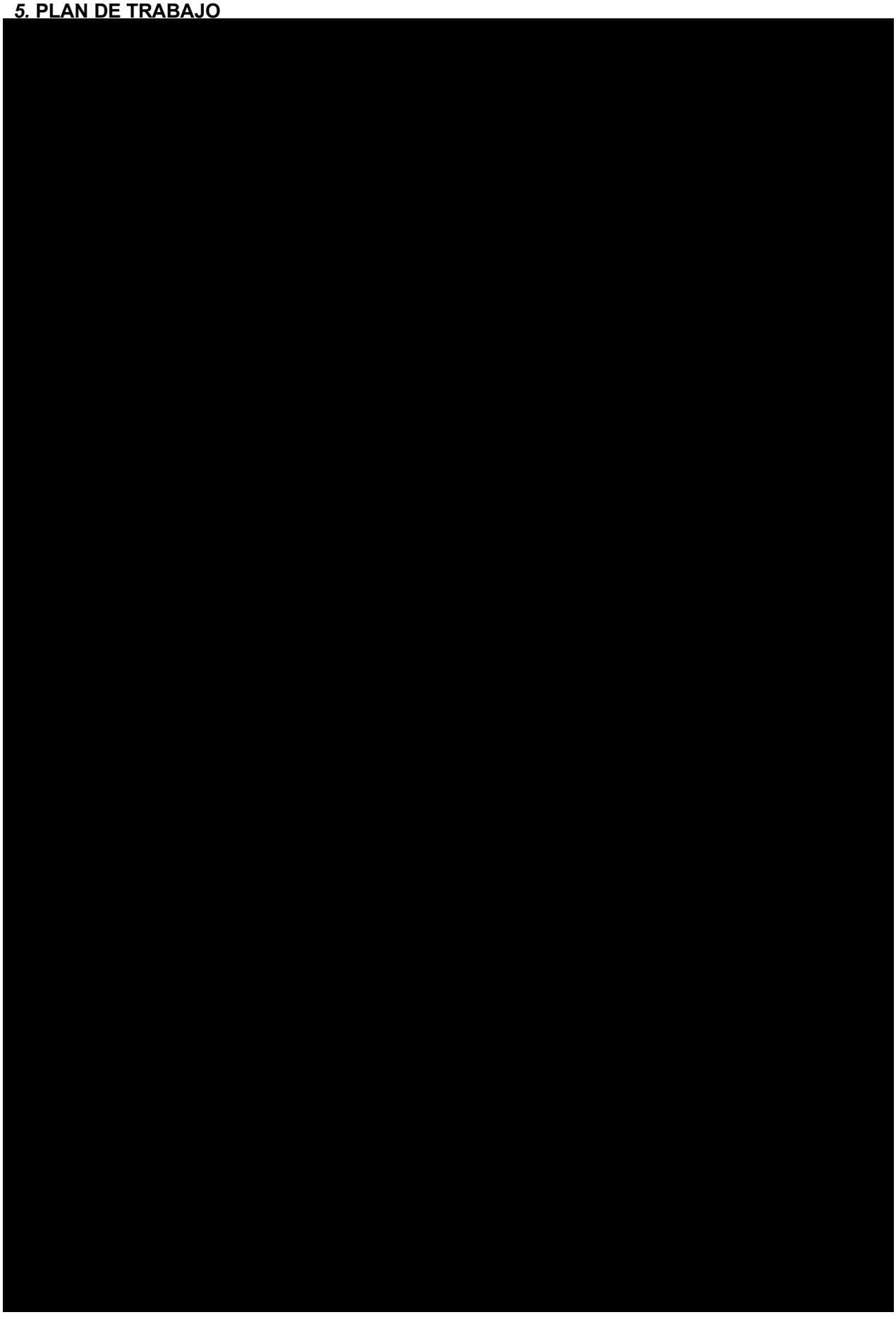
3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA



5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos	
Identificador único*	SSA-03-CAE-01
(Nombre del sistema)*	Sistema de Titulación
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	Reportes generados por el Sistema tales como: listados de egresados, estadísticas de titulación y constancias de eventos realizados.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema de Titulación no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No se cuenta con bitácoras de acceso.

IV. REGISTRO DE INCIDENTES

Si se detecta el acceso al Servidor desde una dirección IP no autorizada, se emite una alerta a la administradora del Sistema de Titulación y, con base en la alerta, se actualizan las reglas de firewall para ser más restrictivos.
En caso de modificación accidental de información contenida en la base de datos, se ha utilizado el respaldo de la base de datos para recuperar la información. Además, se cuenta con la bitácora de los movimientos realizados a través del Sistema de Titulación

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:
¿Cómo las identifica?
Deberá ser personal adscrito a la CAE.

¿Cómo las autentifica?
Identificación visual.
¿Cómo les autoriza el acceso?
Identificación visual y acceso con llave para cerradura mecánica.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:
¿Cómo las identifica?
Únicamente el responsable del área puede ingresar a dicho espacio.
¿Cómo las autentifica?
Identificación visual.
¿Cómo les autoriza el acceso?
El responsable del área es el único que cuenta con la autorización para ingresar.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los usuarios pueden realizar la actualización de sus datos personales una vez que han ingresado al Sistema de Titulación mediante sus credenciales de acceso (usuario y contraseña), en el apartado “Cambios” del menú principal.

VII. PERFILES DE USUARIO Y CONTRASEÑA

1. Modelo de control de acceso: **Basado en roles**.
   Perfiles de usuario y contraseñas en el sistema operativo de red:
   a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
   No.
   b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
   No.
   c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
   No.

2. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
   a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
   Si
   b) ¿Cifra el mencionado software los nombres de usuario y las contraseña cuando los almacena?
   Solo las contraseñas

3. Administración de perfiles de usuario y contraseñas:
   a) ¿Quién da de alta nuevos perfiles?
   La Administradora del Sistema de Titulación
   b) ¿Quién autoriza la creación de nuevos perfiles?
   El Coordinador de Administración Escolar
   c) ¿Se lleva registro de la creación de nuevos perfiles?

Desde el Sistema de Titulación es posible visualizar la creación de perfiles.

4. Acceso remoto al sistema de tratamiento de datos personales:
   a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
   No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.
   b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
   Si
   c) ¿Cómo se evita el acceso remoto no autorizado?
   El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a la administradora del sistema a través de credenciales por cada administrador.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos.
   a) Completos _X_, diferenciales ____ o incrementales ___;
   b) De forma automática _X_, manual,
   c) Periodicidad con los que los realiza: diariamente

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad; Disco duro local y disco duro remoto

3. Cómo y dónde archiva esos medios, Consultar los documentos: Carpeta comprimida en el disco duro del servidor y en una computadora que no se encuentra en la misma red del sistema
4. Quién es el responsable de realizar estas operaciones (al área universitaria o un tercero). La administradora del Sistema de Titulación.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia.

Se cuenta con algunas medidas de seguridad, pero no se tiene desarrollado e instrumentado por completo un plan de contingencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

I. Herramientas y recursos para monitoreo de la protección de datos personales

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos	
Identificador único*	SSA-03-CAE-01

(Nombre del sistema)*	Sistema de Titulación	
Recurso*	**Descripción****	**Control***
Bitácora del sistema	Revisión aleatoria	Se realiza una revisión en horario aleatorio, para validar algún comportamiento inusual.

II. Procedimiento para la revisión de las medidas de seguridad

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos		
Identificador único*:	SSA-03-CAE-01	
(Nombre del sistema)*	Sistema de Titulación	
Recurso*	**Descripción***	**Responsable***
Plan de respaldos de información	Revisión y validación del historial de respaldos del sistema.	Administradora del Sistema de Titulación
Instalar y mantener actualizado el software antimalware	Revisión y actualización de la versión del firewall y de la base de datos.	Administradora del Sistema de Titulación. La duración de la revisión es un día hábil.

III. Resultados de la evaluación y pruebas a las medidas de seguridad

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos	
Identificador único*:	SSA-03-CAE-01
Nombre del sistema*:	Sistema de Titulación

Medida de seguridad*	Resultado de evaluación*	Responsable*
Plan de respaldos de información	Se cuenta con respaldos actualizados de la información del sistema.	Administradora del Sistema de Titulación
Instalar y mantener actualizado el software antimalware	El software opera conforme a lo esperado.	Administradora del Sistema de Titulación

IV. Acciones para la corrección y actualización de las medidas de seguridad

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos		
Identificador único*:	SSA-03-CAE-01	
(Nombre del sistema)*	Sistema de Titulación	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Realizar la renovación periódica del certificado SSL para el dominio donde se encuentra el sistema.	Administradora del Sistema de Titulación

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

I. Programa de a los usuarios del sistema

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos	
Identificador único*:	SSA-03-CAE-01
(Nombre del sistema)*	Sistema de Titulación

Actividad*	Descripción*	Duración*	Cobertura*
Se está implementando un programa de capacitación integral para el manejo del sistema.	Se encuentran en elaboración los manuales de usuario.	Indefinido	Personal administrativo y de apoyo, y responsables de las áreas académicas

II. Programa de difusión de la protección a los datos personales

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos			
Identificador único*:	SSA-03-CAE-01		
(Nombre del sistema)*	Sistema de Titulación		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se cuenta con un programa de difusión de la protección de datos personales

9. MEJORA CONTINUA

I. Actualización y mantenimiento de sistemas de información

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos			
Identificador único*:		SSA-03-CAE-01	
(Nombre del sistema)*		Sistema de Titulación	
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mejora continua con base en nuevos requerimientos y apoyándonos en las nuevas tecnologías.	Actualizar el sistema operativo del host.	Tiempo indefinido	Mejorar el rendimiento y protección del sistema.

II. Actualización y mantenimiento de equipo de cómputo

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos	
Identificador único*:	SSA-03-CAE-01

(Nombre del sistema)*		Sistema de Titulación	
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento de equipos	Reemplazo o integración de nuevos componentes de hardware.	Cuando se presenta una incidencia.	Insuficiente por falta de recursos económicos.

III. Procesos para la conservación, preservación y respaldos de información

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos		
Identificador único*	SSA-03-CAE-01	
(Nombre del sistema)*	Sistema de Titulación	
Proceso*	**Descripción***	**Responsable***
Respaldo de archivos de la base de datos.	Elaboración de copias de seguridad del sistema.	Administrador del Sistema de titulación. Tiempo máximo de ejecución en día: 1

IV. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos		
Identificador único*	SSA-03-CAE-01	
(Nombre del sistema)*	Sistema de Titulación	
Proceso*	**Descripción***	**Responsable***

No se cuenta con proceso de borrado seguro.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con proceso de cancelación del Sistema de Titulación.

Sistema de Servicios Escolares (SSEFI)

El Sistema de Servicios Escolares permite automatizar los servicios que ofrece el área de servicios escolares de la Facultad de Ingeniería a los cuales tienen derecho todos los alumnos de la institución, entre los servicios que ofrece se encuentran:

1. La emisión de constancias automatizadas para alumnos inscritos en el semestre lectivo con validación digital a través de un código QR.
2. Seguimiento a la solicitud de revisión de estudios académica, suspensión de estudios, registro de exámenes extraordinarios y certificado de estudios.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad de Servicios de Cómputo Administrativo (USECAD) - Secretaría de Servicios Académicos	
Identificador único*	SSA-04-CAE-02
(Nombre del sistema)*	Sistema de Servicios Escolares
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, número de cuenta, carrera, asignaturas inscritas en el semestre lectivo (clave y nombre), horario de clases, grupo, claves y nombres de las asignaturas inscritas en el semestre inmediato anterior, datos académicos.
Responsable*:	CAE – FACULTAD DE INGENIERÍA
Nombre*:	**ING. JESÚS VALLEJO GONZÁLEZ**
Cargo*:	**COORDINADOR**
Funciones*:	Coordinar las actividades que se realizan en la CAE.
Obligaciones*:	Mantener, actualizar y resguardar los sistemas que opera la CAE cuidando en todo momento la integridad de la información contenida en ellos.
	Encargados:
(Nombre del Encargado 1*)	**Ing. María Fernanda Hernández Delgadillo**
Cargo*:	Administradora del Sistema de Servicios Escolares
Funciones*:	Administración y mantenimiento del Sistema de Servicios Escolares.
Obligaciones*:	Procurar la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento. Ofrecer asesoría a los nuevos usuarios del Sistema de Servicios Escolares para su correcto funcionamiento.
	Usuarios:
(Perfil del Usuario 1*)	Ing. Leobardo Ramos Vieyra
Cargo*:	Jefe del área de Servicios Escolares
Funciones*:	Autorizar solicitudes de Revisión de Estudios y registrar información académica de los egresados (semestre de ingreso, semestre de egreso, promedio de egreso, etc.) Validar y autorizar constancias escolares.

Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 2*)	María Antonieta Rivas Roque
Cargo*:	Personal de apoyo
Funciones*:	Generación de constancias escolares. Validar requisitos solicitudes de Revisión de Estudios.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 3*)	María Guadalupe Yáñez Lira
Cargo*:	Personal de apoyo
Funciones*:	Generación de constancias escolares. Validar requisitos solicitudes de Revisión de Estudios.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 4*)	Elia Luz Gómez Cristino
Cargo*:	Personal de apoyo
Funciones*:	Generación de constancias escolares. Validar requisitos solicitudes de Revisión de Estudios.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 5*)	Guadalupe Palafox González
Cargo*:	Personal de apoyo
Funciones*:	Generación de constancias escolares. Validar requisitos solicitudes de Revisión de Estudios.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 6*)	Ivett Arianna Campos Escamilla
Cargo*:	Personal de apoyo
Funciones*:	Generación de constancias escolares. Validar requisitos solicitudes de Revisión de Estudios.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 7*)	Karina Tonantzin Paredes Correa
Cargo*:	Personal de apoyo
Funciones*:	Generación de constancias escolares. Validar requisitos solicitudes de Revisión de Estudios.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Perfil del Usuario 8*)	Planta de alumnos
Cargo*:	Alumnos inscritos en el semestre lectivo, alumnos sin derecho a reinscripción y egresados de la Facultad de Ingeniería.
Funciones*:	Generación de constancias de interés propio y generación de solicitudes de Revisión de Estudios, generación de solicitudes de Suspensión de Estudios, generación de solicitudes de Certificado de Estudios, generación de solicitudes registros de Exámenes Extraordinarios ASDRI.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos

	personales.
(Perfil del Usuario 9*)	Ing. Diego Javier Santamaría Nájera
Cargo*:	Asistente de procesos
Funciones*:	Gestionar las solicitudes del trámite de Suspensión de Estudios.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos	
Identificador único*	SSA-04-CAE-02
(Nombre del sistema)*	Sistema de Servicios Escolares
Tipo de soporte:	Electrónico
Descripción:	Base de datos
Características del lugar donde se resguardan los soportes:	Centro de datos de la USECAD.

3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos	
Identificador único*	SSA-04-CAE-02
(Nombre del sistema)*	Sistema de Servicios Escolares
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema de Servicios Escolares no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en una ubicación determinada del sistema en el servidor.

No se cuenta con bitácoras de acceso.

IV. REGISTRO DE INCIDENTES

En caso de modificación accidental de información contenida en la base de datos, se ha utilizado el respaldo de la base de datos para recuperar la información. Además, se cuenta con la bitácora de los movimientos realizados a través del Sistema de Servicios Escolares.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

   Para las personas que acceden a sus instalaciones:
   ¿Cómo las identifica?
   Deberá ser personal adscrito a la CAE.
   ¿Cómo las autentifica?
   Identificación visual.
   ¿Cómo les autoriza el acceso?
   Identificación visual y acceso con llave para cerradura mecánica.

2. **Seguridad perimetral interior**

   Para las personas que acceden a dichos espacios interiores:
   ¿Cómo las identifica?
   Únicamente el responsable del área de la CAE puede ingresar a dicho espacio.
   ¿Cómo las autentifica?
   Identificación visual.
   ¿Cómo les autoriza el acceso?
   El responsable del área es el único que cuenta con la autorización para ingresar.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Si se debe actualizar alguna información para los alumnos, se deberá notificar a la administradora del Sistema de Servicios Escolares, ya que tratándose de datos académicos o trámites administrativos se debe validar que los cambios efectivamente proceden.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso: **Basado en roles y perfiles.**
2. Perfiles de usuario y contraseñas en el sistema operativo de red:
   a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
      No
   b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
      No
   c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
      No

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si.
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo las contraseñas.

4. Administración de perfiles de usuario y contraseñas:
   a) ¿Quién da de alta nuevos perfiles?
   La Administradora del sistema.
   b) ¿Quién autoriza la creación de nuevos perfiles?
   El Coordinador de la CAE.
   c) ¿Se lleva registro de la creación de nuevos perfiles?
   Si, se cuenta incluso con el registro histórico de los perfiles creados y asignados.

5. Acceso remoto al sistema de tratamiento de datos personales:
   a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
   Perfil Administrativo: Si. Alumno, Exalumnos y Egresados: No.
   b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
   Si.
   c) ¿Cómo se evita el acceso remoto no autorizado?
   El acceso remoto al sistema se realiza mediante conexiones VPN habilitadas para los usuarios. Implementación de captcha en el inicio de sesión del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos:
   a) Completos_X_, diferenciales ___ o incrementales___;
   b) De forma automática __X__ o Manual _____,
   c) Periodicidad con que los realiza: De acuerdo con el calendario de procesos de cada semestre definido por la Facultad, al finalizar cada uno de ellos se realiza el respaldo correspondiente

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Disco duro local

3. Cómo y dónde archiva esos medios, *Carpeta comprimida en el disco duro del servidor*

4.Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero):
El Jefe del Área de Infraestructura en Tecnologías de Información.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia.

Se cuenta con algunas medidas de seguridad, pero no se tiene desarrollado e instrumentado por completo un plan de contingencia

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

I. Herramientas y recursos para monitoreo de la protección de datos personales

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos		
Identificador único*	SSA-04-CAE-02	
(Nombre del sistema)*	Sistema de Servicios Escolares	
Recurso*	**Descripción***	**Control***
Herramientas automatizadas	Se hace uso de herramientas de integración continua.	Se realiza una revisión posterior a cada actualización al sistema. Responsables: La Administradora del Sistema de Servicios Escolares. Licencia: asignada para el usuario y de código abierto.
Bitácora del sistema	Revisión aleatoria	Se realiza una revisión en horario aleatorio, para validar algún comportamiento inusual. Responsables: La Administradora del Sistema de Servicios Escolares.

II. Procedimiento para la revisión de las medidas de seguridad

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos		
Identificador único*:	SSA-04-CAE-02	
(Nombre del sistema)*	Sistema de Servicios Escolares	
Recurso*	**Descripción***	**Responsable***
Plan de respaldos de información	Revisión y validación del historial de respaldos del sistema.	Jefe del Área de Infraestructura en Tecnologías de Información de la USECAD. La duración de la revisión es un día hábil

Instalar y mantener actualizado el software antimalware	Revisión y actualización de la versión del firewall y de la base de datos.	Jefe del Área de Infraestructura en Tecnologías de Información de la USECAD. La duración de la revisión es un día hábil
Instalar las actualizaciones de seguridad más recientes disponibles	Revisión y actualizaciones del sistema operativo.	Jefe del Área de Infraestructura en Tecnologías de Información de la USECAD. La duración de la revisión es un día hábil

III. Resultados de la evaluación y pruebas a las medidas de seguridad

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos		
Identificador único*:	SSA-04-CAE-02	
(Nombre del sistema)*	Sistema de Servicios Escolares	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Plan de respaldos de información	Se cuenta con respaldos actualizados de la información del sistema.	Jefe del Área de Infraestructura en Tecnologías de Información de la USECAD. La duración de la revisión es un día hábil
Instalar y mantener actualizado el software antimalware	El software opera conforme a lo esperado.	Jefe del Área de Infraestructura en Tecnologías de Información de la USECAD. La duración de la revisión es un día hábil
Instalar las actualizaciones de seguridad más recientes disponibles	El sistema operativo cuenta con las actualizaciones correspondientes.	Jefe del Área de Infraestructura en Tecnologías de Información de la USECAD. La duración de la revisión es un día hábil

IV. Acciones para la corrección y actualización de las medidas de seguridad

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos	
Identificador único*:	SSA-04-CAE-02

(Nombre del sistema)*	Sistema de Servicios Escolares	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Realizar la renovación periódica del certificado SSL para el dominio donde se encuentra el sistema.	Administradora del Sistema de Titulación

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

I. Programa de capacitación a los usuarios

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos			
Identificador único*:	SSA-04-CAE-02		
(Nombre del sistema)*	Sistema de Servicios Escolares		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Se está implementando un programa de capacitación integral para el manejo del sistema.	Se encuentran en elaboración los manuales de usuario.	Indefinido	La Administradora del Sistema de Servicios Escolares.

II. Programa de difusión de la protección a los datos personales

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos			
Identificador único*:	SSA-04-CAE-02		
(Nombre del sistema)*	Sistema de Servicios Escolares		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se cuenta con un programa de difusión de la protección de datos personales.

9. MEJORA CONTINUA

I. Actualización y mantenimiento de sistemas de información

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos			
Identificador único*	SSA-04-CAE-02		
(Nombre del sistema)*	Sistema de Servicios Escolares		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización y mantenimiento del Servidor.	Actualizar el sistema operativo del host.	Tiempo indefinido	Mejorar el rendimiento y protección del sistema.
Mejora continua con base en nuevos requerimientos.	Implementación de nuevas funcionalidades.	Constante	Mejorar la atención a usuarios.

II. Actualización y mantenimiento de equipo de cómputo

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos			
Identificador único*	SSA-04-CAE-02		
(Nombre del sistema)*	Sistema de Servicios Escolares		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Adquisición de nuevos equipos.	Reemplazo de equipos descontinuados.	Cuando se presenta una incidencia.	Insuficiente por falta de recursos económicos.
Mantenimiento de equipos.	Reemplazo o integración de componentes de hardware.	Cuando se presenta una incidencia.	Insuficiente por falta de recursos económicos.

III. Procesos para la conservación, preservación y respaldos de información

Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos		
Identificador único*:	SSA-04-CAE-02	
(Nombre del sistema)*	Sistema de Servicios Escolares	
Proceso	**Descripción**	**Responsable**
Respaldo de archivos de la base de datos.	Elaboración de copias de seguridad del sistema.	Jefe del Área de Infraestructura en Tecnologías de Información. Tiempo estimado 1 día.
Montaje de respaldo en un ambiente de QA.	Carga de los archivos en ambientes controlados para la elaboración de pruebas.	Jefe del Área de Infraestructura en Tecnologías de Información. Tiempo estimado 1 día.

IV. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

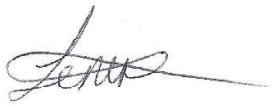
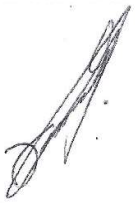
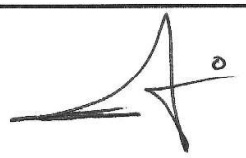
Coordinación de Administración Escolar (CAE)-Secretaría de Servicios Académicos		
Identificador único*	SSA-04-CAE-02	
(Nombre del sistema)*	Sistema de Servicios Escolares	
Proceso*	**Descripción***	**Responsable***

No se cuenta con proceso de borrado seguro. No se han desechado los equipos que han alojado este sistema.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del Sistema de Servicios Escolar.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsables del desarrollo:	Ing. Lenin Guevara López Jefe de Departamento de Procesamiento de datos Tel. 55 5622 0960 lguevaral@ssafi.unam.mx	
	Ing. María Fernanda Hernández Delgadillo Administradora del Sistema Tel. 55 5622 0915 hernandezdelgadillofernanda@gmail.com	
Revisaron:	Ing. Jesús Vallejo González Coordinador de CAE Tel. 55 5622 0919 jesus.vallgo@comunidad.unam.mx	
	M. I. Aurelio Sánchez Vaca Coordinador de USECAD Tel. 55 5622 0960 aurelio@unam.mx	
Autorizó:	M. I. Miguel Figueroa Bustos Secretario de Servicios Académicos Tel. 55 5622 0861 miguelf@unam.mx	
Fecha de aprobación:	25 de agosto de 2022	
Fecha de actualización:		

SECRETARÍA DE APOYO A LA DOCENCIA

ANEXO I: DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

ÍNDICE

SECRETARÍA DE APOYO A LA DOCENCIA

La Secretaría de Apoyo a la Docencia tiene como misión contribuir al cumplimiento de los planes y programas educativos de la Facultad de Ingeniería. Para este fin la secretaría cuenta con las cuatro coordinaciones siguientes:

1. Coordinación de Evaluación Educativa.
2. Coordinación de Programas de Atención Diferenciada para Alumnos.
3. Coordinación del Centro de Docencia.
4. Coordinación de Sistemas de Gestión de la Calidad.

Cada coordinación tiene funciones bien definidas en conjunto se impacta de manera positiva mediante la programación, realización y apoyo de actividades de formación y desarrollo de profesores, de formación integral y diferenciada de los estudiantes, de la implantación de un sistema de gestión de la calidad en los laboratorios de docencia y de la evaluación educativa en general.

La Secretaría de Apoyo a la Docencia busca ser un referente de la Facultad de Ingeniería de la UNAM para instituciones de educación superior, tanto nacionales como internacionales, garantía de la calidad de sus programas educativos, modelo de la formación integral de los alumnos y de los procesos de formación, desarrollo y profesionalización de los docentes, así como de la certificación de los laboratorios de docencia bajo la norma ISO9001:2015.

Sistema TUTORFI

Automatiza los procesos del Programa Institucional de Tutoría de la Facultad de Ingeniería, entre ellos:

- Consultar información de los estudiantes del programa.
- Registro de sesiones grupales.
- Registro de sesiones individuales.
- Registro de disponibilidad de horario para el siguiente semestre.
- Descarga de constancia de actividades.
- Consulta de material de apoyo para las sesiones de tutoría.
- Consulta de datos de su tutor.
- Consulta de información académica.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría de Apoyo a la Docencia (SAD) **Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)**	
Identificador único*	SAD-01-COPADI-01
(Nombre del sistema) *	**Sistema TUTORFI**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, teléfono (particular, celular y/o institucional), correo electrónico (personal o institucional), RFC, CURP, fecha de nacimiento, sexo, tipo de usuario (estudiante, profesor o administrador), número de trabajador (UNAM) o número de cuenta (alumnos y exalumnos UNAM), división, ubicación, grado académico, semblanza, nombramiento.
Responsable*:	Facultad de Ingeniería, SAD-COPADI
Nombre*:	M.I. Juan Carlos Cedeño Vázquez
Cargo*:	Coordinador de la COPADI
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como del contenido, la finalidad y el uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema conprivilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades enel sistema. Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Ing. Enrique Felipe Anastacio
Cargo*:	Ayudante de profesor B, Apoyo a los programas de la COPADI
Funciones*:	Desarrollo, actualización y mantenimiento de software con la finalidad de atender las necesidades de la COPADI, dicha actividad involucra la captación de datos personales de usuarios con la finalidad de recabar información para el Programa Institucional de Tutoría. Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.

Obligaciones*:	Procurar la protección de los datos personales contenidos enel sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento. Cumplir con la Normatividad de la Facultad de Ingeniería.
	Usuarios:
(Nombre del Usuario 1*)	M. en A. María de Lourdes Campos Luna.
Cargo*:	Técnico Académico, Apoyo a los programas de la COPADI.
Funciones*:	Brindar seguimiento de recuperación de contraseña de tutores registrados.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales. Cumplir con la Normatividad de la Facultad de Ingeniería.
(Nombre del Usuario 2*)	MI. Juan Carlos Cedeño Vázquez
Cargo*:	Coordinador de la COPADI
Funciones*:	Análisis de la información recabada por el sistema
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales. Cumplir con la Normatividad de la Facultad de Ingeniería.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único¨*	SAD-01-COPADI-01
(Nombre del sistema *)	**Sistema TutorFI**
Tipo de soporte:*	Electrónico.
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Cubículo cerrado, ingreso exclusivo de personal de la COPADI, dentro de un servidor tipo torre. **Los datos están en el servidor:** **http://copadi.fi-c.unam.mx/**

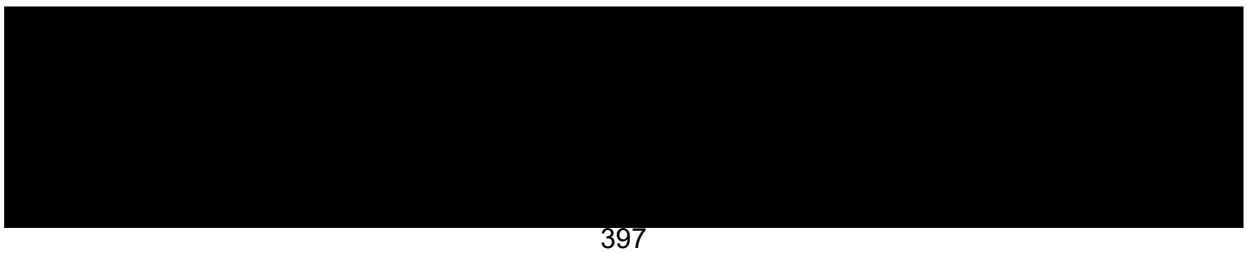
3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 396 a 398.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único*	SAD-01-COPADI-01
(Nombre del sistema)*	**Sistema TutorFI**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante eltraslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Para el Sistema TutorFI se realizan resguardos en unidades externas, mismas que están bajo resguardo del personal de la COPADI y se encuentran almacenadas en el manejador de bases de datos, y encriptados de acuerdo a su propio algoritmo.
Personal:
Ing. Enrique Felipe Anastacio, ayudante de profesor. Desarrollo de sistemas y administrador de bases de datos.
M. en A. María de Lourdes Campos Luna. Técnico Académico. Acceso a base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema en el servidor.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?
No se cuenta con mecanismos de identificación.

c) ¿Cómo les autoriza el acceso?
Como es un departamento cerrado únicamente tiene acceso la persona asignada al cubículo, que cuenta con su llave para las cerraduras.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   No se identifica.
2. ¿Cómo las autentifica?
   No se autentifica.
3. ¿Cómo les autoriza el acceso?
   Como es un departamento cerrado, únicamente tiene acceso la persona asignada al cubículo, que cuenta con su llave para las cerraduras.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se realiza directamente a la base de datos por el responsable del sistema.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

Está basado en roles.

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?
c) ¿Está basado en roles (perfiles) o grupos?
d) ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
   a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
      Si.
   b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
   c) Si
   d) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
      Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
   a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
      Si
   b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
      Solo las contraseñas.

4. Administración de perfiles de usuario y contraseñas:
   a) ¿Quién da de alta nuevos perfiles?
      Los usuarios administradores.
   b) ¿Quién autoriza la creación de nuevos perfiles?
      El coordinador de la COPADI, así como el responsable del programa.
   c) ¿Se lleva registro de la creación de nuevos perfiles?
      Desde el sistema es posible visualizar la creación de perfiles.

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
   No.
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
   Sí, pero no está implementado por seguridad.
c) ¿Cómo se evita el acceso remoto no autorizado?
   - Se cuenta con controles de acceso basados en roles y privilegios.
   - El acceso remoto está deshabilitado tanto en el servidor como en el NAT de la Facultad.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   1. Completos_X_, diferenciales ___ o incrementales___;
   2. De forma automática ____ o Manual __X___,
   3. Periodicidad con que los realiza: _semestral_____

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Disco duro

3. Cómo y dónde archiva esos medios? En una unidad portátil resguardada bajo llave en el cubículo del responsable,

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
El área universitaria.

IX. PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-01-COPADI-01	
(Nombre del sistema)*	**Sistema TutorFI**	
Recurso*	**Descripción***	**Control***
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Las herramientas utilizadas están bajo el control y operaciónde personal de UNICA-SG. Responsables: Personal de la Coordinación de Seguridad de laInformación – UNICA-SG.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar sihubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones. Responsable: Ing. Enrique Felipe Anastacio
Herramientas de Programación	Cross-site scripting (XSS).	Se implementa el XSS en cada apartado que lo requiere para evitar esta vulnerabilidad Responsable: Ing. Enrique Felipe Anastacio

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-01-COPADI-01	
(Nombre del sistema)*	**Sistema TutorFI**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio. a) La duración de la revisión es undía hábil.

Plan de respaldos de información	Revisión y validación del historialde respaldos del sistema	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio La duración de la revisión es undía hábil.
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	El responsable de realizar larevisión es el Ing. Enrique Felipe Anastacio La duración de la revisión es de 3 días hábiles.
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	El responsable de realizar larevisión es el Ing. Enrique Felipe Anastacio La duración de la revisión es undía hábil.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-01-COPADI-01	
(Nombre del sistema)*	**Sistema TutorFI**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistemacuentan con los privilegios correspondientes.	a) El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio
Plan de respaldos de información	Se cuenta con respaldos actualizados de la información del sistema.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio
Instalar las actualizaciones de seguridad más recientesdisponibles.	El sistema operativo cuenta conlas actualizaciones correspondientes.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único*	SAD-01-COPADI-01

(Nombre del sistema)*	Sistema TutorFI	
Medida de seguridad*	**Acciones***	**Responsable***
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la última versiónestable disponible	El responsable de las acciones es el Ing. Enrique Felipe Anastacio

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)			
Identificador único*	SAD-01-COPADI-01		
(Nombre del sistema)*	**Sistema TutorFI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación de la protección de datos personales.	No se cuenta con un programa de capacitación de la protección de datos personales.	No se cuenta con un programa de capacitación de la protección de datos personales.	No se cuenta con un programa de capacitación de la protección de datos personales.

8.2. Programa de difusión de la protección a los datos personales

(Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)			
Identificador único*	SAD-01-COPADI-01		
(Nombre del sistema)*	**Sistema TutorFI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.	No se cuenta con un programa de difusión de la protección de datos personales.	No se cuenta con un programa de difusión de la protección de datos personales.	No se cuenta con un programa de difusión de la protección de datos personales.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único*	SAD-01-COPADI-01

(Nombre del sistema)*	Sistema TutorFI		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de tecnologías de desarrollo	1. Solicitar la actualización del lenguaje de programación en el servidor de pruebas. 2. Actualizar el framework de desarrollo de la aplicación y sus dependencias. 3. Realizar exhaustivas pruebas de funcionalidad en busca de errores, bugs o problemas de compatibilidad como consecuencia de las actualizaciones anteriores. 4. Corregir y/o refactorizar características delsistema. 5. Aplicar modificaciones realizadas en el servidor de pruebas y verificar el correctofuncionamiento. 6. Llevar a cabo todas las actualizacionesanteriores en el servidor de producción.	6 meses	BackEnd de la aplicación: tecnologías de desarrollo.

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)			
Identificador único*	SAD-01-COPADI-01		
(Nombre del sistema)*	**Sistema TutorFI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se han asignado recursos para la actualización del equipo de cómputo	No se han asignado recursos para la actualización del equipo de cómputo	No se han asignado recursos para la actualización del equipo de cómputo	No se han asignado recursos para la actualización del equipo de cómputo

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-01-COPADI-01	
(Nombre del sistema)*	**Sistema TutorFI**	
Proceso*	**Descripción***	**Responsable***
El formato de los archivos de respaldo de informacióncorresponde a informaciónen texto plano.	Se realiza una verificación regular de que el contenido de los respaldos de información es accesible.	Responsable del proceso: Ing.Enrique Felipe Anastacio Tiempo máximo de ejecución endías: 1
El proceso de respaldo de información de la COPADI	El proceso se realiza en la COPADI	Responsable del proceso: Ing.Enrique Felipe Anastacio Tiempo máximo de ejecución endías: 1

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-01-COPADI-01	
(Nombre del sistema)*	**Sistema TutorFI**	
Proceso*	**Descripción***	**Responsable***
No se cuenta con el procedimiento de borrado	No se cuenta con el procedimiento de borrado	No se cuenta con el procedimiento de borrado

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No hay procedimiento para la cancelación de un sistema.

Sistema BITACORAFI (SAD-02-COPADI-02)

En la Facultad de Ingeniería de la UNAM se ha puesto en marcha un sistema en línea, denominado Bitácora FI, en donde los estudiantes de primer ingreso cada semana escriben acerca de sus actividades, vivencias y circunstancias de aprendizaje, a partir de preguntas orientadas a la reflexión constructiva, para propiciar la regulación de su desempeño escolar.

El diseño pedagógico de la Bitácora FI se basa en la pregunta. Incluir preguntas en el proceso de enseñanza puede hacerse con diversos propósitos, en la Bitácora FI la pregunta es una estrategia para enfocar la atención en aspectos relevantes de una tarea, para ayudar a la comprensión de determinado estado de cosas, para valorar experiencias recientes y para estimular la autorregulación.

Cada semana se emiten tres preguntas (preguntas-bitácora) y además se deja un área abierta para que los estudiantes escriban sobre cualquier otro asunto que deseen. La Bitácora FI incluye también una pregunta-encuesta semanal, que se formula principalmente con fines entretenimiento (por ejemplo, cuál es tu programa de televisión favorito, dónde se presenta la Orquesta Sinfónica de Minería, etc.). El estudiante puede contestar esta pregunta-encuesta y consultar la estadística de las respuestas, una vez que haya contestado las tres preguntas-bitácora.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único*	SAD-02-COPADI-02
(Nombre del sistema) *	**Sistema BITACORAFI**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, número de cuenta, carrera, generación, correo electrónico (personal o institucional).
Responsable*:	Facultad de Ingeniería Secretaría de Apoyo a la Docencia Coordinación de Programas de Atención Diferenciada para Alumnos Coordinación de Evaluación Educativa
Nombre*:	M. I. Juan Carlos Cedeño Vázquez
Cargo*:	Coordinador de la COPADI
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema conprivilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades enel sistema. Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Ing. Enrique Felipe Anastacio
Cargo*:	Ayudante de profesor B, Apoyo a los programas de la COPADI

Funciones*:	Realizar el proceso de software con la finalidad de atender las necesidades administrativas de la COPADI, dicha actividad involucra la captación de datos personales de usuarios con la finalidad de brindar apoyo técnico y administrativo a los responsables de procesos de registro a la semana de sus actividades, como lo indican las preguntas
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales. Cumplir con la Normatividad de la Facultad de Ingeniería.
(Nombre del Encargado 2*)	Lic. Griselda Núñez Núñez
Cargo*:	Coordinadora de Evaluación Educativa
Funciones*:	Brindar seguimiento a las respuestas de los estudiantes y actualización a la incorporación de preguntas.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único¨*	SAD-02-COPADI-02
(Nombre del sistema *)	**Sistema BITACORAFI**
Tipo de soporte:*	Electrónico.
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Cubículo cerrado, ingreso exclusivo de personal de la COPADI, dentro de un servidor tipo torre. **Los datos están en el servidor: http://copadi.fi-c.unam.mx/**

3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único*	SAD-02-COPADI-02
(Nombre del sistema)*	**Sistema BITACORAFI**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante eltraslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Para el sistema BITACORAFI se realizan resguardos en unidades externas, mismas que están bajo responsabilidad del personal de la COPADI y se encuentran almacenadas en el manejador de bases de datos, y encriptados de acuerdo a su propio algoritmo.
Personal:
Ing. Enrique Felipe Anastacio, ayudante de profesor. Desarrollo de sistemas y administrados de bases de datos.
M. en A. María de Lourdes Campos Luna. Técnico Académico. Acceso a base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema en el servidor.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación.
b) ¿Cómo las autentifica?
No se cuenta con mecanismos de autentificación.
c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
No se cuenta con mecanismos de identificación.
2. ¿Cómo las autentifica?
No se cuenta con mecanismos de autentificación.
3. ¿Cómo les autoriza el acceso?
El coordinador.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se realiza directamente a la base de datos por el responsable del sistema

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?
c) ¿Está basado en roles (perfiles) o grupos?

Está basado en roles.

d) ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Si

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo las contraseñas.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
El administrador del servidor, con el fin de registrar las preguntas de la semana.

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo las contraseñas

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El administrador del servidor, con el fin de registrar las preguntas de la semana.

b) ¿Quién autoriza la creación de nuevos perfiles?
El coordinador de la COPADI, así como el responsable del programa.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Desde el sistema es posible visualizar la creación de perfiles.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, pero no está implementado por seguridad.

c) ¿Cómo se evita el acceso remoto no autorizado?

- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto está deshabilitado tanto en el servidor como en el NAT de la Facultad.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos _X_, diferenciales ___ o incrementales___;

b) De forma automática ____ o Manual __X___,

c) Periodicidad con que los realiza: _Semestral_____

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:[1] Disco duro externo.

3. Cómo y dónde archiva esos medios, y En una unidad portátil resguardada bajo llave en el cubículo 7.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria.

IX. PLAN DE CONTINGENCIA

No se cuenta con un sitio redundante.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-02-COPADI-02	
(Nombre del sistema)*	**Sistema BITACORAFI**	
Recurso*	**Descripción***	**Control***
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Las herramientas utilizadas están bajo el control y operaciónde personal de UNICA-SG. Responsables: Personal de la Coordinación de Seguridad de laInformación – UNICA-SG.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar sihubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones. Responsable: Ing. Enrique Felipe Anastacio
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales.	Responsables: Personal de la Coordinación de Seguridad de laInformación – UNICA-SG.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-02-COPADI-02	
(Nombre del sistema)*	**Sistema BITACORAFI**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio.	Revisiones periódicas de las cuentas de los usuarios del sistema.	Lo realiza el Ing. Enrique Felipe Anastacio.

Plan de respaldos de información	Revisión y validación del historialde respaldos del sistema.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio La duración de la revisión es undía hábil.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Revisiones periódicas de la horay fecha del sistema.	No se cuenta con una metodología
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	El responsable de realizar larevisión es el Ing. Enrique Felipe Anastacio La duración de la revisión es de 3 días hábiles.
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	El responsable de realizar larevisión es el Ing. Enrique Felipe Anastacio La duración de la revisión es undía hábil.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-02-COPADI-02	
(Nombre del sistema)*	**Sistema BITACORAFI**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistemacuentan con los privilegios correspondientes.	Lo realiza el Ing. Enrique Felipe Anastacio.
Plan de respaldos de información	Se cuenta con respaldos actualizados de la información del sistema.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	No se cuenta con una metodología

Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio
Instalar las actualizaciones de seguridad más recientesdisponibles.	El sistema operativo cuenta conlas actualizaciones correspondientes.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-02-COPADI-02	
(Nombre del sistema)*	**Sistema BITACORAFI**	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Realizar la renovación anual delcertificado SSL para el subdominio donde se encuentra el sistema.	Responsables: Personal de la Coordinación de Seguridad de laFacultad – UNICA-SG. fecha límite de conclusión.
Actualización del lenguaje de programación	Actualización del lenguajede programación	No se cuenta con esta metodología.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)			
Identificador único*	SAD-02-COPADI-02		
(Nombre del sistema)*	**Sistema BITACORAFI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación de la protección de datos personales	No se cuenta con un programa de capacitación de la protección de datos personales	No se cuenta con un programa de capacitación de la protección de datos personales	No se cuenta con un programa de capacitación de la protección de datos personales

8.2. Programa de difusión de la protección a los datos personales

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)			
Identificador único*	SAD-02-COPADI-02		
(Nombre del sistema)*	**Sistema BITACORAFI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.	No se cuenta con un programa de difusión de la protección de datos personales.	No se cuenta con un programa de difusión de la protección de datos personales.	No se cuenta con un programa de difusión de la protección de datos personales.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)			
Identificador único*	SAD-02-COPADI-02		
(Nombre del sistema)*	**Sistema BITACORAFI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de tecnologías de desarrollo	1. Solicitar la actualización del lenguaje deprogramación en el servidor de pruebas. 2. Realizar exhaustivas pruebas de funcionalidad en busca de errores, bugs o problemas de compatibilidad como consecuencia de las actualizaciones anteriores. 3. Actualizar el framework de desarrollo de la aplicación y sus dependencias. 4. Corregir y/o refactorizar características del sistema. 5. Aplicar modificaciones realizadas en el servidor de pruebas y verificar el correcto funcionamiento. 6. Llevar a cabo todas las actualizaciones anteriores en el servidor de producción.	2 semanas	BackEnd de la aplicación: tecnologías de desarrollo

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)			
Identificador único*	SAD-02-COPADI-02		
(Nombre del sistema)*	**Sistema BITACORAFI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se han asignado recursos para la actualización del equipo de cómputo	No se han asignado recursos para la actualización del equipo de cómputo.	No se han asignado recursos para la actualización del equipo de cómputo	No se han asignado recursos para la actualización del equipo de cómputo.

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-02-COPADI-02	
(Nombre del sistema)*	**Sistema BITACORAFI**	
Proceso*	**Descripción***	**Responsable***
El formato de los archivos de respaldo de informacióncorresponde a informaciónen texto plano.	Se realiza una verificación regular de que el contenido de los respaldos de información esaccesible.	Responsable del proceso: Ing.Enrique Felipe Anastacio Tiempo máximo de ejecución endías: 1
El proceso de respaldo de información de la COPADI	El proceso se realiza en la COPADI	Responsable del proceso: Ing.Enrique Felipe Anastacio Tiempo máximo de ejecución endías: 1

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único*	SAD-02-COPADI-02
(Nombre del sistema)*	**Sistema BITACORAFI**

Proceso*	Descripción*	Responsable*
No se cuenta con el procedimiento de borrado	No se cuenta con el procedimiento de borrado	No se cuenta con el procedimiento de borrado

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

Sistema de cursos Intersemestrales COPADI

La Facultad de Ingeniería como impulsora en el uso e implementación de Sistemas de Apoyo Académico-Docente, con el propósito de innovar y seguir a la vanguardia, ofrece apoyo a los alumnos mediante la impartición de diferentes cursos extracurriculares que permiten el mejoramiento en la formación académica de los estudiantes y la integración a la práctica profesional creando en ellos una formación integral.

Dado que en la COPADI las inscripciones a sus cursos se realizaban en las oficinas y de manera manual, se vio la necesidad de agilizar las inscripciones y se desarrolló el sistema de Registro de alumnos, el cual da apoyo a la coordinación mediante el registro vía internet de los estudiantes a los cursos o talleres de su elección, el propósito es llevar un registro detallado de los estudiantes inscritos, que a su vez proveerá información estadística a la misma coordinación para analizar las necesidades educativas y ayudar en el óptimo desempeño escolar.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único*	SAD-03-COPADI-03
(Nombre del sistema) *	**Sistema de cursos Intersemestrales**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, teléfono (particular, celular y/o institucional), correo electrónico (personal o institucional), número de cuenta (alumnos y exalumnos UNAM), semestre y carrera.
Responsable*:	Facultad de Ingeniería, COPADI
Nombre*:	MI. Juan Carlos Cedeño Vázquez
Cargo*:	Coordinador de la COPADI
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema conprivilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema.
	Encargados:
(Nombre del Encargado 1*)	Ing. Enrique Felipe Anastacio
Cargo*:	Ayudante de profesor B, Apoyo a los programas de la COPADI
Funciones*:	Desarrollo, actualización y mantenimiento de software con la finalidad de atender las necesidades de la COPADI, dicha actividad involucra la captación de datos personales de usuarios con la finalidad de recabar información para el Programa Institucional de Tutoría. Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas
Obligaciones*:	Procurar la protección de los datos personales contenidos

	enel sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento.
(Nombre del Encargado 2*)	M.A. María de Lourdes Campos Luna
Cargo*:	Técnico Académico, Apoyo a los programas de la COPADI
Funciones*:	Brindar seguimiento de inscripciones a los cursos
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
	Usuarios:
(Nombre del Usuario 1*)	MI. Juan Carlos Cedeño Vázquez
Cargo*:	Coordinador de la COPADI
Funciones*:	Análisis de la información recabada por el sistema
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 2*)	Lic. Ma. De la Paz González Anaya
Cargo*:	Responsable del programa
Funciones*:	Recibir la información de los estudiantes inscritos
Obligaciones*:	Detallar y compartir listado de alumnos inscritos los ponentes de los cursos

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único¨*	SAD-03-COPADI-03
(Nombre del sistema *)	**Sistema de cursos Intersemestrales**
Tipo de soporte:*	Electrónico.
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Cubículo 7 cerrado, ingreso exclusivo de personal de la COPADI, dentro de un servidor tipo torre. **Los datos están en el servidor: http://copadi.fi-c.unam.mx/**

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 419 a 421.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS
I.TRANSFERENCIAS DE DATOS PERSONALES

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único*	SAD-03-COPADI-03
(Nombre del sistema)*	**Sistema de cursos Intersemestrales**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante eltraslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II.RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Para el Sistema de cursos Intersemestrales se realizan resguardos en unidades externas, mismas que están bajo resguardo del personal de la COPADI y se encuentran almacenadas en el manejador de bases de datos, y encriptados de acuerdo a su propio algoritmo.

Personal:
Ing. Enrique Felipe Anastacio, ayudante de profesor. Desarrollo de sistemas y administrados de bases de datos
M. en A. María de Lourdes Campos Luna. Técnico Académico. Acceso a base de datos

III.BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema en el servidor.

IV.REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
   No se cuenta con mecanismos de identificación.
b) ¿Cómo las autentifica?
   No se cuenta con mecanismos de autentificación.
c) ¿Cómo les autoriza el acceso?
   Como es un departamento cerrado, únicamente tiene acceso la persona asignada al cubículo, que cuenta con su llave para las cerraduras.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   No se identifica
2. ¿Cómo las autenfitica?
   Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
   Como es un departamento cerrado, únicamente tiene acceso la persona asignada al cubículo, que cuenta con su llave para las cerraduras.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se realiza directamente a la base de datos por el responsable del sistema.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

Está basado en roles.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a)¿Cuenta con un sistema operativo de red instalado en sus equipos?
Si
b)¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si
c)¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a)¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si
b)¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo las contraseñas.

4. Administración de perfiles de usuario y contraseñas:
a)¿Quién da de alta nuevos perfiles?
Los usuarios administradores.
b)¿Quién autoriza la creación de nuevos perfiles?
El coordinador de la COPADI, así como el responsable del programa.
c)¿Se lleva registro de la creación de nuevos perfiles?
Desde el servidor es posible visualizar la creación de perfiles.

5. Acceso remoto al sistema de tratamiento de datos personales:
a)¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No.
b)¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, pero no está implementado por seguridad.
c)¿Cómo se evita el acceso remoto no autorizado?
- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto está deshabilitado tanto en el servidor como en el NAT de la Facultad.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1.Señalar si realiza respaldos
1. Completos _X_, diferenciales ___ o incrementales___;
2. De forma automática ____ o Manual __X___,
3. Periodicidad con que los realiza: _Semestral_____

2.El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad[1] Disco duro externo.

3.Cómo y dónde archiva esos medios, y En una unidad portátil resguardada bajo llave en el cubículo 7.

4.Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria.

IX. PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia.

No se cuenta con un sitio redundante.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-03-COPADI-03	
(Nombre del sistema)*	**Sistema de cursos Intersemestrales**	
Recurso*	**Descripción***	**Control***
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Las herramientas utilizadas están bajo el control y operaciónde personal de UNICA-SG. Responsables: Personal de la Coordinación de Seguridad de laInformación – UNICA-SG.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar sihubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones. Responsable: Ing. Enrique Felipe Anastacio
Herramientas de Programación	Cross-site scripting (XSS).	Se implementa el XSS en cada apartado que lo requiere para evitar esta vulnerabilidad Responsable: Ing. Enrique Felipe Anastacio

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-03-COPADI-03	
(Nombre del sistema)*	**Sistema de cursos Intersemestrales**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio La duración de la revisión es un día hábil.
Plan de respaldos de información	Revisión y validación del historialde respaldos del sistema.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio La duración de la revisión es undía hábil.
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	El responsable de realizar larevisión es el Ing. Enrique Felipe Anastacio La duración de la revisión es de 3 días hábiles.
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	El responsable de realizar larevisión es el Ing. Enrique Felipe Anastacio La duración de la revisión es undía hábil.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-03-COPADI-03	
(Nombre del sistema)*	**Sistema de cursos Intersemestrales**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Indique el resultado de la evaluación de la medida de seguridad	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio

Plan de respaldos de información	Se cuenta con respaldos actualizados de la información del sistema.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	El responsable de realizar la revisión es el Ing. Enrique Felipe Anastacio

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-03-COPADI-03	
(Nombre del sistema)*	**Sistema de cursos Intersemestrales**	
Medida de seguridad*	**Acciones***	**Responsable***
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la última versiónestable disponible.	El responsable de las acciones es el Ing. Enrique Felipe Anastacio

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)			
Identificador único*	SAD-03-COPADI-03		
(Nombre del sistema)*	**Sistema de cursos Intersemestrales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación.	No se cuenta con un programa de capacitación.	No se cuenta con un programa de capacitación.	No se cuenta con un programa de capacitación.

8.2 Programa de difusión de la protección a los datos personales

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único*	SAD-03-COPADI-03

(Nombre del sistema)*	Sistema de cursos Intersemestrales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.	No se cuenta con un programa de difusión de la protección de datos personales.	No se cuenta con un programa de difusión de la protección de datos personales.	No se cuenta con un programa de difusión de la protección de datos personales.

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)			
Identificador único*	SAD-03-COPADI-03		
(Nombre del sistema)*	**Sistema de cursos Intersemestrales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de tecnologías de desarrollo	1. Solicitar la actualización del lenguaje deprogramación en el servidor de pruebas. 2. Actualizar el framework de desarrollo de laaplicación y sus dependencias. 3. Realizar exhaustivas pruebas de funcionalidad en busca de errores, bugs o problemas de compatibilidad como consecuencia de las actualizaciones anteriores. 4. Corregir y/o refactorizar características del sistema. 5.Aplicar modificaciones realizadas en elservidor de pruebas y verificar el correcto funcionamiento. 6.Llevar a cabo todas las actualizacionesanteriores en el servidor de producción.	1 mes	BackEnd de la aplicación: tecnologías de desarrollo.

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)			
Identificador único*	SAD-03-COPADI-03		
(Nombre del sistema)*	**Sistema de cursos Intersemestrales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se han asignado recursos para la actualización del equipo de cómputo.	No se han asignado recursos para la actualización del equipo de cómputo.	No se han asignado recursos para la actualización del equipo de cómputo.	No se han asignado recursos para la actualización del equipo de cómputo.

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-03-COPADI-03	
(Nombre del sistema)*	**Sistema de cursos Intersemestrales**	
Proceso*	**Descripción***	**Responsable***
El formato de los archivos de respaldo de informacióncorresponde a informaciónen texto plano.	Se realiza una verificación regular de que el contenido de los respaldos de información esaccesible.	Responsable del proceso: Ing. Enrique Felipe Anastacio Tiempo máximo de ejecución en días: 1
El proceso de respaldo de información de la COPADI	El proceso se realiza en la COPADI	Responsable del proceso: Ing.Enrique Felipe Anastacio Tiempo máximo de ejecución en días: 1

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)		
Identificador único*	SAD-03-COPADI-03	
(Nombre del sistema)*	**Sistema de cursos Intersemestrales**	
Proceso*	**Descripción***	**Responsable***
No se cuenta con el procedimiento de borrado.	No se cuenta con el procedimiento de borrado.	No se cuenta con el procedimiento de borrado.

10 PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

Sistema de Concurso de Cuento (SAD-04-COPADI-04)
El concurso de cuento es una actividad dentro del Programa de Formación Integral de la COPADI cuyo objetivo es fomentar la formación integral, la participación de los estudiantes en una actividad cultural y el desarrollo de la creatividad, característica con la que cuenta la ingeniería en su especificidad.

Cada año la Secretaría de Apoyo a la Docencia a través de la Coordinación de Programas de Atención Diferenciada para Alumnos, (COPADI) invita a estudiantes inscritos en la Facultad de Ingeniería de la UNAM al Concurso de Cuento Gonzalo López de Haro.

El registro de los estudiantes que participan en el concurso se lleva a través de un sistema donde se almacenan la información de los participantes. Este sistema fue desarrollado por la COPADI.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para Alumnos (COPADI)	
Identificador único*	SAD-04-COPADI-04
(Nombre del sistema) *	**Sistema CONCURSO DE CUENTO**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, número de cuenta, carrera, facultad, teléfono (particular, celular y/o institucional), correo electrónico (personal o institucional).
Responsable*:	Facultad de Ingeniería Secretaría de Apoyo a la Docencia Coordinación de Programas de Atención Diferenciada para Alumnos
Nombre*:	M. I. Juan Carlos Cedeño Vázquez
Cargo*:	Coordinador de Programas de Atención Diferenciada para Alumnos
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema conprivilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades enel sistema. Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	M. A. María de Lourdes Campos Luna
Cargo*:	Técnico Académico, Apoyo a los programas de la COPADI
Funciones*:	Actividad donde se reciben datos personales de usuarios

	con la finalidad de brindar soporte técnico para proporcionar la cuenta y contraseña, enviar recordatorios para que envíen los cuentos pendientes de participación, así como entrega de reportes y apoyo a la Mtra. Ana Georgina García y Colomé.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales. Así como la normatividad de la Facultad de Ingeniería.
(Nombre del Encargado 2*)	Ing. Enrique Felipe Anastacio
Cargo*:	Ayudante de profesor B, Apoyo a los programas de la COPADI
Funciones*:	Realizar el proceso de software con la finalidad de atender las necesidades administrativas de la COPADI, dicha actividad involucra la captación de datos personales de usuarios con la finalidad de brindar apoyo técnico.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales. Así como la normatividad de la Facultad de Ingeniería.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para alumnos (COPADI)	
Identificador único¨*	SAD-04-COPADI-04
(Nombre del sistema *)	**Sistema CONCURSO DE CUENTO**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	**Los datos están en el servidor: http://copadi.fi-c.unam.mx/** Cubículo 7, edificio K.

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 430 a 432.
Período de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para alumnos (COPADI)	
Identificador único*	SAD-04-COPADI-04
(Nombre del sistema)*	**Sistema CONCURSO DE CUENTO**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Sistema CONCURSO DE CUENTO no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Se cuenta con un respaldo en disco duro externo almacenado en ubicación del sistema en el servidor.

No se cuenta con un registro.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación.
b)¿Cómo las autentifica?
No se cuenta con mecanismos de autentificación.
c)¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema?

Una puerta con 2 cerraduras y otra puerta con 3 cerraduras, si cuenta con vigilancia las 24 horas por parte del personal de vigilancia de la UNAM.

Para las personas que acceden a dichos espacios interiores:

a) ¿Cómo las identifica?
Hay cámaras externas.
b) ¿Cómo las autentifica?
No se cuenta con mecanismos de identificación.
c) ¿Cómo les autoriza el acceso?
Se accede con llave.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Cada vez que se activa el sistema que es el mes de agosto.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

e) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
f) ¿Es discrecional (matriz de control de acceso)?
g) ¿Está basado en roles (perfiles) o grupos?
h) ¿Está basado en reglas?

Está basado en roles.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Si
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Proporciona un código a cada participante.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo las contraseñas.

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
El sistema da de alta a los nuevos usuarios dependiendo el perfil.
b) ¿Quién autoriza la creación de nuevos perfiles?
El coordinador autoriza la creación de los nuevos perfiles con privilegios administrativos.
c) ¿Se lleva registro de la creación de nuevos perfiles?
Desde el sistema es posible visualizar la creación de perfiles.

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet
Con la finalidad de registrarse al concurso y después para el envío del cuento.
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si
c) ¿Cómo se evita el acceso remoto no autorizado?
Se cuenta con controles de acceso basados en roles y privilegios.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual _X____,
   c) Periodicidad con que los realiza: _Semestral_____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Disco duro externo.
3. Cómo y dónde archiva esos medios, y Consultar los documentos: Cubículo 7.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   el área universitaria

IX. PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para alumnos (COPADI)		
Identificador único*	SAD-04-COPADI-04	
(Nombre del sistema)*	**Sistema CONCURSO DE CUENTO**	
Recurso*	**Descripción***	**Control***

No se cuenta con Herramientas y recursos para monitoreo de la protección de datos personales.
Las herramientas utilizadas están bajo el control y operación de personal de UNICA-SG.
Responsables: Personal de la Coordinación de Seguridad de la Información – UNICA-SG.
Así como la normatividad de la Facultad de Ingeniería.

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para alumnos (COPADI)		
Identificador único*	SAD-04-COPADI-04	
(Nombre del sistema)*	**Sistema CONCURSO DE CUENTO**	
Medida de seguridad*	**Procedimiento***	**Responsable***

No se cuenta con Herramientas y recursos para monitoreo de la protección de datos personales.
Las herramientas utilizadas están bajo el control y operación de personal de UNICA-SG.
Responsables: Personal de la Coordinación de Seguridad de la Información – UNICA-SG.
Así como la normatividad de la Facultad de Ingeniería.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para alumnos (COPADI)		
Identificador único*	SAD-04-COPADI-04	
(Nombre del sistema)*	**Sistema CONCURSO DE CUENTO**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***

No se cuenta con procedimiento para obtener resultados para la revisión de las medidas de seguridad.
Las herramientas utilizadas están bajo el control y operación de personal de UNICA-SG.
Responsables: Personal de la Coordinación de Seguridad de la Información – UNICA-SG.
Así como la normatividad de la Facultad de Ingeniería.

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para alumnos (COPADI)		
Identificador único*	SAD-04-COPADI-04	
(Nombre del sistema)*	**Sistema CONCURSO DE CUENTO**	
Medida de seguridad*	**Acciones***	**Responsable***

No se cuenta con procedimiento para obtener resultados para la revisión de las medidas de seguridad.
Las herramientas utilizadas están bajo el control y operación de personal de UNICA-SG.
Responsables: Personal de la Coordinación de Seguridad de la Información – UNICA-SG.
Así como la normatividad de la Facultad de Ingeniería.

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para alumnos (COPADI)	
Identificador único*	SAD-04-COPADI-04

(Nombre del sistema)*	**Sistema CONCURSO DE CUENTO**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con programa de capacitación	No se cuenta con programa de capacitación	No se cuenta con programa de capacitación	No se cuenta con programa de capacitación

8.2 Programa de difusión de la protección a los datos personales

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para alumnos (COPADI)			
Identificador único*	SAD-04-COPADI-04		
(Nombre del sistema)*	**Sistema CONCURSO DE CUENTO**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con programa de difusión	No se cuenta con programa de difusión	No se cuenta con programa de difusión	No se cuenta con programa de difusión

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para alumnos (COPADI)			
Identificador único*	SAD-04-COPADI-04		
(Nombre del sistema)*	**Sistema CONCURSO DE CUENTO**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con una metodología y/o procedimiento para el mantenimiento y actualización de los sistemas de cómputo	No se cuenta con una metodología y/o procedimiento para el mantenimiento y actualización de los sistemas de cómputo	No se cuenta con una metodología y/o procedimiento para el mantenimiento y actualización de los sistemas de cómputo	No se cuenta con una metodología y/o procedimiento para el mantenimiento y actualización de los sistemas de cómputo

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para alumnos (COPADI)			
Identificador único*	SAD-04-COPADI-04		
(Nombre del sistema)*	**Sistema CONCURSO DE CUENTO**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se han asignado recursos para la actualización del equipo de cómputo	No se han asignado recursos para la actualización del equipo de cómputo	No se han asignado recursos para la actualización del equipo de cómputo	No se han asignado recursos para la actualización del equipo de cómputo

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para alumnos (COPADI)		
Identificador único*	SAD-04-COPADI-04	
(Nombre del sistema)*	**Sistema CONCURSO DE CUENTO**	
Proceso*	**Descripción***	**Responsable***
No hay proceso para la conservación, preservación y respaldos de información.	No hay proceso para la conservación, preservación y respaldos de información.	No hay proceso para la conservación, preservación y respaldos de información.

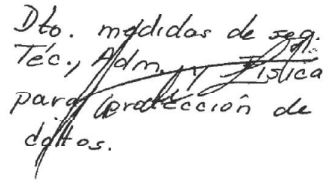
9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría de Apoyo a la Docencia (SAD) Coordinación de Programas de Atención Diferenciada para alumnos (COPADI)		
Identificador único*	SAD-04-COPADI-04	
(Nombre del sistema)*	**Sistema CONCURSO DE CUENTO**	
Proceso*	**Descripción***	**Responsable***
No hay procesos de borrado seguro y disposición final de equipos y componentes informáticos.	No hay procesos de borrado seguro y disposición final de equipos y componentes informáticos.	No hay procesos de borrado seguro y disposición final de equipos y componentes informáticos.

10 PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento para la cancelación del sistema de tratamiento de datos personales.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	María de Lourdes Campos Luna Responsable de cómputo de la COPADI Teléfono UNAM 55 56228201 lulucas@unam.mx	
Revisó:	Juan Carlos Cedeño Vázquez Coordinador de la COPADI Teléfono UNAM 55 56228101 ext 103 jcedevaz@comunidad.unam.mx	
Autorizó:	Claudia Loreto Miranda Secretaria de Apoyo a la Docencia Teléfono UNAM 55 56223004 al 06 cloretomi@gmail.com	
Fecha de aprobación:		17/08/2022
Fecha de actualización:		17/08/2022

COORDINACIÓN DE PLANEACIÓN Y DESARROLLO

ÍNDICE

COORDINACIÓN DE PLANEACIÓN Y DESARROLLO

Objetivo

Colaborar con el Director en instrumentar el proceso de planeación estratégica, desarrollar programas y proyectos institucionales orientados al mejoramiento de la calidad académica, consolidar sistemas eficientes de comunicación e información con la comunidad con el objeto de involucrarlos en el quehacer de la facultad y evaluar sistemática y automatizadamente el desempeño institucional.

Entre sus funciones

- Contribuir a la formulación e implantación de procedimientos y técnicas de planeación-programación-presupuestación que permitan el óptimo desarrollo institucional de la Facultad.
- Coordinar y supervisar la elaboración del plan de desarrollo institucional, de los proyectos y programas anuales.
- Integrar, organizar y difundir la información de carácter estadístico requerida para la formulación de planes y programas de desarrollo de la Facultad.
- Establecer un sistema eficaz y eficiente de seguimiento y evaluación que permita medir la evolución del plan de desarrollo, programas anuales, programas y proyectos estratégicos.
- Proporcionar la información requerida por las distintas áreas de la Facultad.
- Establecer sistemas eficientes de comunicación.
- Mantener una efectiva comunicación interpersonal con todos los involucrados en el proceso de planeación de la entidad.
- Generar e implementar un sistema de información en línea que apoye las tareas en el seguimiento de cada una de las acciones definidas dentro de los grupos de trabajo, para la consecución de metas de los proyectos estratégicos, con base en las necesidades establecidas por la Coordinación.

- Mantener actualizadas las bases de datos de información correspondientes a los proyectos del plan de desarrollo, para que siempre estén a disposición de la instancia que lo requiera.
- Capacitar a los involucrados en el proceso de planeación en el uso del sistema de información, y atender cualquier duda al respecto.
- Brindar soporte técnico para fortalecer los recursos informáticos de la Coordinación de Planeación y Desarrollo.

A continuación se enlistan los sistemas que tratan datos personales dentro de la Coordinación de Planeación y Desarrollo:

- Agenda de las Academias
- Sistema de Información y Estadísticas para Laboratorios de Docencia e Investigación, **SIELDI**
- Registro de Equipos de Cómputo de la Facultad de Ingeniería, RECFI

AGENDA DE LAS ACADEMIAS

Sistema encargado de llevar el control de las reuniones de las distintas Academias de la Facultad de Ingeniería, permitiéndoles a los presidentes programar reuniones, permite dar de alta a sus miembros y administrar a los mismos (modificar y eliminar datos personales), realizar minutas, hacer seguimiento a los acuerdos producto de las reuniones, reprogramar reuniones, enviar por correo las minutas. Así mismo, los jefes de departamento pueden consultar todas las academias pertenecientes a dicho departamento, y a su vez, los jefes de división pueden consultar todos sus departamentos. Adicionalmente también los presidentes pueden editar minutas y bloquear la edición una vez que lo decidan. Por último, en el sistema se pueden consultar minutas, documentos y evidencias de reuniones anteriores.

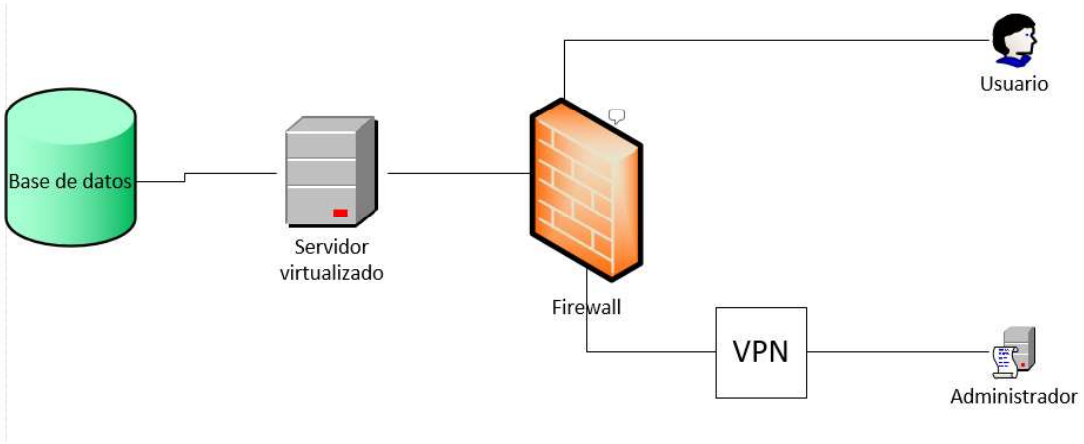
1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Planeación y Desarrollo	
Identificador único*	CPD-01-SIS-01
Nombre del sistema *	Agenda de las Academias
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, correo electrónico/ correo electrónico institucional
Responsable*:	
Nombre*:	**Abigail Serralde Ruiz**
Cargo*:	Coordinadora de Planeación y Desarrollo
Funciones*:	Consulta de datos en el sistema, verificación de la información.
Obligaciones*:	Indicar sobre los cambios de algún tipo de cuenta. Indicar que tipos de cambios o nuevas funcionalidades requiere el sistema.
	Encargados:
(Nombre del Encargado 1*)	Viridiana Vázquez Andrade
Cargo*:	Responsable de Sistemas
Funciones*:	Realizar cambios en el diseño del sistema, desarrollo de nuevas funcionalidades, captura, modificación y eliminación de datos, etc.
Obligaciones*:	Mantener la información de usuarios actualizada, garantizar que el mantenimiento y desarrollo de funcionalidades no pongan en riesgo los datos personales. .
	Usuarios:
(Nombre del Usuario 1*)	Jefes de división
Cargo*:	Jefes de división
Funciones*:	Pueden consultar, modificar y eliminar la información de todas las academias pertenecientes a esa división.
Obligaciones*:	Verificar a nivel división que todos sus departamentos se encuentran en orden y actualizados y llevar a cabo el

	resguardo de los datos personales.
(Nombre del Usuario 2*)	Jefes de departamento
Cargo*:	Jefes de departamento
Funciones*:	Pueden consultar, modificar y eliminar la información de todas las academias pertenecientes a su departamento.
Obligaciones*:	Verificar a nivel departamento que todos sus academias se encuentran en orden y actualizados y llevar a cabo la obligación de resguardar los datos personales.
(Nombre del Usuario 3*)	Presidentes de academias
Cargo*:	Presidentes de academias
Funciones*:	Dar de alta, consultar, modificar y eliminar la información de los miembros de su academia.
Obligaciones*:	Son los encargados de dar de alta nuevos miembros, verificar que la información de nuevos participantes sea verídica, que esté completa y por último resguardar los datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Planeación y Desarrollo	
Identificador único¨*	CPD-01-SIS-01
Nombre del sistema*	Agenda de las Academias
Tipo de soporte: *	Soporte electrónico
Descripción: *	Base de datos relacional en servidor virtualizado
Características del lugar donde se resguardan los soportes: *	Se localiza en una sala especializada donde se almacenan otros servidores virtualizados, pertenecientes a Secretaría General.



3. ANÁLISIS DE RIESGOS

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las paginas 445 a 446.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Coordinación de Planeación y Desarrollo	
Identificador único*	CPD-01-SIS-01
Nombre del sistema*	Agenda de las Academias
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	**a)** Deberá señalar si el envío se realiza a través de mensajero oficial, mensajero privado o correspondencia ordinaria, El envío se realiza a través de mensajero interno de la dependencia. **b)** Deberá precisar si utiliza un sobre o paquete sellado de manera que sea perceptible si fue abierto antes de su entrega; Se utiliza un sobre sellado **c)** Deberá manifestar si el sobre o paquete enviado es entregado en mano al destinatario, previa acreditación con identificación oficial; El sobre se entrega personalmente o se deja con la secretaria del área, quien conoce perfectamente al destinatario. **d)** Deberá indicar si el remitente pide al destinatario que le informe en caso de que reciba el sobre o paquete con señas de apertura; No se solicita tal informe **e)** Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales,

	No se genera acuse de recibo, pero se confirma entrega a través de llamada telefónica **f)** Deberá señalar si el remitente registra la o las transferencias en su bitácora, así como en el Sistema. No se registra ese evento **g)** Indicar si las transferencias de datos personales se formalizaron mediante algún instrumento jurídico No se han formalizado
Transferencias mediante el traslado de soportes electrónicos:	No se llevan a cabo transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	**a)**Deberá precisar si los archivos electrónicos que contienen datos personales son cifrados antes de su envío y proporcionar detalles técnicos del cifrado tales como el tipo de algoritmo utilizado y la longitud de la llave (o clave). No se realiza ningún cifrado previo de la información **b)** Deberá precisar si utiliza un canal de comunicación dedicado o una red privada virtual especificando detalles técnicos relativos al cifrado de dicho canal como la longitud de llave (o clave); en su caso, deberá precisar si para dicho canal utiliza una red pública (como Internet) especificando el protocolo de transferencias protegidas utilizado. No se utiliza vpn **c)** Deberá manifestar si el remitente y/o el destinatario cuentan con dispositivos que faciliten la detección de intrusiones en el canal de comunicaciones. No se cuenta con ello **d)** Sí, para indicarle al remitente que los datos enviados fueron ingresados correctamente Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales y **e)** Deberá señalar si el remitente registra la o las transferencias en su bitácora, así como en el Sistema de tratamiento de datos personales. No se realiza bitácora acerca de los datos enviados **f)** Indicar si las transferencias de datos personales se formalizaron mediante algún instrumento jurídico. No.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema de Agenda de las Academias no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Se encuentra en la base de datos, se guardan el tipo de acciones que realiza, usuario, fecha, hora, se mantienen en una base y se mantienen hasta que se indique por el responsable que pueden borrarse;

IV. REGISTRO DE INCIDENTES:

Formalmente no se cuenta con un procedimiento de atención de incidentes, pero se realizarían las siguientes acciones: La persona que resuelve los incidentes en caso de haberlos es siempre el encargado del sistema. El incidente debe ser reportado al responsable del sistema, mientras el encargado es el encargado de restaurar los datos faltantes. En caso de haber sido un robo de datos personales, se realizarán cambios en las credenciales de acceso al sistema de la cuenta donde se presentó el problema, se notificará a los afectados (personas cuyos datos pueden estar expuestos para que tomen precauciones) por medio de un oficio que debe incluir un acuse de recibido.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuentan con mecanismos de identificación

b) ¿Cómo las autentifica?
No se realiza una autentificación

c) ¿Cómo les autoriza el acceso?
Es libre acceso

Se utiliza un servidor virtualizado fuera de las instalaciones de la CPD, el acceso a las mismas depende del área encargada de los servidores, en este caso es Secretaría General.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El acceso a las instalaciones de la Unidad de Cómputo donde se encuentran los servidores físicamente es limitado, por lo que personas ajenas a dichas instalaciones no tiene acceso.

Se utiliza un servidor virtualizado fuera de las instalaciones de la CPD, el acceso a las mismas depende del área encargada de los servidores, en este caso es Secretaría General

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los presidentes de las academias se pueden comunicar con nosotros para actualizar los datos de sus miembros, enviándolos por correo, o directamente ellos pueden llevar a cabo la actualización de dichos datos desde el sistema.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):
Sí, está basado perfiles

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos? Sólo a nivel Coordinación, pero no con los usuarios del sistema.
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? No aplica.
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? No aplica.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Sí
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? No

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles? El encargado del sistema crea los perfiles.
- **b)** ¿Quién autoriza la creación de nuevos perfiles? El responsable del sistema.
- **c)** ¿Se lleva registro de la creación de nuevos perfiles? Por el momento no se lleva ningún tipo de registro.

5. Acceso remoto al sistema de tratamiento de datos personales:
- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? Sí, los usuarios pueden acceder desde cualquier computadora con conexión a internet.
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? No
- **c)** ¿Cómo se evita el acceso remoto no autorizado?
Se hace uso de una VPN para acceder a la administración del sistema, se realiza cambio de las credenciales de acceso al servidor regularmente.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
- **a)** Completos __X_, diferenciales ___ o incrementales___;
- **b)** De forma automática ____ o Manual __X__,
- **c)** Periodicidad con que los realiza: Diariamente

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Se almacena en un disco duro externo, así como en el mismo servidor, por si alguno de los dos falla.

3. Cómo y dónde archiva esos medios: Una vez almacenados se dejan ahí, por alrededor de un mes, al realizarse chequeos diarios en el volumen de datos es fácilmente saber si por alguna razón se llegaron a eliminar múltiples registros.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
El encargado del Sistema es quien realiza estas operaciones.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   No existe un plan de contingencia formalizado.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No existe un plan de contingencia
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);
   b) Si el sitio es propio o subcontratado con un tercero;
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

   No se cuenta con ninguna clase de sitio redundante.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-01-SIS-01	
Nombre del sistema*	Agenda de las Academias	
Recurso*	**Descripción***	**Control***
Bitácoras	Monitorear bitácoras	Revisión constante de las bitácoras de acceso para saber si hay accesos irregulares y poder corregir las fallas.
Software de escaneo	Pen testing con software	Se realizan pruebas para encontrar puntos vulnerables en el sistema y verificar si las contraseñas son suficientemente seguras.

7.2. Procedimiento para la revisión de las medidas de seguridad

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-01-SIS-01	
Nombre del sistema*	Agenda de las Academias	
Medida de seguridad*	**Procedimiento***	**Responsable***
Actualizaciones de seguridad	Mantener actualizado el sistema operativo con los últimos parches de seguridad para reducir riesgos.	Persona a cargo: Ing. Viridiana Vázquez Andrade 30 min - 1 hora
Plan de respaldos de la información	Checar la consistencia del volumen de datos en caso de pérdidas y restaurar la información perdida.	Persona a cargo: Ing. Viridiana Vázquez Andrade 2 horas
Principio del mínimo privilegio	Checar la posibilidad de reducir permisos innecesarios en los algunos perfiles, logrando garantizar que tengan los permisos necesarios únicamente.	Persona a cargo: Ing. Viridiana Vázquez Andrade 10 horas

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-01-SIS-01	
(Nombre del sistema)*	**Agenda de las Academias**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Actualizaciones de seguridad	El servidor cuenta con todas las actualizaciones posibles hasta la fecha de finalización.	Persona a cargo: Ing. Viridiana Vázquez Andrade 16/08/2022
Plan de respaldos de la información	Se cuentan con los respaldos pertinentes actualizados.	Persona a cargo: Ing. Viridiana Vázquez Andrade 15/08/2022
Principio del mínimo privilegio	Se llegó a la conclusión de que puede ser viable quitar privilegios a algunos tipos de	Persona a cargo: Ing. Viridiana Vázquez Andrade

	perfiles, con el fin de disminuir los riesgos.	14/08/2022

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-01-SIS-01	
Nombre del sistema*	**Agenda de las Academias**	
Medida de seguridad*	**Acciones***	**Responsable***
Integrar algún tipo de malware/antivirus	Adicionar alguna capa extra de protección	Persona a cargo: Ing. Viridiana Vázquez Andrade
Actualizar las versiones de los lenguajes de programación utilizados	Usar la versión más reciente posible de todas las tecnologías utilizadas	Persona a cargo: Ing. Viridiana Vázquez Andrade

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Coordinación de Planeación y Desarrollo			
Identificador único*	CPD-01-SIS-01		
(Nombre del sistema)*	**Agenda de las Academias**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de capacitación			

Por el momento no se tienen contemplado ningún curso de capacitación para el tratamiento seguro de datos personales.

8.2. Programa de difusión de la protección a los datos personales

Coordinación de Planeación y Desarrollo			
Identificador único*	CPD-01-SIS-01		
(Nombre del sistema)*	**Agenda de las Academias**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Esta actividad no se realiza			

Por el momento no se tienen contemplada realizar esta actividad para la difusión de la protección de datos personales.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Coordinación de Planeación y Desarrollo			
Identificador único*	CPD-01-SIS-01		
Nombre del sistema*	**Agenda de las Academias**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del sistema de información	Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término	Mencione los aspectos del sistema de información que son resueltos, total o parcialmente, por la actividad.

9.2. Actualización y mantenimiento de equipo de cómputo

Coordinación de Planeación y Desarrollo			
Identificador único*	CPD-01-SIS-01		
Nombre del sistema*	**Agenda de las Academias**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Solicitar más recursos para el servidor virtualizado al área correspondiente.	Al ser un servidor virtualizado no se tienen tantas restricciones, si el sistema lo requiriera, se podrían solicitar más recursos en memoria, y procesamiento para que el	Cuando se requiera	Esta acción cubriría en su totalidad los requerimientos necesarios para tener actualizado el sistema en cuanto a actualización de equipo

	sistema funcione sin problemas		

9.3. Procesos para la conservación, preservación y respaldos de información

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-01-SIS-01	
Nombre del sistema*	Agenda de las Academias	
Proceso*	**Descripción***	**Responsable***
Los respaldos se encuentran en un disco duro, en un lugar físicamente sin riesgo (seco, con temperatura adecuada),	Se revisa periódicamente el estado del disco para que los respaldos más antiguos no sufran una pérdida si el disco duro comienza a fallar	Persona a cargo: Ing. Viridiana Vázquez Andrade 30 min -1 hora

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-01-SIS-01	
Nombre del sistema*	**Agenda de las Academias**	
Proceso*	**Descripción***	**Responsable***
Los equipos de cómputo se envían a la Secretaría Administrativa	Se realiza un oficio donde se indican los equipos, dichos equipos se hacen llegar a la Secretaría Administrativa	Persona a cargo: • Ing. Viridiana Vázquez Andrade; • Ing. Cesar Osvaldo Pereida Gómez; • O Secretaria perteneciente a la Coordinación. 1 día
Uso de software para borrado seguro	Se utiliza software para realizar borrado seguro para garantizar que los datos no sean posibles recuperarlos si es que se va a desechar el	Persona a cargo: Ing. Viridiana Vázquez Andrade 2 días

	dispositivo de almacenamiento.	

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se dan de baja las credenciales, se crean perfiles que sólo puedan consultar información (no datos personales) y el sistema de consulta prevalecerá hasta que se indique lo contrario. Cuando se llegue a indicar, se procederá al borrado de datos seguros.

A) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
Dejar visible sólo información indispensable para consulta, que no incluya datos personales

B) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES
Una vez que el sistema esté totalmente bloqueado a partir del tiempo que haya seguido funcionando, el encargado deberá realizar el borrado de datos seguro.

C) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Verificar con software que la información borrada no sea recuperada para garantizar que el borrado seguro se llevó a cabo de manera adecuada.

SISTEMA DE INFORMACIÓN Y ESTADÍSTICAS PARA LABORATORIOS DE DOCENCIA E INVESTIGACIÓN, SIELDI

El Sistema de Información y Estadísticas para Laboratorios de Docencia e Investigación, **SIELDI**, ha sido diseñado para facilitar el desarrollo de las actividades de administración de los recursos de los laboratorios, así como la programación del equipamiento y mantenimientos. Tiene como objeto proveer información veraz y oportuna que coadyuve en la toma de decisiones y en el uso más eficiente de los recursos con los que cuenta nuestra institución.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Planeación y Desarrollo	
Identificador único*	CPD-02-RYS-01
(Nombre del sistema)*	**Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre completo, Teléfono, Correo electrónico, ubicación física del lugar de trabajo, grado académico.
Responsable*:	Coordinación de Planeación y Desarrollo
Nombre*:	**Abigail Serralde Ruiz**
Cargo*:	**Coordinadora de Planeación y Desarrollo**
Funciones*:	Responsable de la información dentro del sistema.
Obligaciones*:	Autorización de modificaciones y creación de la información dentro del sistema,
	Encargados:
(Nombre del Encargado 1*)	**Cesar Osvaldo Pereida Gómez**
Cargo*:	**Responsable de redes y servidores**
Funciones*:	Administración general del sistema
Obligaciones*:	Diseño y desarrollo de nuevos módulos, respaldo de las bases de datos, mantenimiento general, creación de usuarios y registro de laboratorios
	Usuarios:
(Nombre del Usuario 1*)	Jefe de División
Cargo*:	Jefe de División
Funciones*:	Máxima autoridad en la toma de decisiones del programa en su División
Obligaciones*:	Revisar y autorizar el programa de Equipamiento y Mantenimiento
(Nombre del Usuario 2*)	Jefe de Departamento
Cargo*:	Jefe de Departamento
Funciones*:	Enlace entre los laboratorios de la División Académica y el Jefe de División
Obligaciones*:	Revisar, Informar y Acordar con el Jefe de División las necesidades de los laboratorios

(Nombre del Usuario 3*)	Responsable de laboratorio
Cargo*:	Responsable de Laboratorio
Funciones*:	Administración general de la cuenta asociada a los laboratorios adscritos
Obligaciones*:	Determinar e ingresar el registro de las necesidades del laboratorio en el marco del Programa de Equipamiento y Mantenimiento de Laboratorios
(Nombre del Usuario 4*)	Miembro del Comité de Laboratorios
Cargo*:	Representante de la División ante el Comité de Laboratorios
Funciones*:	Ser el enlace entre el Comité de Laboratorios y el Jefe de División y los responsables de los laboratorios de la División a la que representan.
Obligaciones*:	Informar al Jefe de División de los acuerdos llegados en el Comité de Laboratorios y comunicar las necesidades de la División al Comité.
(Nombre del Usuario 5*)	Usuarios específicos
Cargo*:	Usuario
Funciones*:	Consulta de información que depende del área a la que pertenece
Obligaciones*:	Consultar, informar y analizar información que emana del sistema.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Planeación y Desarrollo	
Identificador único¨*	CPD-02-RYS-01
(Nombre del sistema)*	**Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI**
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos relacional
Características del lugar donde se resguardan los soportes: *	Servidor dentro de la Coordinación

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 457 a 458.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Coordinación de Planeación y Desarrollo	
Identificador único*	CPD-02-RYS-01

(Nombre del sistema)*	**Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se lleva a cabo ningún tipo de transferencia de datos personales.
Transferencias mediante el traslado de soportes electrónicos:	No se lleva a cabo ningún tipo de transferencia de datos personales.
Transferencias mediante el traslado sobre redes electrónicas:	No se lleva a cabo ningún tipo de transferencia de datos personales.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No se resguardan datos personales con soportes físicos por lo que no hay alguien responsable del resguardo.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Se registra en una bitácora interna del sistema los ingresos y las actividades en general que realiza el usuario que se conectó, incluyendo fecha y hora.

IV. REGISTRO DE INCIDENTES:

No se ha presentado ningún incidente de gravedad en el sistema por lo que no se tiene registro de ello.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

El acceso a los edificios está controlado por los trabajadores de vigilancia UNAM, aplicando los protocolos de acceso a instalaciones

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

La oficina es pequeña, por lo que no se requiere un control de acceso complejo

1. ¿Cómo las identifica? Preguntas directas, la mayoría de las personas que entran son conocidos.
2. ¿Cómo las autentifica? Muy rara vez es necesaria una autenticación
3. ¿Cómo les autoriza el acceso? De palabra

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se solicita semestralmente a los representantes ante el Comité de Operación y Seguimiento de Laboratorios que revisen la información y en caso de requerir actualización se hace la solicitud a la Coordinación de Planeación. Para el caso de la creación de cuentas de usuario se hace el mismo procedimiento.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? Sí
- **b)** ¿Es discrecional (matriz de control de acceso)? Sí
- **c)** ¿Está basado en roles (perfiles) o grupos? Sí
- **d)** ¿Está basado en reglas? Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos? Sí
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Sí
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Sí

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Sí
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Sí, sólo las contraseñas

4. Administración de perfiles de usuario y contraseñas:

- **a)** ¿Quién da de alta nuevos perfiles? El administrador del sistema
- **b)** ¿Quién autoriza la creación de nuevos perfiles? La Coordinadora
- **c)** ¿Se lleva registro de la creación de nuevos perfiles? Sí

5. Acceso remoto al sistema de tratamiento de datos personales:

- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? Sí
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Sí
- **c)** ¿Cómo se evita el acceso remoto no autorizado? Acceso por protocolos SSH para el caso de los mantenimientos y al sistema por medio de usuario y contraseña.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

- **d)** Completos _x_, diferenciales ___ o incrementales___;
- **e)** De forma automática ____ o Manual _x_,
- **f)** Periodicidad con que los realiza: _Semanal__

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Discos duros externos
3. Cómo y dónde archiva esos medios,
   Bajo llave en un estante
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Se realiza por parte de la Coordinación

IX. PLAN DE CONTINGENCIA

No se tiene un plan de contingencia como tal, sin embargo sí se cuenta con los respaldos listos para poder restaurarse a la brevedad.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-02-RYS-01	
(Nombre del sistema)*	Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI	
Recurso*	**Descripción***	**Control***
No se utilizan herramientas específicas	Se realizan revisiones aleatorias	No se utiliza una herramienta específica.

7.2. Procedimiento para la revisión de las medidas de seguridad

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-02-RYS-01	
(Nombre del sistema)*	**Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Actualización de los parches de seguridad.	Se comprueban las actualizaciones del SO periódicamente.	a) César Osvaldo Pereida Gómez b) Mensualmente, a menos que surja un boletín de seguridad.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-02-RYS-01	
(Nombre del sistema)*	**Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Pruebas generales de intentos de intrusión	Satisfactorio	a) Cesar Osvaldo Pereida Gómez b) Julio 2022.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-02-RYS-01	
(Nombre del sistema)*	**Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI**	
Medida de seguridad*	**Acciones***	**Responsable***
Monitoreo de nuevas actualizaciones.	a) Instalación de parches de seguridad en el sistema. b) Revisión de boletines de seguridad de acuerdo a la versión del sistema operativo.	Indicar: a) Cesar Osvaldo Pereida Gómez b) Un día.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Coordinación de Planeación y Desarrollo			
Identificador único*	CPD-02-RYS-01		
(Nombre del sistema)*	**Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No existe una capacitación formal	Aprendizaje autodidacta	2 horas semanales	Administrador del sistema

8.2. Programa de difusión de la protección a los datos personales

Coordinación de Planeación y Desarrollo			
Identificador único*	CPD-02-RYS-01		
(Nombre del sistema)*	**Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Sin difusión			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Coordinación de Planeación y Desarrollo			
Identificador único*	CPD-02-RYS-01		
(Nombre del sistema)*	**Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento general del sistema	Mantener el sistema en buen funcionamiento, con la información actualizada	Constante durante el semestre	Información actualizada y consistente

9.2. Actualización y mantenimiento de equipo de cómputo

Coordinación de Planeación y Desarrollo			
Identificador único*	CPD-02-RYS-01		
(Nombre del sistema)*	**Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento general del equipo de cómputo	Limpieza a nivel de hardware y también actualización del	Una semana, semestralmente	Se resuelven en su totalidad los aspectos relacionados con el desempeño del equipo.

	software del equipo.		

9.3. Procesos para la conservación, preservación y respaldos de información

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-02-RYS-01	
(Nombre del sistema)*	**Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI**	
Proceso*	**Descripción***	**Responsable***
Respaldo del Sistema	Cada semana se realiza un respaldo de la totalidad del sistema, se comprime y se guarda en una unidad externa. Los respaldos son adjuntos	Indicar: a) Cesar Osvaldo Pereida Gómez b) Un día
Respaldo de la base de datos del sistema	Cada semana se realiza el respaldo de la base de datos en formato de texto plano, se comprime y se resguarda en una unidad externa.	a) Cesar Osvaldo Pereida Gómez b) Un día

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-02-RYS-01	
(Nombre del sistema)*	**Sistema de Información y Estadística para Laboratorios de Docencia e Investigación, SIELDI**	
Proceso*	**Descripción***	**Responsable***
Al momento no se ha cambiado de equipo, por lo que la disposición no ha sido necesaria		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un Sistema próximo a cancelarse.

REGISTRO DE EQUIPOS DE CÓMPUTO

El sistema de Registro de Equipos de Cómputo tiene la función de facilitar la gestión de inventarios de las diferentes áreas y la realización del censo de cómputo anual de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Planeación de Desarrollo	
Identificador único*	CPD-03-RYS-02
(Nombre del sistema)*	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre del responsable del área, correo electrónico, teléfono y ubicación del área responsable.
Responsable*:	Coordinación de Planeación y Desarrollo.
Nombre*:	**Abigail Serralde Ruiz**
Cargo*:	**Coordinadora**
Funciones*:	Responsable de la información del sistema
Obligaciones*:	Decidir a qué usuarios se les da acceso al sistema con privilegios administrativos. Autorizar nuevas funcionalidades del sistema.
	Encargados:
(Nombre del Encargado 1*)	César Osvaldo Pereida Gómez
Cargo*:	**Responsable de redes y servidores**
Funciones*:	Administración del sistema
Obligaciones*:	Diseño e implementación de nuevos requerimientos, así como administración, respaldo de las bases de datos Además creación de usuarios y laboratorios.
(Nombre del Encargado 2*)	Ing. Luciralia Hernández Hernández
Cargo*:	**Apoyo en el área de redes y servidores**
Funciones*:	Diseño y desarrollo de nuevas funcionalidades del sistema.
Obligaciones*:	Diseño e implementación de nuevos requerimientos, así como administración y respaldo de las bases de datos Además creación de usuarios y áreas.
	Usuarios:
(Nombre del Usuario 1*)	Nombre del usuario del jefe del departamento correspondiente
Cargo*:	Jefe de departamento
Funciones*:	Concentrar la información estadística sobre la infraestructura de cómputo, así como necesidades de equipamiento de cómputo de la cada una de sus áreas adscritas.
Obligaciones*:	Actualizar el inventario de equipos de cómputo de las áreas adscritas a su departamento Revisar y supervisar los censos de equipo registrados en su departamento, así como en cada área del departamento. Registrar órdenes de compra para equipos de cómputo.

(Nombre del Usuario 2*)	Nombre del usuario miembro del Comité Asesor de Cómputo de la Facultad de Ingeniería correspondiente.
Cargo*:	Miembro del Comité Asesor de Cómputo de la Facultad de Ingeniería.
Funciones*:	Concentrar la información estadística sobre la infraestructura de cómputo, así como necesidades de equipamiento de cómputo de la Facultad de Ingeniería.
Obligaciones*:	Revisar los requerimientos de equipamiento de cada división. Revisar los censos de equipo de cómputo de la facultad de Ingeniería, así como por cada división.
(Nombre del Usuario 3*)	Nombre del usuario encargado de cada área correspondiente.
Cargo*:	Encargado de área.
Funciones*:	Revisar la información de los equipos de cómputo a su cargo.
Obligaciones*:	Revisar el correcto registro del equipo de cómputo a su cargo.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Planeación y Desarrollo	
Identificador único¨*	CPD-03-RYS-02)
(Nombre del sistema)*	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)**
Tipo de soporte: *	Electrónico
Descripción: *	Servidor y la base de datos
Características del lugar donde se resguardan los soportes: *	Se cuenta con un respaldo en un servidor de pruebas en las instalaciones de la Coordinación; así como en herramienta alterna.

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 466 a 467.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Coordinación de Planeación o Desarrollo	
Identificador único*	CPD-03-RYS-02
Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)**
TRANSFERENCIAS DE DATOS PERSONALES	

Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No se resguardan datos personales con soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El sistema cuenta con una bitácora interna que registra los ingresos y las actividades en general que realiza el usuario, incluyendo fecha y hora.

IV. REGISTRO DE INCIDENTES:

No hay incidentes registrados.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

El acceso a los edificios está controlado por los trabajadores de vigilancia UNAM, aplicando los protocolos de seguridad para el ingreso a las instalaciones

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?
No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

La oficina es pequeña, por lo que no se requiere un control de acceso complejo

1. ¿Cómo las identifica? Preguntas directas, la mayoría de las personas que entran son conocidos.
2. ¿Cómo las autentifica? Muy rara vez es necesaria una autenticación
3. ¿Cómo les autoriza el acceso? De palabra

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El sistema proporciona la opción de editar los datos personales de los responsables de área. En caso de solicitar la creación de una cuenta y contraseña de usuario de ingreso al sistema se solicita a los encargados del área realizar la petición a la Coordinación de Planeación y Desarrollo.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:
Es obligatorio usuario y contraseña que se le proporcionó como miembro del Comité Asesor de Cómputo de la Facultad de Ingeniería.
Está basado en roles

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? Si
b) ¿Es discrecional (matriz de control de acceso)? Si
c) ¿Está basado en roles (perfiles) o grupos? Si
d) ¿Está basado en reglas? Si

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Solo cifra contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si, solo las contraseñas se cifran

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles? El administrador del sistema
b) ¿Quién autoriza la creación de nuevos perfiles? La coordinadora
c) ¿Se lleva registro de la creación de nuevos perfiles? Si, además se envía un oficio con usuario y contraseña a cada responsable del área.

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Si
c) ¿Cómo se evita el acceso remoto no autorizado? Para realizar mantenimiento y actualizaciones se utilizan herramientas con credenciales autorizadas, para el acceso al sistema se controla a través de usuario y contraseña

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
    a) Completos_X_, diferenciales ___ o incrementales___;
    b) De forma automática ____ o Manual ___X__,
    c) Periodicidad con que los realiza: ___cada semestre____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Se respalda en disco duro
3. Cómo y dónde archiva esos medios, en el servidor local, además en una cuenta de administrador de archivos ambos medios con usuario y contraseña.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   El área universitaria

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   No se tiene, sin embargo está en desarrollo uno debido a que en algún momento se requirió.
2. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   No como tal, se cuenta con la imagen del sistema y el respaldo de la base de datos.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-03-RYS-02	
(Nombre del sistema)*	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)**	
Recurso*	**Descripción***	**Control***
No se utilizan herramientas específicas	Revisiones aleatorias	No se utiliza una herramienta específica.

7.2. Procedimiento para la revisión de las medidas de seguridad

Coordinación de Planeación y Desarrollo	
Identificador único*	CPD-03-RYS-02
(Nombre del sistema)*	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)**

Medida de seguridad*	Procedimiento*	Responsable*
Principio de menor privilegio	Revisiones de las cuentas de los usuarios del sistema.	Luciralia Hernández Hernández La duración de la revisión es un día hábil
Respaldos de información	Revisión y validación de los respaldos del sistema	Luciralia Hernández Hernández La duración de la revisión es un día hábil
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus	Viridiana Vázquez Andrade La duración de la revisión es un día hábil

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-03-RYS-02	
(Nombre del sistema)*	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Prueba de accesos no autorizados	Satisfactorio	Luciralia Hernández Hernández
Instalar las actualizaciones de seguridad más recientes disponibles	Se realizó la última actualización del software	Viridiana Vázquez Andrade
Respaldos de información	Se realizó el último respaldo de la base de datos	César Osvaldo Pereida Gómez Fecha de realización en:julio de 2022

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-03-RYS-02	
(Nombre del sistema)*	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)**	
Medida de seguridad*	**Acciones***	**Responsable***
Monitoreo de nuevas actualizaciones.	a) Instalación de parches de seguridad en el sistema.	Indicar: a) Cesar Osvaldo Pereida Gómez

	b) Revisión de boletines de seguridad de acuerdo a la versión del sistema operativo.	b) Un día.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Coordinación de Planeación y Desarrollo*			
Identificador único*	CPD-03-RYS-02		
(Nombre del sistema)*	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No existe capacitación	Autodidacta	2 horas semanales	Gestión del sistema

8.2. Programa de difusión de la protección a los datos personales

Coordinación de Planeación y Desarrollo			
Identificador único*	CPD-03-RYS-02		
(Nombre del sistema)*	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)**)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No existe			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Coordinación de Planeación y Desarrollo	
Identificador único*	CPD-03-RYS-02
(Nombre del sistema)*	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI**)

Actividad*	Descripción*	Duración*	Cobertura*
Mantenimiento general del sistema	Mantener el sistema con un funcionamiento óptimo.	Continuamente durante el semestre	Información consistente.
Actualización del sistema	Realización de las nuevas funcionalidades del sistema.	De manera continua, cuando se solicitan nuevas funcionalidades	Actualización de nuevas funcionalidades en el sistema.

9.2. Actualización y mantenimiento de equipo de cómputo

Coordinación de Planeación y Desarrollo			
Identificador único*	CPD-03-RYS-02		
(Nombre del sistema)*	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento del equipo de cómputo.	Actualización del software del equipo	Dos días	Funcionamiento del equipo.

9.3. Procesos para la conservación, preservación y respaldos de información

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-03-RYS-02	
(Nombre del sistema)*	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)**	
Proceso*	**Descripción***	**Responsable***
Respaldo del sistema	Se realizan diferentes respaldos cada vez al finalizar cada funcionalidad, se almacena en el servidor local, además en el repositorio del administrador de archivos y en unidades externas.	Indicar: a) Luciralia Hernández Hernández b) Un día

Respaldo de las bases de datos	Cada semestre se realiza un respaldo de la información, se almacena en el servidor local y en unidades externas..	a) Luciralia Hernández Hernández b) Un día

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Coordinación de Planeación y Desarrollo		
Identificador único*	CPD-03-RYS-02	
(Nombre del sistema)*	**Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)**	
Proceso*	**Descripción***	**Responsable***
No se ha cambiado el equipo.		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No hay sistemas que vayan a ser cancelados.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Cesar Osvaldo Pereida Gómez, Técnico Académico, 56223232, pereida@unam.mx	 Cesar Osvaldo Pereida Gómez
Revisó:	Abigail Serralde Ruiz, Coordinadora de Planeación y Desarrollo, 56223232, abigail@ingenieria.unam.mx	 Abigail Serralde Ruiz
Autorizó:	Abigail Serralde Ruiz, Coordinadora de Planeación y Desarrollo, 56223232, abigail@ingenieria.unam.mx	 Abigail Serralde Ruiz
Fecha de aprobación:	16 de agosto de 2022	
Fecha de actualización:	16 de agosto de 2022	

DIVISIÓN DE CIENCIAS BÁSICAS

ÍNDICE

DIVISIÓN DE CIENCIAS BÁSICAS

La División de Ciencias Básicas (DCB) es una de las cinco Divisiones académicas que conforman a la Facultad de Ingeniería de la UNAM, con sede en Ciudad Universitaria, Cd. De México. Se ubica en el conjunto sur de la Facultad de Ingeniería (Circuito exterior sin número)

Misión:

> “Desarrollar en los estudiantes de la Facultad de Ingeniería una madurez intelectual que les permita contar con una alta capacidad de análisis y síntesis para formular y resolver problemas relacionados con su área de trabajo. Esta madurez y capacidades están basadas en un entendimiento profundo de fenómenos físicos y químicos y de su conceptualización matemática, con lo cual se logra un dominio del conocimiento completo. Para ello, la formación básica de los estudiantes incluye la asimilación de conocimientos científicos y técnicos por medio del dominio de herramientas básicas matemáticas y su aplicación a las diferentes especialidades de la ingeniería.”

Algunos de sus funciones son:

- Impartir cursos de las asignaturas de ciencias básicas contenidas en los planes de estudio de todas las carreras que se imparten en la Facultad de Ingeniería.
- Coordinar y supervisar el cumplimiento de los programas de las asignaturas que corresponden a la División y proporcionar el material de apoyo y las condiciones adecuadas para la ejecución de dichos programas.
- Revisar y actualizar los programas de las asignaturas correspondientes a la División, atendiendo las propuestas y sugerencias de los profesores que las imparten.

- Desarrollar actividades tendientes a la superación y actualización de su personal académico con el objetivo de mejorar el proceso enseñanza-aprendizaje, atendiendo a las políticas académicas de la Facultad.
- Mantener y fomentar las relaciones de intercambio con dependencias universitarias e instituciones de educación media superior, con el fin de realizar acciones que fortalezcan la orientación vocacional y los conocimientos antecedentes de los estudiantes que ingresan a la Facultad.
- Promover la realización de conferencias, seminarios, exposiciones, cursos y demás actividades tendientes a la difusión científica, tecnológica y humanística.
- Establecer, coordinar y controlar los programas de servicio social que los alumnos de diversas carreras desarrollan en la División.

Para cumplir con sus funciones, la DCB, a través de su **Coordinación de Cómputo**, ha desarrollado una serie de sistemas de cómputo que apoyan a todas las áreas a desarrollar eficientemente sus laborares, proporcionado acceso ágil, oportuno y confiable a la información relacionada con la programación de actividades académicas semestrales, tales como programación de grupos, asesorías, talleres, conferencias, cursos intersemestrales, etc; así como a la información relacionada con los docentes que las imparten, su trayectoria docente y procesos de solicitudes de contratación; además de los datos estrictamente necesarios para el registro de los estudiantes que participan en las citadas actividades.

SISTEMA INTEGRAL DE INFORMACIÓN DE LA DCB

Con el objetivo de mantener en un único sistema de base de datos toda la información de las actividades semestrales de la DCB y de los académicos adscritos a ella se tiene una base de datos relacional a la que se accede a través de un sistema con diversos módulos, algunos de ellos con via web y otros vía ODBC.

Entre los módulos se cuentan:

- Captura y consulta de la programación semestral de actividades
- Captura y consulta de horarios de puerta de los docentes
- Captura y consulta de cursos extracurriculares para alumnos y docentes y sus correspondientes constancias de participación
- Captura y consulta de Currículum Vitae de los docentes
- Captura de solicitudes al Consejo Técnico para la contratación de docentes.
- Captura de datos para Incorporación de materiales didácticos al repositorio CERAFIN

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

DCB-01-CCO-01 SII-DCB

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único*	DCB-01-CCO-01
(Nombre del sistema) *	**Sistema Integral de Información de la DCB**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, nacionalidad, CURP, RFC, Cédula profesional, número de trabajador UNAM, domicilio, números telefónicos, correo electrónico (personal o institucional), fecha de nacimiento, edad, trayectoria educativa, títulos, certificados, reconocimientos, género.
Responsable*:	
Nombre*:	Mtra. Irene Patricia Valdez y Alfaro
Cargo*:	Coordinadora de Cómputo en la DCB
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:
Nombre del Encargado 1*	Ariel Jiménez Juárez
Cargo*:	Ayudante de Profesor.
Funciones*:	- Desarrollo de software. - Análisis, planeación y programación de funcionalidades del sistema. - Análisis y mantenimiento de base de datos.
Obligaciones*:	- Procurar la protección de datos personales contenidos

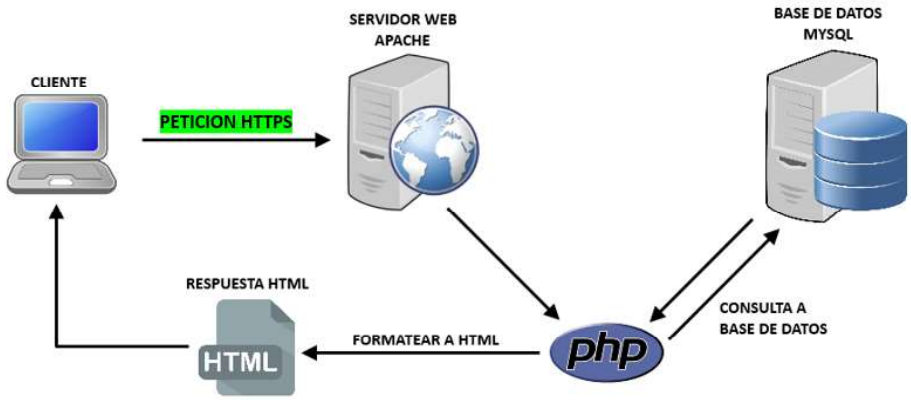
	en el sistema con estrategias y mecanismos de seguridad en el desarrollo y mantenimiento. - Accesos al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, así como las diferentes funcionalidades de los módulos del sistema.
(Nombre del Encargado 2*)	M. I. Janete Mejía Jiménez
Cargo*:	Técnico Académico
Funciones*:	Administración del servidor. Administración del sistema de bases de datos. Dar de alta y controlar acceso de usuarios de las bases de datos.
Obligaciones*:	Administrar el servidor que aloja al sistema, administrar las bases de datos del servidor. Procurar la protección de datos contenidos en el servidor con estrategias y mecanismos de seguridad. Mantener un registro de usuarios con acceso al servidor y a las bases de datos (nombre de la persona, nombre de usuario, contraseñas otorgadas y privilegios). Realizar el monitoreo de incidentes en el servidor y aplicar las políticas de seguridad pertinentes para evitar ataques. Registrar y reportar incidentes de seguridad.
	Usuarios:
(Nombre del Usuario 1*)	Cuerpo de funcionarios de la División de Ciencias Básicas
Cargo*:	Jefe de División, Secretarios Académico y Auxiliar, Coordinadores, Jefes de Departamento, Jefes de Sección.
Funciones*:	Capturar la programación semestral de actividades. Consultar datos personales de los docentes adscritos a la División de Ciencias Básicas con el fin de programar actividades.
Obligaciones*:	Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Usuario 2*)	Margarita Cárdenas Pérez
Cargo*:	Asistente de procesos
Funciones*:	Elaborar las solicitudes de contratación de personal docente que se asigna a las diversas actividades programadas. Consultar datos personales de los docentes adscritos a la División de Ciencias Básicas con el fin de realizar procesos y reportes que solicitan otras instancias y de elaborar solicitudes de contratación.
Obligaciones*:	Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Usuario 3*)	Gloria Guadalupe Martínez Rosas
Cargo*:	Técnico Académico
Funciones*:	Capturar y dar mantenimiento a la información relacionada

	con las actividades semestrales. Consultar datos personales de los docentes adscritos a la División de Ciencias Básicas con el fin de realizar procesos y reportes que solicitan otras instancias
Obligaciones*:	Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Usuario 4*)	Ana María Vieyra Ávila
Cargo*:	Técnico Académico
Funciones*:	Revisar currículum y validar grados académicos de los docentes en función de los documentos probatorios incorporados al sistema. elaborar constancias de participación en eventos académicos, otras relativas al apoyo a la Secretaría Académica.
Obligaciones*:	Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Usuario 5*)	Personal docente en general de la División de Ciencias Básicas
Cargo*:	Profesores de Carrera, Técnicos Académicos, Ayudantes de Profesor, Funcionarios.
Funciones*:	Consultar carga académica asignada al semestre. Para personal de tiempo completo, capturar horario de puerta. Capturar y mantener actualizado su currículum y copias de documentos probatorios del mismo.
Obligaciones*:	Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

DCB-01-CCO-01

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único¨*	DCB-01-CCO-01
(Nombre del sistema *)	Sistema Integral de Información de la DCB
Tipo de soporte:*	Electrónico.
Descripción:*	Base de datos relacional con interfaz de acceso por web y herramienta de administración de bases de datos.

Características del lugar donde se resguardan los soportes:*	Alojamiento en un servidor dedicado para el propio sistema. 

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 482 a 483.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

6.I.- TRANSFERENCIAS DE DATOS PERSONALES

DCB-01-CCO-01

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único*	DCB-01-CCO-01
(Nombre del sistema)*	**Sistema Integral de Información de la DCB**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza transferencia de datos personales en soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realiza transferencia de datos en soportes electrónicos (USB's, CD's, etc).
Transferencias mediante el traslado sobre redes electrónicas:	Se realiza solamente transferencia interna entre los funcionarios de la DCB o de la Facultad, la información que se envía es número de trabajador, nombre completo, correo electrónico y en ocasiones RFC, así como la carga académica asignada durante el semestre. Se envía la información estrictamente indispensable para que el funcionario cumpla con la tarea requerida. La transferencia se realiza en hojas de cálculo y mediante correo electrónico. En caso de no recibir rechazo del servidor de correo, se asume que el destinatario recibió la información.

6.II.- RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

DCB-01-CCO-01

Sistema Integral de Información de la DCB

1. Salvo los respaldos periódicos del sistema en disco duro portátil y en la nube; no se almacenan los datos personales en ningún otro tipo de soporte físico. El disco duro de respaldo se resguarda en el cubículo de la Coordinación de Cómputo.
2. Tienen acceso a los respaldos en la nube y en disco duro:

Mtra. Irene Patricia Valdez y Alfaro.	Coordinadora de Cómputo
M.I. Janete Mejía Jiménez.	Técnica Académica y Web Master
Sr. Ariel Juárez Jiménez.	Ayudante de la Profesor de la Coord. de Cómputo

6.III.- BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

DCB-01-CCO-01

Sistema Integral de Información de la DCB

A nivel base de datos, a manera de bitácora, se generan registros en una tabla la base de datos que indican la última fecha y hora de ingreso de los usuarios al sistema.

A nivel servidor, se registran bitácoras de sucesos. Las bitácoras de servidor se revisan ocasionalmente, o puntualmente en caso de atención incidentes.

6.IV.- REGISTRO DE INCIDENTES:

DCB-01-CCO-01

Sistema Integral de Información de la DCB

Cuando ocurre un incidente: Falta de disponibilidad del sistema, o sospecha de intrusión o aviso de detección de vulnerabilidad por parte de DGTIC, el encargado del sistema procede a realizar la revisión y en su caso, aplicar las acciones correctivas para prevenir futuros incidentes.

En caso de que incidente sea catastrófico con pérdida de datos, se procede a restaurar el sistema a partir del último respaldo conocido.

6.V.- ACCESO A LAS INSTALACIONES

DCB-01-CCO-01

Sistema Integral de Información de la DCB

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

El acceso a las instalaciones exteriores es libre, no se controla.
La Secretaría Administrativa de la Facultad ha colocado cámaras de video vigilancia en algunos puntos críticos.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de da para soportes electrónicos):

Para los servidores alojados en la DCB:

El acceso al site en el que se localizan los servidores está limitado, mediante llave, a personas que son responsables de su administración:

- Cecilia Teresa Carmona Téllez, Técnica Académica
- Alejandro Rodríguez Rodríguez, Técnic0 Académic0
- Janete Mejía Jiménez, Técnica Académica
- Irene Patricia Valdez y Alfaro, Técnica Académica y Coordinadora de Cómputo.
- Ayudantes de Profesor de la Coordinación, bajo la supervisión de alguno de los técnic académicos.

Para los servidores alojados en el centro de datos de la Facultad:

La Unidad de servicios de Cómputo Académico (UNICA) es las responsable del control acceso.

6.VI.- ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

DCB-01-CCO-01

Sistema Integral de Información de la DCB

La actualización de datos personales de los académicos la realiza la Srita Margarita Cárdenas, al momento de registrarlo en el sistema y posteriormente en el momento en que los académicos le solicitan algún cambio de domicilio, teléfono o de grado académico.
Los académicos, a través del sistema pueden solicitar la actualización de su correo electrónico.
Los académicos realizan ellos mismos la actualización de su currículum.

Las medidas de seguridad previstas que se aplican para soportes electrónicos

6. VII.- PERFILES DE USUARIO Y CONTRASEÑAS

DCB-01-CCO-01

Sistema Integral de Información de la DCB

1. El modelo de control de acceso está basado en roles y reglas.
2. Perfiles de Usuario y contraseña:
   - ✓ ¿Cuenta con un sistema operativo de red instalado en sus equipos? Sí
   - ✓ ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Sí
   - ✓ ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? No
   - ✓ El acceso de los usuarios remotos es vía web, mediante nombre de usuario y contraseña.
   - ✓ El acceso de los administradores a la base de datos es a través de conectores ODBC y manejadores de bases de dtos, mediante usuario, contraseña y VPN

6.VIII.- PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

DCB-01-CCO-01

Sistema Integral de Información de la DCB

Se realizan semanalmente respaldos completos, de forma manual. Los respaldos se conservan en nube privada; ocasionalmente algunos de los respaldos se conservan también en un disco duro portátil que se resguarda en el cubículo de la Coordinación de Cómputo. El responsable de realizar los respaldos es el encargado principal del sistema.
NO SE CUENTAN CON DOS LUGARES QUE CUMPLAN CON LAS CONDICIONES DE SEGURIDAD ESPECIFICADAS EN EL ARTICULADO DEL CAPÍTULO V DE LOS LINEAMIENTOS

6.IX.- PLAN DE CONTINGENCIA

DCB-01-CCO-01

Sistema Integral de Información de la DCB

No se tiene formulado por escrito un plan de contingencia. Si ocurre un incidente de pérdida de datos por daño del servidor, el encargado principal del sistema en conjunto con el Administrador del servidor, recurren a restaurarlo en un servidor alterno provisional mediante la recuperación del último respaldo conocido. Posteriormente, analiza las causas y procede a aplicar medidas correctivas y preventivas en el servidor de producción y reactivar el sistema en su servidor original.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-01-CCO-01	
(Nombre del sistema)*	**Sistema Integral de Información de la DCB**	
Recurso*	**Descripción***	**Control***
Pruebas del sistema	Revisión aleatoria	Revisar de manera regular la funcionalidad con el fin de indagar si hubiera algún hueco de inseguridad en la aplicación. Responsables: Ariel Juárez Jiménez Irene Patricia Valdez y Alfaro

7.2. Procedimiento para la revisión de las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-01-CCO-01	
(Nombre del sistema)*	**Sistema Integral de Información de la DCB**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	Ariel Juárez Jiménez Irene P. Valdez y Alfaro

Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo	Janete Mejía Jiménez

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-01-CCO-01	
(Nombre del sistema)*	**Sistema Integral de Información de la DCB**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	Ariel Juárez Jiménez Irene P. Valdez y Alfaro
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Janete Mejía Jiménez

7.4. Acciones para la corrección y actualización de las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-01-CCO-01	
(Nombre del sistema)*	**Sistema Integral de Información de la DCB**	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL (Próximamente)	Realizar la renovación trimestral del certificado SSL para el subdominio donde se encuentra el sistema.	Janete Mejía Jiménez Ariel Juárez Jiménez
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la última versión estable.	Janete Mejía Jiménez Ariel Juárez Jiménez

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-01-CCO-01		
(Nombre del sistema)*	**Sistema Integral de Información de la DCB**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La importancia de la protección de datos personales	Seminario en línea	1 hora. Fecha:16 de junio de 2022	Seminario cursado por la responsable de red de la DCB, por lo que aplica para todos los sistemas

Seminario cursado por la responsable de red de la DCB, por lo que aplica para todos los sistemas.			de la DCB que manejan datos personales.

8.2. Programa de difusión de la protección a los datos personales

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-01-CCO-01		
(Nombre del sistema)*	**Sistema Integral de Información de la DCB**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difundir Aviso de privacidad	En todas las páginas de acceso a los datos se incluye el aviso de privacidad	Permanente	Toda la comunidad de la División y Público en general que consulta nuestros sitios

9. MEJORA CONTINUA

No se tiene formulado por escrito un programa para la mejora continua, pero se describe las actividades que se realizan regularmente para dar continuidad a los servicios.

9.1. Actualización y mantenimiento de sistemas de información

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-01-CCO-01		
(Nombre del sistema)*	**Sistema Integral de Información de la DCB**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Programación	De manera continua se trabaja en la programación del sistema para añadir funcionalidades, así como para mejorar la protección de los datos.	Permanente	Se avanza por módulos del sistema.

9.2. Actualización y mantenimiento de equipo de cómputo

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-01-CCO-01		
(Nombre del sistema)*	**Sistema Integral de Información de la DCB**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Mantenimiento preventivo al Hardware del servidor, contratado con proveedor externo.	Puntual, una vez al año	Se realiza mantenimiento preventivo al Hardware del servidor con el fin de evitar posibles daños y pérdida de disponibilidad del sistema.

9.3. Procesos para la conservación, preservación y respaldos de información

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-01-CCO-01	
(Nombre del sistema)*	**Sistema Integral de Información de la DCB**	
Proceso	**Descripción***	**Responsable**
Respaldo de base de datos y archivos del servido	Se realizan respaldos semanales de la base de datos y de los archivos del servidor.	Ariel Juárez Jiménez

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-01-CCO-01	
(Nombre del sistema)*	**Sistema Integral de Información de la DCB**	
Proceso	**Descripción***	**Responsable**
No se cuenta con proceso de borrado seguro		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

DCB-01-CCO-01

Sistema Integral de Información de la DCB

No se cuenta actualmente con un mecanismo definido formalmente para la supresión del sistema.

LABORATORIO VIRTUAL DE MATEMÁTICAS

Plataforma educativa mediante la cual los alumnos de las asignaturas de matemáticas realizan prácticas virtuales empleando Moodle y simuladores gráficos.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

DCB-02-CCO-02 LVM

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único*	DCB-02-CCO-02
(Nombre del sistema) *	**Laboratorio Virtual de Matemáticas**
Datos personales (sensibles o no) contenidos en el sistema*:	A. **Datos de Identificación:** Nombre completo, correo electrónico, fecha de nacimiento, género. Opcionales: Institución, departamento, teléfono, teléfono móvil, dirección, fotografía B. **Datos académicos:** Número de cuenta, calificaciones. C. **Datos de administración interna:** identificadores de bases de datos y reportes para fines analíticos y estadísticos.
Responsable*:	División de Ciencias Básicas de la Facultad de Ingeniería
Nombre*:	Mtra. Irene Patricia Valdez y Alfaro
Cargo*:	Coordinadora de Cómputo
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	Verificar la puesta en operación de la plataforma en tiempo y forma.
	Encargados:
(Nombre del Encargado 1*)	Cecilia Teresa Carmona Téllez
Cargo*:	Técnica académica
Funciones*:	Responsable del Laboratorio Virtual de Matemáticas. Configuración de la plataforma, responsable del correcto funcionamiento a nivel de servidor y operación de los servicios que en ella se ofrecen.
Obligaciones*:	Coordinar las tareas de administración de servidores y aplicativos en plataforma. Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Encargado 2*)	Yessica Gisela Arredondo Guzmán
Cargo*:	Ayudante de profesor
Funciones*:	Brindar apoyos en área de plataformas educativas.
Obligaciones*:	Apoyar en las tareas de administración de servidores y aplicativos en plataforma. Mantener la confidencialidad de los datos personales incorporados en el sistema.

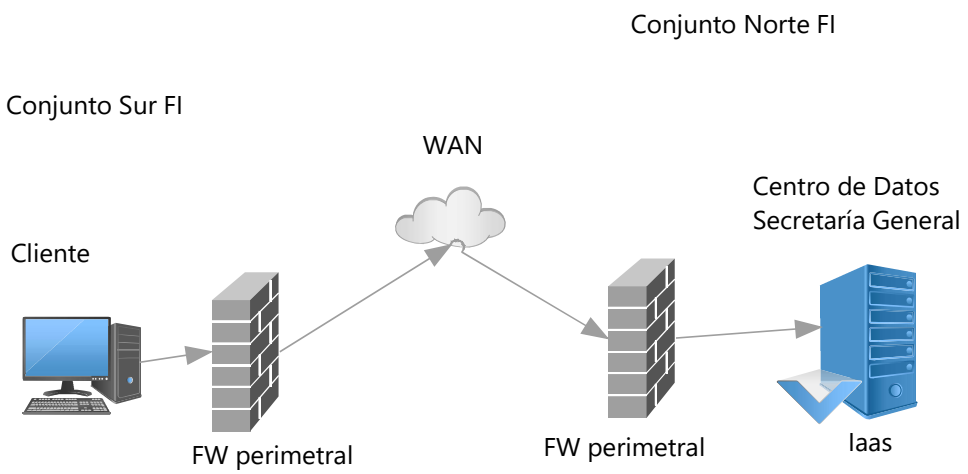
	Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Encargado 3*)	Gloria Luz Castillo Barrera
Cargo*:	Ayudante de profesor
Funciones*:	Brindar apoyos en área de plataformas educativas.
Obligaciones*:	Apoyar en las tareas de administración de servidores y aplicativos en plataforma. Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Encargado 3*)	Mario Alejandro Vasquez Martínez
Cargo*:	Ayudante de profesor
Funciones*:	Brindar apoyos en área de plataformas educativas.
Obligaciones*:	Apoyar en las tareas de administración de servidores y aplicativos en plataforma. Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
	Usuarios:
(Nombre del Usuario 1*)	María del Rocío Ávila Núñez
Cargo*:	Jefa del Departamento de Matemáticas
Funciones*:	Miembro del equipo revisor del LVM
Obligaciones*:	Observadora de calificaciones de grupos y revisora de prácticas. Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Usuario 2*)	Sergio Roberto Arzamendi Pérez
Cargo*:	Jefe de Academia de Cálculo
Funciones*:	Miembro del equipo revisor del LVM
Obligaciones*:	Observador de calificaciones de grupos y revisor de prácticas. Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Usuario 3*)	Alicia Pineda Ramírez
Cargo*:	Jefa de sección de Álgebra Lineal
Funciones*:	Miembro del equipo revisor del LVM
Obligaciones*:	Observadora de calificaciones de grupos y revisora de prácticas. Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Usuario 4*)	Héctor Hernández López
Cargo*:	Jefe de sección de Cálculo y Geometría
Funciones*:	Miembro del equipo revisor del LVM
Obligaciones*:	Observador de calificaciones de grupos y revisor de prácticas.

	Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Usuario 5*)	Sergio Carlos Crail Corzas
Cargo*:	Jefa de sección de Cálculo Integral y Vectorial
Funciones*:	Miembro del equipo revisor del LVM
Obligaciones*:	Observador de calificaciones de grupos y revisor de prácticas. Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Usuario 6*)	Cuerpo de profesores de la División de Ciencias Básicas
Cargo*:	Profesores de Asignatura y Profesores de Carrera
Funciones*:	Ingresar al sistema para monitorear la actividad de sus estudiantes y descargar resultados/calificaciones.
Obligaciones*:	Mantener la confidencialidad de los datos personales incorporados en el sistema. Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.
(Nombre del Usuario 7*)	Estudiantes inscritos en las asignaturas de la División con laboratorio virtual
Cargo*:	Usuario estudiante
Funciones*:	Ingresar al sistema para realizar las actividades del laboratorio.
Obligaciones*:	Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

DCB-02-CCO-02

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único¨*	DCB-02-CCO-02
(Nombre del sistema *)	**Laboratorio Virtual de Matemáticas**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Centro de Datos de la Secretaría General (IaaS)

	Conexión interna FI UNAM desde el Conjunto Sur 

3. ANÁLISIS DE RIESGOS

[redacted]

[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

5. PLAN DE TRABAJO

[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

6.I.- TRANSFERENCIAS DE DATOS PERSONALES

DCB-02-CCO-02

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único*	DCB-02-CCO-02
(Nombre del sistema)*	**Laboratorio Virtual de Matemáticas**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	a) La transferencia de datos personales mediante el traslado de soportes físicos se lleva a cabo por la vía elegida de común acuerdo entre las partes: visita

	personal o a través de encargados del sistema. b) Se realiza mediante correspondencia ordinaria en folder o sobre cerrado, no sellado, toda vez que se realiza entre responsables, encargados y/o usuarios del sistema. c) La entrega de información se lleva a cabo únicamente entre responsables, encargados y/o usuarios del sistema, en mano y sin solicitud de identificación de ninguna índole. d) El remitente no hace ninguna solicitud al destinatario referente al estado en que recibe la información. e) Dado que el traspaso de información se realiza directamente entre responsables, encargados y/o usuarios el acuse de recibo no se solicita. f) No se lleva a cabo registro alguno del traslado de información en bitácora. g) No existe instrumento jurídico que formalice las transferencias de datos personales.
Transferencias mediante el traslado de soportes electrónicos:	a) La transferencia de datos personales mediante el traslado de soportes electrónicos se lleva a cabo por la vía elegida de común acuerdo entre las partes. b) Se realiza mediante el empleo de medios físicos, correo electrónico, administración de la plataforma y/o aplicaciones de colaboración entre responsables y encargados de la plataforma. c) La entrega de información se lleva a cabo en mano o en las direcciones o carpetas digitales correspondientes, sin solicitud de identificación de ninguna índole entre responsables y encargados del sistema. d) El remitente no hace ninguna solicitud al destinatario referente al estado en que recibe la información. e) Dado que el traspaso de información se realiza directamente entre responsables y encargados el acuse de recibo no se solicita. f) No se lleva a cabo registro alguno del traslado de información en bitácora. g) En algunas ocasiones, los archivos electrónicos que contienen datos personales se comprimen y encriptan con herramientas de software libre empleando distintos métodos de encriptación tales como AES-256 sin restricción en la longitud de la clave. h) No existe instrumento jurídico que formalice las transferencias de datos personales mediante el traslado de soportes electrónicos.

Transferencias mediante el traslado sobre redes electrónicas:	a) Para envío a través de correo electrónico, en algunas ocasiones, los archivos electrónicos que contienen datos personales se comprimen y encriptan con herramientas de software libre empleando distintos métodos de encriptación tales como AES-256 sin restricción en la longitud de la clave. b) No existe instrumento jurídico que formalice las transferencias de datos personales mediante el traslado de soportes electrónicos.

6.II.- RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

DCB-02-CCO-02

Laboratorio Virtual de Matemáticas

1. Salvo los respaldos periódicos del sistema en disco duro portátil y en la nube; no se almacenan los datos personales en ningún otro tipo de soporte físico. El disco duro de respaldo se resguarda en el cubículo del Taller de Cómputo para Académicos.
2. Tienen acceso a los respaldos en disco duro:

Mtra. Irene Patricia Valdez y Alfaro.	Coordinadora de Cómputo
Ing. Cecilia Teresa Carmona Téllez.	Técnica Académica y Administradora de red
Yessica Gisela Arredondo Guzmán.	Ayudante de la Profesor de la Coord. de Cómputo
Gloria Luz Castillo Barrera.	Ayudante de la Profesor de la Coord. de Cómputo
Mario Alejandro Vasquez Martínez.	Ayudante de la Profesor de la Coord. de Cómputo

6.III.- BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

DCB-02-CCO-02

Laboratorio Virtual de Matemáticas

Se utilizan bitácoras generadas por el sistema operativo y aplicativos, los cuales tienen soporte electrónico y presentan información de acceso al sistema.

6.IV.- REGISTRO DE INCIDENTES:

DCB-02-CCO-02

Laboratorio Virtual de Matemáticas

Cuando ocurre un incidente: Falta de disponibilidad del sistema, o sospecha de intrusión o aviso de detección de vulnerabilidad por parte de DGTIC, el encargado del sistema procede a realizar la revisión y en su caso, aplicar las acciones correctivas para prevenir futuros incidentes.

En caso de que incidente sea catastrófico con pérdida de datos, se procede a restaurar el sistema a partir del último respaldo conocido.

6.V.- ACCESO A LAS INSTALACIONES

DCB-02-CCO-02

Laboratorio Virtual de Matemáticas

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

El acceso a las instalaciones exteriores es libre, no se controla.

La Secretaría Administrativa de la Facultad ha colocado cámaras de video vigilancia en algunos puntos críticos.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de da para soportes electrónicos):

Para los servidores alojados en la DCB:

El acceso al site en el que se localizan los servidores está limitado, mediante llave, a personas que son responsables de su administración:

- Cecilia Teresa Carmona Téllez, Técnica Académica
- Alejandro Rodríguez Rodríguez, Técnic0 Académic0
- Janete Mejía Jiménez, Técnica Académica
- Irene Patricia Valdez y Alfaro, Técnica Académica y Coordinadora de Cómputo.
- Ayudantes de Profesor de la Coordinación, bajo la supervisión de alguno de los técnic académicos.

Para los servidores alojados en el centro de datos de la Facultad:

La Unidad de servicios de Cómputo Académico (UNICA) es las responsable del control acceso.

6.VI.- ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

DCB-02-CCO-02

Laboratorio Virtual de Matemáticas

Anualmente se solicita a la Secretaría de Servicios Académicos de la Facultad el listado de estudiantes de nuevo ingreso, con lo que se realiza una actualización incremental a la base de datos de alumnos a la cual accede el sistema. En caso de que algún alumno solicite corrección de sus datos, se le solicita mostrar un comprobante oficial donde aparezca el dato correcto y se procede por parte del administrador a actualizar el registro correspondiente en la base de datos.

Las medidas de seguridad previstas que se aplican para soportes electrónicos

6. VII.- PERFILES DE USUARIO Y CONTRASEÑAS

DCB-02-CCO-02

Laboratorio Virtual de Matemáticas

1. El modelo de control de acceso está basado en roles.
2. Perfiles de Usuario y contraseña:
   - ✓ ¿Cuenta con un sistema operativo de red instalado en sus equipos? Sí
   - ✓ ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Sí
   - ✓ ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Sí
   - ✓ El acceso de los usuarios es vía web, mediante nombre de usuario y contraseña.
   - ✓ El acceso de los administradores a la base de datos es a través de conectores ODBC y manejadores de bases de datos, mediante usuario, contraseña y VPN

6.VIII.- PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

DCB-02-CCO-02

Laboratorio Virtual de Matemáticas

Se realizan periódicamente respaldos completos, de forma automática, la periodicidad depende de los procesos en curso. El responsable de realizar los respaldos es el encargado principal del sistema.
Los respaldos se conservan en disco duro portátil que se resguarda en un área de cómputo de acceso controlado.
NO SE CUENTAN CON DOS LUGARES QUE CUMPLAN CON LAS CONDICIONES DE SEGURIDAD ESPECIFICADAS EN EL ARTICULADO DEL CAPÍTULO V DE LOS LINEAMIENTOS

6.IX.- PLAN DE CONTINGENCIA

DCB-02-CCO-02

Laboratorio Virtual de Matemáticas

No se cuenta con un plan de contingencia, sin embargo, se llevan a cabo algunas medidas para la continuidad de operaciones tales como el respaldo de la información de manera periódica, además de estar apoyados por las medidas de protección del centro de datos de la secretaría general (IaaS).

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-02-CCO-02	
(Nombre del sistema)*	**Laboratorio Virtual de Matemáticas**	
Recurso*	**Descripción***	**Control***
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación. Responsable: Ing. Mario Alejandro Vasquez Martínez

7.2. Procedimiento para la revisión de las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-02-CCO-02	
(Nombre del sistema)*	**Laboratorio Virtual de Matemáticas**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	El responsable de realizar la revisión es el Ing. Mario Alejandro Vasquez Martínez. La duración de la revisión es un día hábil.
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo	El responsable de realizar la revisión es el Ing. Mario Alejandro Vasquez Martínez. La duración de la revisión es un día hábil.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-02-CCO-02	
(Nombre del sistema)*	**Laboratorio Virtual de Matemáticas**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	El responsable de realizar la revisión es el Ing. Mario Alejandro Vasquez Martínez. La duración de la revisión es un día hábil.
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	El responsable de realizar la revisión es el Ing. Mario Alejandro Vasquez Martínez. La duración de la revisión es un día hábil.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-02-CCO-02	
(Nombre del sistema)*	**Laboratorio Virtual de Matemáticas**	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Realizar la renovación trimestral del certificado SSL para el subdominio donde se encuentra el sistema.	Ing. Mario Alejandro Vasquez Martínez
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la última versión estable.	Ing. Mario Alejandro Vasquez Martínez

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-02-CCO-02		
(Nombre del sistema)*	**Laboratorio Virtual de Matemáticas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La importancia de la protección de datos personales Seminario cursado por la responsable de red de la DCB, por lo que aplica para todos los sistemas.	Seminario en línea	1 hora. Fecha:16 de junio de 2022	Seminario cursado por la responsable de red de la DCB, por lo que aplica para todos los sistemas de la DCB que manejan datos personales.

8.2. Programa de difusión de la protección a los datos personales

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-02-CCO-02		
(Nombre del sistema)*	**Laboratorio Virtual de Matemáticas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difundir Aviso de privacidad	En todas las páginas de acceso a los datos se incluye el aviso de privacidad	Permanente	Toda la comunidad de la División y Público en general que consulta nuestros sitios

9. MEJORA CONTINUA

No se tiene formulado por escrito un programa para la mejora continua, pero se describe las actividades que se realizan regularmente para dar continuidad a los servicios.

9.1. Actualización y mantenimiento de sistemas de información

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-02-CCO-02		
(Nombre del sistema)*	**Laboratorio Virtual de Matemáticas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del core de Moodle	Se realiza el upgrade de la versión de moodle implementada en el sitio, con el fin de mitigar las vulnerabilidades que han sido encontradas.	Variable	Se cierra la brecha de vulnerabilidades e incompatibilidad de software.
Actualización de plugins de Moodle	Actualización de programas complementarios que amplían la funcionalidad del aplicativo web	Variable	Se cierra la brecha de vulnerabilidades e incompatibilidad de software.
Actualización del sistema operativo	Actualización de versiones del sistema operativo con el fin de corregir o mitigar vulnerabilidades encontradas	variable	Se cierra la brecha de vulnerabilidades.
Actualización de utilerías del Sistema Operativo	Actualización de programas que añaden funcionalidad al Sistema operativo	variable	Se cierra la brecha de vulnerabilidades.

9.2. Actualización y mantenimiento de equipo de cómputo

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-02-CCO-02		
(Nombre del sistema)*	**Laboratorio Virtual de Matemáticas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica, depende del	El sistema se aloja en un servidor virtual a cargo de	--	--

Centro de Datos de Secretaría General	la Secretaría General de la Facultad, por lo que no es aplicable el mantenimiento.		

9.3. Procesos para la conservación, preservación y respaldos de información

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-02-CCO-02	
(Nombre del sistema)*	**Laboratorio Virtual de Matemáticas**	
Proceso	**Descripción***	**Responsable**
Respaldo de base de datos y archivos del servidor	Se realizan respaldos de la base de datos de Moodle en función de los periodos de exámenes programados. Tiempo máximo de ejecución: en función del tamaño del respaldo.	Mario Alejandro Vasquez Martínez

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-02-CCO-02	
(Nombre del sistema)*	**Laboratorio Virtual de Matemáticas**	
Proceso	**Descripción***	**Responsable**
No se cuenta con proceso de borrado seguro		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

DCB-02-CCO-02

Laboratorio Virtual de Matemáticas

No se cuenta actualmente con un mecanismo definido formalmente para la supresión del sistema.

EXÁMENES EN LÍNEA DE LA DIVISIÓN DE CIENCIAS BÁSICAS V.1

Plataforma en Moodle empleada para la realización de exámenes colegiados, extraordinarios, de suficiencia y especiales, en línea, de 25 asignaturas de la División de Ciencias Básicas. El sistema permite la consulta de calificaciones tanto de estudiantes como de profesores, jefes de academia y coordinadores de asignatura en función de los calendarios establecidos para dicho fin. Adicionalmente, es posible generar reportes para fines estadísticos

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

DCB-03-CCO-03 EXLIN

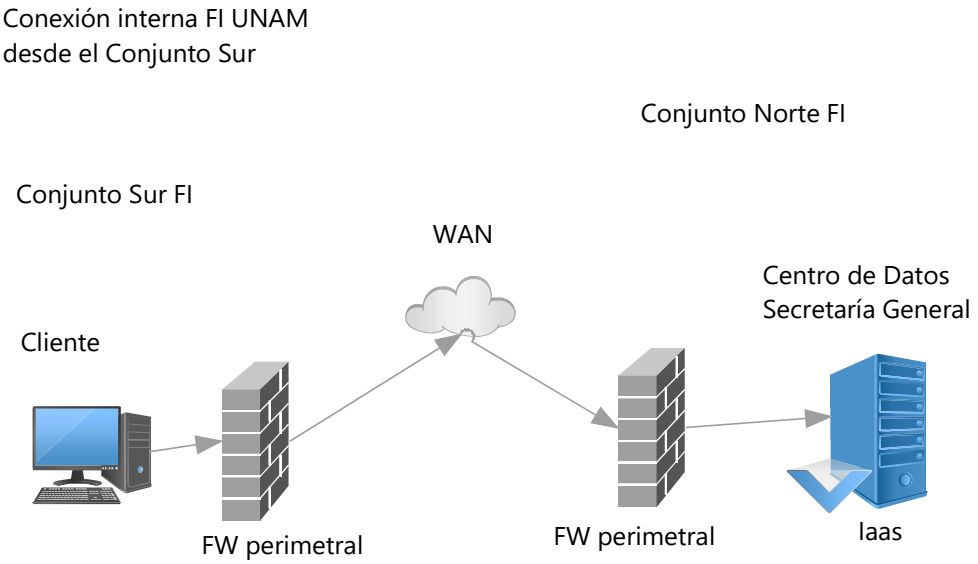
División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único*	DCB-03-CCO-03
(Nombre del sistema) *	**Exámenes en Línea de la División de Ciencias Básicas**
Datos personales (sensibles o no) contenidos en el sistema*:	A. **Datos de Identificación:** Nombre completo, RFC de profesores, correo electrónico, fecha de nacimiento y género. Opcionales: Institución, departamento, teléfono, teléfono móvil, dirección, fotografía B. **Datos académicos:** Número de cuenta, calificaciones, exámenes, carrera, grupos, año de ingreso a la carrera. C. **Datos laborales:** número de trabajador. D. **Datos de administración interna:** identificadores de bases de datos y reportes para fines analíticos y estadísticos
Responsable*:	División de Ciencias Básicas de la Facultad de Ingeniería
Nombre*:	Mtra. Irene Patricia Valdez y Alfaro
Cargo*:	Coordinadora de Cómputo
Funciones*:	Responsable del contenido de datos personales en bases de datos autorizadas y de la remisión y transferencia de datos a los responsables de la plataforma para su configuración o empleo en el sistema. Responsable de definir los mecanismos para el control de acceso a la plataforma.
Obligaciones*:	Registrar en bases de datos de la DCB los datos personales de alumnos y profesores. Proporcionar información del alumnado y profesorado del semestre en turno para su configuración en plataforma.
	Encargados:
(Nombre del Encargado 1*)	Cecilia Teresa Carmona Téllez
Cargo*:	Técnica académica
Funciones*:	Responsable del correcto funcionamiento de la plataforma a nivel de servidor y operación de los servicios que en ella se ofrecen.
Obligaciones*:	Coordinar las tareas de administración de servidores y aplicativos en plataforma.
(Nombre del Encargado 2*)	Yessica Gisela Arredondo Guzmán
Cargo*:	Ayudante de profesor
Funciones*:	Brindar apoyos en área de plataformas educativas.

Obligaciones*:	Apoyar en las tareas de administración de servidores y aplicativos en plataforma.
(Nombre del Encargado 3*)	Gloria Luz Castillo Barrera
Cargo*:	Ayudante de profesor
Funciones*:	Brindar apoyos en área de plataformas educativas.
Obligaciones*:	Apoyar en las tareas de administración de servidores y aplicativos en plataforma.
(Nombre del Encargado 4*)	Mario Alejandro Vasquez Martínez
Cargo*:	Ayudante de profesor
Funciones*:	Brindar apoyos en área de plataformas educativas.
Obligaciones*:	Apoyar en las tareas de administración de servidores y aplicativos en plataforma.
	Usuarios:
(Nombre del Usuario 1*)	Janete Mejía Jiménez
Cargo*:	Técnica académica
Funciones*:	Corresponsable de los exámenes extraordinarios en plataforma
Obligaciones*:	Crear grupos y configurar exámenes de acuerdo con las fechas establecidas para la realización de exámenes extraordinarios de la DCB en los periodos correspondientes.
(Nombre del Usuario 2*)	Irene Patricia Valdez y Alfaro
Cargo*:	Coordinadora de Cómputo
Funciones*:	Corresponsable de los exámenes extraordinarios en plataforma
Obligaciones*:	Crear grupos y configurar exámenes de acuerdo con las fechas establecidas para la realización de exámenes extraordinarios de la DCB en los periodos correspondientes.
(Nombre del Usuario 3*)	Yahvé Abdul Ledezma Rubio
Cargo*:	Jefe de Academia de Mecánica
Funciones*:	Responsable de los exámenes colegiados de las asignaturas de Mecánica, Estática y Dinámica
Obligaciones*:	Alta de reactivos y creación de exámenes colegiados de las asignaturas de Mecánica, Estática y Cinemática y Dinámica.
(Nombre del Usuario 4*)	Casiano Aguilar Morales
Cargo*:	Jefe de Academia de Matemáticas Aplicadas
Funciones*:	Responsable de los exámenes colegiados de las asignaturas de Matemáticas Avanzadas, Análisis Numérico, Ecuaciones Diferenciales.
Obligaciones*:	Alta de reactivos y creación de exámenes colegiados de las asignaturas de Matemáticas Avanzadas, Análisis Numérico, Ecuaciones Diferenciales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

DCB-03-CCO-03

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único¨*	DCB-03-CCO-03
(Nombre del sistema *)	**Exámenes en Línea de la División de Ciencias Básicas**
Tipo de soporte:*	Electrónico

Descripción:*	Base de datos de la DCB para el almacenamiento de datos personales de identificación de alumnos. Base de datos de Moodle para el almacenamiento de datos personales de identificación de profesores, personales académicos y de administración interna.
Características del lugar donde se resguardan los soportes:*	Ambas bases se alojan en el Centro de Datos de la Secretaría General (IaaS) 

3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

6.I.- TRANSFERENCIAS DE DATOS PERSONALES

DCB-03-CCO-03

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único*	DCB-03-CCO-03
(Nombre del sistema)*	**Exámenes en Línea de la División de Ciencias Básicas**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	a) En algunas ocasiones, los archivos electrónicos que contienen datos personales se comprimen y encriptan con herramientas de software libre empleando distintos métodos de encriptación tales como AES-256 sin restricción en la longitud de la clave. b) No existe instrumento jurídico que formalice las transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado de soportes electrónicos:	a) La transferencia de datos personales mediante el traslado de soportes electrónicos se lleva a cabo por la vía elegida de común acuerdo entre las partes. b) Se realiza mediante el empleo de medios físicos, correo electrónico, administración de la plataforma y/o aplicaciones de colaboración entre responsables y encargados de la plataforma. c) La entrega de información se lleva a cabo en mano o en las direcciones o carpetas digitales correspondientes, sin solicitud de identificación de ninguna índole entre responsables y encargados del sistema. d) El remitente no hace ninguna solicitud al destinatario referente al estado en que recibe la información. e) Dado que el traspaso de información se realiza directamente entre responsables y encargados el acuse de recibo no se solicita. f) No se lleva a cabo registro alguno del traslado de información en bitácora. g) En algunas ocasiones, los archivos electrónicos que contienen datos personales se comprimen y encriptan con herramientas de software libre empleando distintos métodos de encriptación tales como AES-256 sin restricción en la longitud de la clave. h) No existe instrumento jurídico que formalice las transferencias de datos personales mediante el traslado de soportes electrónicos.

Transferencias mediante el traslado sobre redes electrónicas:	a) Se realiza mediante el empleo de medios físicos, correo electrónico, administración de la plataforma y/o aplicaciones de colaboración entre responsables y encargados de la plataforma. b) No se emplean canales de comunicación dedicados, se hace uso de internet para el acceso a las plataformas de colaboración (https). c) No se envía acuse de recibo al remitente. d) El remitente no registra las transferencias en bitácora ni en el sistema de tratamiento de datos personales. e) No existe instrumento jurídico que formalice las transferencias de datos personales mediante el traslado de soportes electrónicos.

6.II.- RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

DCB-03-CCO-03

Exámenes en Línea de la División de Ciencias Básicas

1. Salvo los respaldos periódicos del sistema en disco duro portátil y en la nube; no se almacenan los datos personales en ningún otro tipo de soporte físico. El disco duro de respaldo se resguarda en el cubículo del Taller de Cómputo para Académicos.
2. Tienen acceso a los respaldos en disco duro:

Mtra. Irene Patricia Valdez y Alfaro.	Coordinadora de Cómputo
Ing. Cecilia Teresa Carmona Téllez.	Técnica Académica y Administradora de red
Yessica Gisela Arredondo Guzmán.	Ayudante de la Profesor de la Coord. de Cómputo
Gloria Luz Castillo Barrera.	Ayudante de la Profesor de la Coord. de Cómputo
Mario Alejandro Vasquez Martínez.	Ayudante de la Profesor de la Coord. de Cómputo

6.III.- BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

DCB-03-CCO-03

Exámenes en Línea de la División de Ciencias Básicas

Se utilizan bitácoras generadas por el sistema operativo y aplicativos, los cuales tienen soporte electrónico y presentan información de acceso al sistema.

6.IV.- REGISTRO DE INCIDENTES:

DCB-03-CCO-03

Exámenes en Línea de la División de Ciencias Básicas

Cuando ocurre un incidente: Falta de disponibilidad del sistema, o sospecha de intrusión o aviso de detección de vulnerabilidad por parte de DGTIC, el encargado del sistema procede a realizar la revisión y en su caso, aplicar las acciones correctivas para prevenir futuros incidentes.

En caso de que incidente sea catastrófico con pérdida de datos, se procede a restaurar el sistema a partir del último respaldo conocido.

6.V.- ACCESO A LAS INSTALACIONES

DCB-03-CCO-03

Exámenes en Línea de la División de Ciencias Básicas

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

   El acceso a las instalaciones exteriores es libre, no se controla.
   La Secretaría Administrativa de la Facultad ha colocado cámaras de video vigilancia en algunos puntos críticos.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de da para soportes electrónicos):

Para los servidores alojados en la DCB:

El acceso al site en el que se localizan los servidores está limitado, mediante llave, a personas que son responsables de su administración:

- Cecilia Teresa Carmona Téllez, Técnica Académica
- Alejandro Rodríguez Rodríguez, Técnic0 Académic0
- Janete Mejía Jiménez, Técnica Académica
- Irene Patricia Valdez y Alfaro, Técnica Académica y Coordinadora de Cómputo.
- Ayudantes de Profesor de la Coordinación, bajo la supervisión de alguno de los técnic académicos.

Para los servidores alojados en el centro de datos de la Facultad:

La Unidad de servicios de Cómputo Académico (UNICA) es las responsable del control acceso.

6.VI.- ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

DCB-03-CCO-03

Exámenes en Línea de la División de Ciencias Básicas

Anualmente se solicita a la Secretaría de Servicios Académicos de la Facultad el listado de estudiantes de nuevo ingreso, con lo que se realiza una actualización incremental a la base de datos de alumnos a la cual accede el sistema. En caso de que algún alumno solicite corrección de sus datos, se le solicita mostrar un comprobante oficial donde aparezca el dato correcto y se procede por parte del administrador a actualizar el registro correspondiente en la base de datos.

Las medidas de seguridad previstas que se aplican para soportes electrónicos

6. VII.- PERFILES DE USUARIO Y CONTRASEÑAS

DCB-03-CCO-03

Exámenes en Línea de la División de Ciencias Básicas

1. El modelo de control de acceso está basado en roles.
2. Perfiles de Usuario y contraseña:
   - ✓ ¿Cuenta con un sistema operativo de red instalado en sus equipos? Sí
   - ✓ ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Sí
   - ✓ ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Sí
   - ✓ El acceso de los usuarios es vía web, mediante nombre de usuario y contraseña.

- ✓ El acceso de los administradores a la base de datos es a través de conectores ODBC y manejadores de bases de datos, mediante usuario, contraseña y VPN

6.VIII.- PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

DCB-03-CCO-03

Exámenes en Línea de la División de Ciencias Básicas

Se realizan periódicamente respaldos completos, de forma automática, la periodicidad depende de los procesos en curso. El responsable de realizar los respaldos es el encargado principal del sistema.

Los respaldos se conservan en disco duro portátil que se resguarda en un área de cómputo de acceso controlado.

NO SE CUENTAN CON DOS LUGARES QUE CUMPLAN CON LAS CONDICIONES DE SEGURIDAD ESPECIFICADAS EN EL ARTICULADO DEL CAPÍTULO V DE LOS LINEAMIENTOS

6.IX.- PLAN DE CONTINGENCIA

DCB-03-CCO-03

Exámenes en Línea de la División de Ciencias Básicas

No se cuenta con un plan de contingencia, sin embargo, se llevan a cabo algunas medidas para la continuidad de operaciones tales como el respaldo de la información de manera periódica, además de estar apoyados por las medidas de protección del centro de datos de la secretaría general (IaaS).

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-03-CCO-03	
(Nombre del sistema)*	**Exámenes en Línea de la División de Ciencias Básicas**	
Recurso*	**Descripción***	**Control***
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación. Responsable: Ing. Mario Alejandro Vasquez Martínez

7.2. Procedimiento para la revisión de las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-03-CCO-03	
(Nombre del sistema)*	**Exámenes en Línea de la División de Ciencias Básicas**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	El responsable de realizar la revisión es el Ing. Mario Alejandro Vasquez Martínez.

		La duración de la revisión es un día hábil.
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo	El responsable de realizar la revisión es el Ing. Mario Alejandro Vasquez Martínez. La duración de la revisión es un día hábil.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-03-CCO-03	
(Nombre del sistema)*	**Exámenes en Línea de la División de Ciencias Básicas**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	El responsable de realizar la revisión es el Ing. Mario Alejandro Vasquez Martínez. La duración de la revisión es un día hábil.
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	El responsable de realizar la revisión es el Ing. Mario Alejandro Vasquez Martínez. La duración de la revisión es un día hábil.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-03-CCO-03	
(Nombre del sistema)*	**Exámenes en Línea de la División de Ciencias Básicas**	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Realizar la renovación trimestral del certificado SSL para el subdominio donde se encuentra el sistema.	Ing. Mario Alejandro Vasquez Martínez
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la última versión estable.	Ing. Mario Alejandro Vasquez Martínez

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-03-CCO-03		
(Nombre del sistema)*	**Exámenes en Línea de la División de Ciencias Básicas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La importancia de la protección de datos personales	Seminario en línea	1 hora. Fecha:16 de junio de 2022	Seminario cursado por la responsable de red de la DCB, por lo que aplica para todos los sistemas

Seminario cursado por la responsable de red de la DCB, por lo que aplica para todos los sistemas.			de la DCB que manejan datos personales.

8.2. Programa de difusión de la protección a los datos personales

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-03-CCO-03		
(Nombre del sistema)*	**Exámenes en Línea de la División de Ciencias Básicas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difundir Aviso de privacidad	En todas las páginas de acceso a los datos se incluye el aviso de privacidad	Permanente	Toda la comunidad de la División y Público en general que consulta nuestros sitios

9. MEJORA CONTINUA

No se tiene formulado por escrito un programa para la mejora continua, pero se describe las actividades que se realizan regularmente para dar continuidad a los servicios.

9.1. Actualización y mantenimiento de sistemas de información

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-03-CCO-03		
(Nombre del sistema)*	**Exámenes en Línea de la División de Ciencias Básicas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del core de Moodle	Se realiza el upgrade de la versión de moodle implementada en el sitio, con el fin de mitigar las vulnerabilidades que han sido encontradas.	Variable	Se cierra la brecha de vulnerabilidades e incompatibilidad de software.
Actualización de plugins de Moodle	Actualización de programas complementarios que amplían la funcionalidad del aplicativo web	Variable	Se cierra la brecha de vulnerabilidades e incompatibilidad de software.
Actualización del sistema operativo	Actualización de versiones del sistema operativo con el fin de corregir o mitigar vulnerabilidades encontradas	variable	Se cierra la brecha de vulnerabilidades.
Actualización de utilerías del Sistema Operativo	Actualización de programas que añaden funcionalidad al Sistema operativo	variable	Se cierra la brecha de vulnerabilidades.

9.2. Actualización y mantenimiento de equipo de cómputo

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-03-CCO-03		
(Nombre del sistema)*	**Exámenes en Línea de la División de Ciencias Básicas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica, depende del Centro de Datos de Secretaría General	El sistema se aloja en un servidor virtual a cargo de la Secretaría General de la Facultad, por lo que no es aplicable el mantenimiento.	--	--

9.3. Procesos para la conservación, preservación y respaldos de información

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-03-CCO-03	
(Nombre del sistema)*	**Exámenes en Línea de la División de Ciencias Básicas**	
Proceso	**Descripción***	**Responsable**
Respaldo de base de datos y archivos del servidor	Se realizan respaldos de la base de datos de Moodle en función de los periodos de exámenes programados. Tiempo máximo de ejecución: en función del tamaño del respaldo.	Mario Alejandro Vasquez Martínez

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-03-CCO-03	
(Nombre del sistema)*	**Exámenes en Línea de la División de Ciencias Básicas**	
Proceso	**Descripción***	**Responsable**
No se cuenta con proceso de borrado seguro		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

DCB-03-CCO-03

Exámenes en Línea de la División de Ciencias Básicas

No se cuenta actualmente con un mecanismo definido formalmente para la supresión del sistema.

PREREGISTRO A PROGRAMAS ESPECIALES DE LA DCB

Sistema web que automatiza los procesos de pre-registro a los programas especiales de la División de Ciencias Básicas. Gestiona diferentes eventos como lo son los exámenes extraordinarios en tres etapas, los exámenes extraordinarios con curso de preparación y los exámenes extraordinarios con taller de preparación. Permite el registro a alumnos de la Facultad de Ingeniería, los usuarios pueden solicitar su pre-registro a los eventos que se encuentren activos, además permite imprimir un acuse de pre-registro donde encontrará los datos de su solicitud.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

DCB-04-CCO-04 Pre-registro ProEs

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único*:	DCB-04-CCO-04
Nombre del sistema *:	**Pre-registro a programas especiales de la DCB**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, número de cuenta (alumnos UNAM), fecha de nacimiento, correo electrónico, carrera.
Responsable*:	**División de Ciencias Básicas.**
Nombre*:	**Irene Patricia Valdez y Alfaro**
Cargo*:	Coordinadora de Cómputo
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les otorga acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
Encargados:	
Nombre del Encargado 1*:	**Ing. Edwin Díaz Caballero**
Cargo*:	Ayudante de profesor
Funciones*:	Realizar el proceso de software con la finalidad de atender las necesidades administrativas relacionadas con la DCB.
Obligaciones*:	Procurar la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento.
(Nombre del Encargado 2*)	M. I. Janete Mejía Jiménez
Cargo*:	Técnico Académico
Funciones*:	Administración del servidor. Administración del sistema de bases de datos. Dar de alta y controlar acceso de usuarios de las bases de datos.
Obligaciones*:	Administrar el servidor que aloja al sistema, administrar las bases de datos del servidor.

	Procurar la protección de datos contenidos en el servidor con estrategias y mecanismos de seguridad. Mantener un registro de usuarios con acceso al servidor y a las bases de datos (nombre de la persona, nombre de usuario, contraseñas otorgadas y privilegios). Realizar el monitoreo de incidentes en el servidor y aplicar las políticas de seguridad pertinentes para evitar ataques. Registrar y reportar incidentes de seguridad.
	Usuarios:
(Nombre del Usuario*)	Estudiantes de las asignaturas de la División de Ciencias Básicas
Cargo*:	Usuario estudiante
Funciones*:	Ingresar al sistema para realizar su pre-rregistro en el programa de su interés.
Obligaciones*:	Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

DCB-04-CCO-04

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único*:	DCB-04-CCO-04
Nombre del sistema*:	**Pre-registro a programas especiales de la DCB**
Tipo de soporte*:	Electrónico
Descripción*:	Base de datos relacional con interfaz de acceso por web y manejador de base de datos.
Características del lugar donde se resguardan los soportes*:	Servidor web y de base de datos conjunto, en el cual se almacena tanto el sistema, como el soporte. Los datos personales no viajan por las redes cuando el sistema se los solicita al soporte ya que se trata de una conexión interna local, esto debido a que el soporte y el sistema se encuentran en el mismo equipo.

3. ANÁLISIS DE RIESGOS

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

6.I.- TRANSFERENCIAS DE DATOS PERSONALES

DCB-04-CCO-04

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único*	**DCB-04-CCO-04**
(Nombre del sistema)*	**Pre-registro a programas especiales de la DCB**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza transferencia de datos personales en soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realiza transferencia de datos en soportes electrónicos (USB's, CD's, etc).
Transferencias mediante el traslado sobre redes electrónicas:	Se realiza solamente transferencia interna entre los funcionarios de la DCB o de la Facultad, los datos personales que se transfieren son número de cuenta del alumno, nombre completo, correo electrónico y nombre del programa al que se inscribe. Se envía la información estrictamente indispensable para que el funcionario cumpla con la tarea requerida. La transferencia se realiza en hojas de cálculo y mediante correo electrónico. En caso de no recibir rechazo del servidor de correo, se asume que el destinatario recibió la información.

6.II.- RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

DCB-04-CCO-04

Pre-registro a programas especiales de la DCB

1. Salvo los respaldos periódicos del sistema en disco duro portátil y en la nube; no se almacenan los datos personales en ningún otro tipo de soporte físico. El disco duro de respaldo se resguarda en el cubículo de la Coordinación de Cómputo.
2. Tienen acceso a los respaldos en la nube y en disco duro:

Mtra. Irene Patricia Valdez y Alfaro.	Coordinadora de Cómputo
M.I. Janete Mejía Jiménez.	Técnica Académica y Web Master
Sr. Edwin Caballero Díaz.	Ayudante de la Profesor de la Coord. de Cómputo

6.III.- BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

DCB-04-CCO-04

Pre-registro a programas especiales de la DCB

A nivel servidor, se registran bitácoras de sucesos. Las bitácoras de servidor se revisan ocasionalmente, o puntualmente en caso de atención incidentes.

6.IV.- REGISTRO DE INCIDENTES:

DCB-04-CCO-04

Pre-registro a programas especiales de la DCB

Cuando ocurre un incidente: Falta de disponibilidad del sistema, o sospecha de intrusión o aviso de detección de vulnerabilidad por parte de DGTIC, el encargado del sistema procede a realizar la revisión y en su caso, aplicar las acciones correctivas para prevenir futuros incidentes.

En caso de que incidente sea catastrófico con pérdida de datos, se procede a restaurar el sistema a partir del último respaldo conocido.

6.V.- ACCESO A LAS INSTALACIONES

DCB-04-CCO-04

Pre-registro a programas especiales de la DCB

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

   El acceso a las instalaciones exteriores es libre, no se controla.
   La Secretaría Administrativa de la Facultad ha colocado cámaras de video vigilancia en algunos puntos críticos.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de da para soportes electrónicos):

   Para los servidores alojados en la DCB:

   El acceso al site en el que se localizan los servidores está limitado, mediante llave, a personas que son responsables de su administración:

   - Cecilia Teresa Carmona Téllez, Técnica Académica
   - Alejandro Rodríguez Rodríguez, Técnic0 Académic0
   - Janete Mejía Jiménez, Técnica Académica

- Irene Patricia Valdez y Alfaro, Técnica Académica y Coordinadora de Cómputo.
- Ayudantes de Profesor de la Coordinación, bajo la supervisión de alguno de los técnic académicos.

Para los servidores alojados en el centro de datos de la Facultad:

La Unidad de servicios de Cómputo Académico (UNICA) es la responsable del control acceso.

6.VI.- ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

DCB-04-CCO-04

Pre-registro a programas especiales de la DCB

Anualmente se solicita a la Secretaría de Servicios Académicos de la Facultad el listado de estudiantes de nuevo ingreso, con lo que se realiza una actualización incremental a la base de datos de alumnos a la cual accede el sistema. En caso de que algún alumno solicite corrección de sus datos, se le solicita mostrar un comprobante oficial donde aparezca el dato correcto y se procede por parte del administrador a actualizar el registro correspondiente en la base de datos.

Las medidas de seguridad previstas que se aplican para soportes electrónicos

6. VII.- PERFILES DE USUARIO Y CONTRASEÑAS

DCB-04-CCO-04

Pre-registro a programas especiales de la DCB

1. El modelo de control de acceso está basado en usuario y contraseña.
   - ✓ ¿Cuenta con un sistema operativo de red instalado en sus equipos? Sí
   - ✓ ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Sí
   - ✓ ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? No
   - ✓ El sistema no permite perfiles distintos.
   - ✓ El acceso de los usuarios es vía web, mediante nombre de usuario y contraseña.

6.VIII.- PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

DCB-04-CCO-04

Pre-registro a programas especiales de la DCB

Se realizan únicamente al finalizar cada periodo de pre-rregistro, de forma manual. Los respaldos se conservan en nube privada; ocasionalmente algunos de los respaldos se conservan también en un disco duro portátil que se resguarda en el cubículo de la Coordinación de Cómputo. El responsable de realizar los respaldos es el encargado principal del sistema.

NO SE CUENTAN CON DOS LUGARES QUE CUMPLAN CON LAS CONDICIONES DE SEGURIDAD ESPECIFICADAS EN EL ARTICULADO DEL CAPÍTULO V DE LOS LINEAMIENTOS

6.IX.- PLAN DE CONTINGENCIA

DCB-04-CCO-04

Pre-registro a programas especiales de la DCB

No se tiene formulado por escrito un plan de contingencia. Si ocurre un incidente de pérdida de datos por daño del servidor, el encargado principal del sistema en conjunto con el Administrador del servidor, recurren a restaurarlo en un servidor alterno provisional mediante la recuperación del último respaldo conocido. Posteriormente, analiza las causas y procede a aplicar medidas correctivas y preventivas en el servidor de producción y reactivar el sistema en su servidor original.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-04-CCO-04	
(Nombre del sistema)*	**Pre-registro a programas especiales de la DCB**	
Recurso*	**Descripción***	**Control***
Pruebas del sistema	Revisión aleatoria	Revisar de manera regular la funcionalidad con el fin de indagar si hubiera algún hueco de inseguridad en la aplicación. Responsables: Edwin Caballero Díaz Irene Patricia Valdez y Alfaro

7.2. Procedimiento para la revisión de las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-04-CCO-04	
(Nombre del sistema)*	**Pre-registro a programas especiales de la DCB**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	Edwin Caballero Díaz Irene P. Valdez y Alfaro
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo	Janete Mejía Jiménez

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-04-CCO-04	
(Nombre del sistema)*	**Pre-registro a programas especiales de la DCB**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema	Edwin Caballero Díaz Irene P. Valdez y Alfaro

	cuentan con los privilegios correspondientes.	
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Janete Mejía Jiménez

7.4. Acciones para la corrección y actualización de las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-04-CCO-04	
(Nombre del sistema)*	**Pre-registro a programas especiales de la DCB**	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL (Próximamente)	Realizar la renovación trimestral del certificado SSL para el subdominio donde se encuentra el sistema.	Janete Mejía Jiménez Edwin Caballero Díaz
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la última versión estable.	Janete Mejía Jiménez Edwin Caballero Díaz

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-04-CCO-04		
(Nombre del sistema)*	**Pre-registro a programas especiales de la DCB**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La importancia de la protección de datos personales Seminario cursado por la responsable de red de la DCB, por lo que aplica para todos los sistemas.	Seminario en línea	1 hora. Fecha:16 de junio de 2022	Seminario cursado por la responsable de red de la DCB, por lo que aplica para todos los sistemas de la DCB que manejan datos personales.

8.2. Programa de difusión de la protección a los datos personales

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-04-CCO-04		
(Nombre del sistema)*	**Pre-registro a programas especiales de la DCB**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difundir Aviso de privacidad	En todas las páginas de acceso a los datos se incluye el aviso de privacidad	Permanente	Toda la comunidad de la División y Público en general que consulta nuestros sitios

9. MEJORA CONTINUA

No se tiene formulado por escrito un programa para la mejora continua, pero se describe las actividades que se realizan regularmente para dar continuidad a los servicios.

9.1. Actualización y mantenimiento de sistemas de información

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-04-CCO-04		
(Nombre del sistema)*	**Pre-registro a programas especiales de la DCB**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Programación de interfaz	Diseño de una interfaz para que el usuario pueda cambiar o recuperar su contraseña de manera segura.	No definida	Acceso más seguro al sistema.

9.2. Actualización y mantenimiento de equipo de cómputo

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-04-CCO-04		
(Nombre del sistema)*	**Pre-registro a programas especiales de la DCB**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Servicio de mantenimiento preventivo al Hardware del servidor, contratado con proveedor externo.	Puntual, una vez al año	Se realiza mantenimiento preventivo al Hardware del servidor con el fin de evitar posibles daños y pérdida de disponibilidad del sistema.

9.3. Procesos para la conservación, preservación y respaldos de información

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-04-CCO-04	
(Nombre del sistema)*	**Pre-registro a programas especiales de la DCB**	
Proceso	**Descripción***	**Responsable**
Respaldo de base de datos y archivos del servidor	Se realizan respaldos de la base de datos función de los periodos de programas especiales.	Irene P. Valdez y Alfaro para los datos de estudiantes.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-04-CCO-04	
(Nombre del sistema)*	**Pre-registro a programas especiales de la DCB**	
Proceso	**Descripción***	**Responsable**
No se cuenta con proceso de borrado seguro		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

DCB-04-CCO-04

Pre-registro a programas especiales de la DCB

No se cuenta actualmente con un mecanismo definido formalmente para la supresión del sistema.

INSCRIPCIÓN A CURSOS EXTRACURRICULARES DE LA DCB

Automatiza los procesos de inscripción a eventos (académicos) de formación complementaria de las diferentes coordinaciones de la DCB. Gestiona diferentes tipos de eventos como cursos (para estudiantes y académicos), actividades complementarias (para estudiantes), entre otros. Permite el registro a estos eventos a estudiantes de la facultad de ingeniería, Académicos que se encuentren laborando en la División de Ciencias Básicas y al público en general. Los eventos a los que se tenga acceso para su registro dependerán del rol de cada uno de los usuarios, por ejemplo, los usuarios que ingresen como Alumnos de la Facultad de Ingeniería, así como los que ingresen como público en general, tendrán acceso a los eventos que son destinados para alumnos, por otra parte, los usuarios que ingresen como Académicos de la DCB, tendrán acceso a los eventos destinados para académicos. Además, el sistema permite que cada usuario consulte su historial de cursos que han sido registrados en este.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

DCB-05-CCO-05 Inscripción a Cursos

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único*	DCB-05-CCO-05
(Nombre del sistema) *	**Inscripción a cursos extracurriculares de la DCB**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, número de cuenta (alumnos UNAM), número de trabajador (Académicos de la DCB), RFC (Académicos de la DCB), correo, fecha de nacimiento, género,
Responsable*:	**División de Ciencias Básicas**
Nombre*:	**Mtra. Irene Patricia Valdez y Alfaro**
Cargo*:	Coordinadora de computo
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se le da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
Encargados:	
(Nombre del Encargado 1*)	**Ing. Edwin Díaz Caballero**
Cargo*:	Ayudante de profesor
Funciones*:	Realizar el proceso de software con la finalidad de atender las necesidades administrativas relacionadas con la DCB.
Obligaciones*:	Procurar la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento.
(Nombre del Encargado 2*)	M. I. Janete Mejía Jiménez
Cargo*:	Técnico Académico
Funciones*:	Administración del servidor.

	Administración del sistema de bases de datos. Dar de alta y controlar acceso de usuarios de las bases de datos.
Obligaciones*:	Administrar el servidor que aloja al sistema, administrar las bases de datos del servidor. Procurar la protección de datos contenidos en el servidor con estrategias y mecanismos de seguridad. Mantener un registro de usuarios con acceso al servidor y a las bases de datos (nombre de la persona, nombre de usuario, contraseñas otorgadas y privilegios). Realizar el monitoreo de incidentes en el servidor y aplicar las políticas de seguridad pertinentes para evitar ataques. Registrar y reportar incidentes de seguridad.
	Usuarios:
(Nombre del Usuario*)	Estudiantes, profesores y Público en General
Cargo*:	Usuario estudiante
Funciones*:	Ingresar al sistema para inscribirse en los cursos de su interés.
Obligaciones*:	Proteger, no compartir y mantener resguardada la información de su cuenta de acceso al sistema.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

DCB-05-CCO-05

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único¨*	DCB-05-CCO-05
(Nombre del sistema *)	**Inscripción a cursos extracurriculares de la DCB**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos relacional con interfaz de acceso por web y manejador de bases de datos.
Características del lugar donde se resguardan los soportes:*	Los soportes se encuentran en 2 lugares (lógicos) diferentes, en ambos casos son servidores web y de base de datos conjuntos, para el caso donde los usuarios son alumnos y público en general, y los registros de inscripción, los datos no viajan por las redes, se hace mediante una conexión directa con el soporte ya que el soporte y el sistema se encuentran en el mismo equipo. Para el caso de los usuarios académicos, el tipo de conexión es indirecta, los datos viajan del servidor del sistema al router (en la intranet sin salir a internet), y del router al otro servidor interno donde se encuentra ese soporte y viceversa cuando se trata de solicitudes que requieren respuesta.

3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

5. PLAN DE TRABAJO

[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

6.I.- TRANSFERENCIAS DE DATOS PERSONALES

DCB-05-CCO-05

División de Ciencias Básicas - Coordinación de Cómputo	
Identificador único*	**DCB-05-CCO-05**
(Nombre del sistema)*	**Inscripción a cursos extracurriculares de la DCB**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza transferencia de datos personales en soportes físicos

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en la página 523.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Transferencias mediante el traslado de soportes electrónicos:	No se realiza transferencia de datos en soportes electrónicos (USB's, CD's, etc).
Transferencias mediante el traslado sobre redes electrónicas:	No sed realiza transferencia de datos por redes electrónicas. El funcionario interesado debe consultar la información que requiera a través del sistema SII-DCB.

6.II.- RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

DCB-05-CCO-05

Inscripción a cursos extracurriculares de la DCB

1. Salvo los respaldos periódicos del sistema en disco duro portátil y en la nube; no se almacenan los datos personales en ningún otro tipo de soporte físico. El disco duro de respaldo se resguarda en el cubículo de la Coordinación de Cómputo.
2. Tienen acceso a los respaldos en la nube y en disco duro:

Mtra. Irene Patricia Valdez y Alfaro.	Coordinadora de Cómputo
M.I. Janete Mejía Jiménez.	Técnica Académica y Web Master
Sr. Edwin Caballero Díaz.	Ayudante de la Profesor de la Coord. de Cómputo
Sr. Ariel Juárez Jiménez.	Ayudante de la Profesor de la Coord. de Cómputo

6.III.- BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

DCB-05-CCO-05

Inscripción a cursos extracurriculares de la DCB

A nivel servidor, se registran bitácoras de sucesos. Las bitácoras de servidor se revisan ocasionalmente o puntualmente en caso de atención incidentes.

6.IV.- REGISTRO DE INCIDENTES:

DCB-05-CCO-05

Inscripción a cursos extracurriculares de la DCB

Cuando ocurre un incidente: Falta de disponibilidad del sistema, o sospecha de intrusión o aviso de detección de vulnerabilidad por parte de DGTIC, el encargado del sistema procede a realizar la revisión y en su caso, aplicar las acciones correctivas para prevenir futuros incidentes.

En caso de que incidente sea catastrófico con pérdida de datos, se procede a restaurar el sistema a partir del último respaldo conocido.

6.V.- ACCESO A LAS INSTALACIONES

DCB-05-CCO-05

Inscripción a cursos extracurriculares de la DCB

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

El acceso a las instalaciones exteriores es libre, no se controla.
La Secretaría Administrativa de la Facultad ha colocado cámaras de video vigilancia en algunos puntos críticos.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de da para soportes electrónicos):

Para los servidores alojados en la DCB:

El acceso al site en el que se localizan los servidores está limitado, mediante llave, a personas que son responsables de su administración:

- Cecilia Teresa Carmona Téllez, Técnica Académica
- Alejandro Rodríguez Rodríguez, Técnic0 Académic0
- Janete Mejía Jiménez, Técnica Académica
- Irene Patricia Valdez y Alfaro, Técnica Académica y Coordinadora de Cómputo.
- Ayudantes de Profesor de la Coordinación, bajo la supervisión de alguno de los técnic académicos.

Para los servidores alojados en el centro de datos de la Facultad:

La Unidad de servicios de Cómputo Académico (UNICA) es las responsable del control acceso.

6.VI.- ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

DCB-05-CCO-05

Inscripción a cursos extracurriculares de la DCB

Anualmente se solicita a la Secretaría de Servicios Académicos de la Facultad el listado de estudiantes de nuevo ingreso, con lo que se realiza una actualización incremental a la base de datos de alumnos a la cual accede el sistema. En caso de que algún alumno solicite corrección de sus datos, se le solicita mostrar un comprobante oficial donde aparezca el dato correcto y se procede por parte del administrador a actualizar el registro correspondiente en la base de datos.

Las medidas de seguridad previstas que se aplican para soportes electrónicos

6. VII.- PERFILES DE USUARIO Y CONTRASEÑAS

DCB-05-CCO-05

Inscripción a cursos extracurriculares de la DCB

1. El modelo de control de acceso está basado en usuario y contraseña.
   - ✓ ¿Cuenta con un sistema operativo de red instalado en sus equipos? Sí
   - ✓ ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Sí
   - ✓ ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? No
   - ✓ El sistema no permite perfiles distintos.
   - ✓ El acceso de los usuarios es vía web, mediante nombre de usuario y contraseña.
   - ✓ El acceso de los administradores a la base de datos es a través de conectores ODBC y manejadores MySQL, mediante usuario, contraseña y VPN

6.VIII.- PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

DCB-05-CCO-05

Inscripción a cursos extracurriculares de la DCB

Se realizan semanalmente respaldos completos, de forma manual. Los respaldos se conservan en nube privada; ocasionalmente algunos de los respaldos se conservan también en un disco duro portátil que se resguarda en el cubículo de la Coordinación de Cómputo. El responsable de realizar los respaldos es el encargado principal del sistema.
NO SE CUENTAN CON DOS LUGARES QUE CUMPLAN CON LAS CONDICIONES DE SEGURIDAD ESPECIFICADAS EN EL ARTICULADO DEL CAPÍTULO V DE LOS LINEAMIENTOS

6.IX.- PLAN DE CONTINGENCIA

DCB-05-CCO-05

Inscripción a cursos extracurriculares de la DCB

No se tiene formulado por escrito un plan de contingencia. Si ocurre un incidente de pérdida de datos por daño del servidor, el encargado principal del sistema en conjunto con el Administrador del servidor, recurren a restaurarlo en un servidor alterno provisional mediante la recuperación del último respaldo conocido. Posteriormente, analiza las causas y procede a aplicar medidas correctivas y preventivas en el servidor de producción y reactivar el sistema en su servidor original.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-05-CCO-05	
(Nombre del sistema)*	**Inscripción a cursos extracurriculares de la DCB**	
Recurso*	**Descripción***	**Control***
Pruebas del sistema	Revisión aleatoria	Revisar de manera regular la funcionalidad con el fin de indagar si hubiera algún hueco de inseguridad en la aplicación. Responsables: Edwin Caballero Díaz Irene Patricia Valdez y Alfaro

7.2. Procedimiento para la revisión de las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-05-CCO-05	
(Nombre del sistema)*	**Inscripción a cursos extracurriculares de la DCB**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	Edwin Caballero Díaz Irene P. Valdez y Alfaro
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo	Janete Mejía Jiménez

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-05-CCO-05	
(Nombre del sistema)*	**Inscripción a cursos extracurriculares de la DCB**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	Edwin Caballero Díaz Irene P. Valdez y Alfaro
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Janete Mejía Jiménez

7.4. Acciones para la corrección y actualización de las medidas de seguridad

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-05-CCO-05	
(Nombre del sistema)*	**Inscripción a cursos extracurriculares de la DCB**	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL (Próximamente)	Realizar la renovación trimestral del certificado SSL para el subdominio donde se encuentra el sistema.	Janete Mejía Jiménez Edwin Caballero Díaz
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la última versión estable.	Janete Mejía Jiménez Edwin Caballero Díaz

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-05-CCO-05		
(Nombre del sistema)*	**Inscripción a cursos extracurriculares de la DCB**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La importancia de la protección de datos personales Seminario cursado por la responsable de red de la DCB, por lo que aplica para todos los sistemas.	Seminario en línea	1 hora. Fecha:16 de junio de 2022	Seminario cursado por la responsable de red de la DCB, por lo que aplica para todos los sistemas de la DCB que manejan datos personales.

8.2. Programa de difusión de la protección a los datos personales

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-05-CCO-05		
(Nombre del sistema)*	**Inscripción a cursos extracurriculares de la DCB**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difundir Aviso de privacidad	En todas las páginas de acceso a los datos se incluye el aviso de privacidad	Permanente	Toda la comunidad de la División y Público en general que consulta nuestros sitios

9. MEJORA CONTINUA

No se tiene formulado por escrito un programa para la mejora continua, pero se describe las actividades que se realizan regularmente para dar continuidad a los servicios.

9.1. Actualización y mantenimiento de sistemas de información

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-05-CCO-05		
(Nombre del sistema)*	**Inscripción a cursos extracurriculares de la DCB**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Programación de interfaz	Diseño de una interfaz para que el usuario pueda cambiar o recuperar su contraseña de manera segura.	No definida	Acceso más seguro al sistema.

9.2. Actualización y mantenimiento de equipo de cómputo

División de Ciencias Básicas - Coordinación de Cómputo			
Identificador único*	DCB-05-CCO-05		
(Nombre del sistema)*	**Inscripción a cursos extracurriculares de la DCB**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	mantenimiento preventivo al Hardware del servidor, contratado con proveedor externo.	Puntual, una vez al año	Se realiza mantenimiento preventivo al Hardware del servidor con el fin de evitar posibles daños y pérdida de disponibilidad del sistema.

9.3. Procesos para la conservación, preservación y respaldos de información

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-05-CCO-05	
(Nombre del sistema)*	**Inscripción a cursos extracurriculares de la DCB**	
Proceso	**Descripción***	**Responsable**
Respaldo de base de datos y archivos del servidor	Se realizan respaldos de la base de datos de en función de los periodos de inscripciones a los cursos. Tiempo máximo de ejecución: en función del tamaño del respaldo.	- Ariel Juárez Jiménez para los datos de académicos - Irene P. Valdez y Alfaro para los datos de estudiantes.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Ciencias Básicas - Coordinación de Cómputo		
Identificador único*	DCB-05-CCO-05	
(Nombre del sistema)*	**Inscripción a cursos extracurriculares de la DCB**	
Proceso	**Descripción***	**Responsable**
No se cuenta con proceso de borrado seguro		

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

DCB-05-CCO-05

Inscripción a cursos extracurriculares de la DCB

No se cuenta actualmente con un mecanismo definido formalmente para la supresión del sistema.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD DE LA DIVISIÓN DE CIENCIAS BÁSICAS

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	(Señalar nombre, puesto, teléfono y correo electrónico del funcionario o empleado universitario que elaboró el documento de seguridad)	 Irene Patricia Valdez y Alfaro Coordinadora de Cómputo en la DCB Tel. 55 5622 81 95 irenev@unam.mx
Revisó:	(Señalar nombre, puesto, teléfono y correo electrónico del funcionario o empleado universitario que revisó el documento de seguridad)	 Ing. Cecilia Teresa Carmona Téllez Técnica Académica Tel. 55 5622 81 95 ctct@unam.mx
Autorizó:	(Señalar nombre, puesto, teléfono y correo electrónico del funcionario o empleado universitario que autorizó el documento de seguridad)	 Dr. Gerardo René Espinosa Pérez Jefe de la División de Ciencias Básicas Tel. 55 5622 81 95 gerardoe@ingenieria.unam.mx
Fecha de aprobación:	(Incluir la fecha de liberación del documento)	17 de agosto de 2022
Fecha de actualización:	(Incluir la primer versión e ir agregando las subsiguientes del documento)	17 de agosto de 2022

DIVISIÓN DE INGENIERÍAS CIVIL Y GEOMÁTICA

-

ÍNDICE

DIVISIÓN DE INGENIERÍAS CIVIL Y GEOMÁTICA

La División de Ingenierías Civil y Geomática (DICYG) apoya académicamente y administrativamente a los alumnos de las carreras de Ingeniería Civil, Ingeniería Geomática e Ingeniería Ambiental. Actualiza y mantiene a la vanguardia los planes y programas de estudio, así como, propone las modificaciones pertinentes para la creación de nuevas asignaturas, acordes a los avances del desarrollo tecnológico que nuestro país vive actualmente.

Apoya ampliamente a la constante actualización y superación de su planta académica que propicien el mejoramiento de las actividades dentro y fuera del salón de clases.
Brinda asesorías, orientación académica, programa de servicio social y prácticas profesionales, orientación y apoyo en el programa de titulación, además de prácticas de campo en donde el estudiante puede aplicar de forma práctica e inmediata todo lo aprendido en el aula escolar, además cuenta con bolsa de trabajo.

Este documento tiene el objetivo de documentar las actividades realizadas para formar parte del Sistema de Gestión de Seguridad de Datos Personales de la DICYG, y que a su vez es revisada y controlada por la UNAM. Se trata de una primera versión del documento, que se enriquecerá conforme se vayan cumpliendo las tareas necesarias y acordes con la reglamentación establecida, también se actualizará conforme se agreguen, editen o termine su tiempo de vida de los desarrollos o procesos mencionados en el presente documento y que se tengan claras las ediciones o modificaciones del tratamiento de datos personales.

El alcance de este sistema se centra en proteger “Todos los datos personales y datos personales sensibles que recabe y trate la DICYG” de accesos no autorizados de tratamientos distintos a los fines para los que fueron recabados.

La División de Ingenierías Civil y Geomática cuenta con diferentes Sistemas y Aplicativos que facilitan la ejecución y seguimiento de los procesos académico-administrativo, algunos de los cuales hacen uso del tratamiento de datos personales de estudiantes, profesores y administrativos.

A continuación se enlistan los sistemas que hacen tratamiento de datos personales en la DICYG:

1. Ambiente Educativo Virtual - AEL
2. Sistema de Horarios DICYG
3. Sistema de Contrataciones

Ambiente Educativo Virtual

El Ambiente Educativo en Línea en esencia es un LMS que fue configurado, personalizado y adaptado específicamente para la División de Ingenierías Civil y Geomática de la Facultad de Ingeniería.

AEL es un Entorno de Aprendizaje Dinámico Modular Orientado a Objetos. Es una plataforma de aprendizaje diseñada para proporcionarle a educadores, administradores y estudiantes un sistema integrado único, robusto y seguro para crear ambientes de aprendizaje personalizados.

Todo es alojado y administrado por la misma División lo cual garantiza que, cada vez que se requiera de nuevas configuraciones, para poder mejorar la experiencia del profesor, se podrían llevar a cabo.

Cualquier profesor de la División, inclusive está abierto para otros profesores de la Facultad, pueden solicitar su inscripción y se les otorga un aula virtual.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingenierías Civil y Geomática	
Identificador único*	DICYG - 01 - Jefatura - 01
(Nombre del sistema) *	**Ambiente Educativo Virtual - AEL**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, Apellidos, correo, ciudad, país.
Responsable*:	Jefatura DICyG
Nombre*:	**M.I. Marco Tulio Mendoza Rosas**
Cargo*:	Jefe de la División de Ingenierías Civil y Geomática
Funciones*:	Tomar las decisiones adecuadas sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, académicas, físicas y administrativas.
	Encargado:
(Nombre del Encargado 1*)	**M.I. Tanya Itzel Arteaga Ricci**
Cargo*:	**Jefa de la Unidad de Cómputo**
Funciones*:	Dar soporte al desarrollo en cómputo necesaria en la División de Ingenierías Civil y Geomática para atender las actividades

	académico-administrativas para las carreras de licenciatura, especialidad y posgrado a cargo de la misma.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias.
(Nombre del Encargado 2*)	Diego Ramírez Romero
Cargo*:	Ayudante de Profesor
Funciones*:	Brindar seguimiento a los procesos de registro de usuarios, calendarizar y efectuar los mantenimientos adecuados y necesarios al sistema.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
	Usuarios:
(Nombre del Usuario 1*)	Académicos que solicitan un aula virtual
Cargo*:	Académicos activos en la UNAM.
Funciones*:	Planificar actividades y material para la impartición de asignaturas.
Obligaciones*:	Cumplir con la obligación legal del manejo de los datos personales de alumnos inscritos a su curso.
(Nombre del Usuario 2*)	Alumnos que solicitan una inscripción a un curso dentro de las aulas virtuales
Cargo*:	Alumnos inscritos a la materia del curso.
Funciones*:	Hacer uso adecuado y académico de la plataforma.
Obligaciones*:	Hacer uso adecuado y académico de la plataforma.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingenierías Civil y Geomática	
Identificador único¨*	DICYG - 01 - Jefatura - 01
(Nombre del sistema *)	**Ambiente Educativo Virtual - AEL**

Tipo de soporte:*	Electrónico.
Descripción:*	Base de datos.
Características del lugar donde se resguardan los soportes:*	Servidores de la División

3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 536 a 538.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

División de Ingenierías Civil y Geomática	
Identificador único*	DICYG - 01 - Jefatura - 01
(Nombre del sistema)*	**Ambiente Educativo Virtual - AEL**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

En el Ambiente Educativo en línea no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema en el servidor.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes. Se considerará como área de oportunidad

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

La división cuenta con un CCTV, 24 horas, ya que para acceder al edificio solo se cuenta con una reja y una puerta de cristal las cuales se encuentran abierta para el ingreso de personal académico, administrativo, y alumnos de 07:00 am a 21:00 pm

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para el acceso a la oficina se requiere identificarse en un biométrico y posteriormente presentarse en el cubículo mencionado, ya que el acceso además incluye llaves físicas.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El sistema tiene la capacidad de hacer la actualización autónomamente, pero también se cuenta con asistencia por parte del administrador si es que el usuario lo requiere. Cotejando la información en la plataforma contra la proporcionada por el usuario.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso:

Basado en roles.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Si

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El sistema tiene la capacidad de que los nuevos usuarios creen su propio usuario, pero también el administrador puede dar de alta a uno o más usuarios.

b) ¿Quién autoriza la creación de nuevos perfiles?
Cuando el administrador crea los usuarios, es obligatorio del profesor del curso.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Se tiene un control de los creados masivamente o por petición de profesor. En el caso de un autorregistro el control lo tienen los logs del sistema.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si

c) ¿Cómo se evita el acceso remoto no autorizado?
Mediante la implementación de llaves en la conexión ssh.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. **Señalar si realiza respaldos**
   Se realizan respaldos completos de forma manual semestralmente.
2. **El tipo de medios que utiliza para almacenar las copias de seguridad**
   El volcado de las copias de seguridad se realiza en los servidores de la División.
3. **Cómo y dónde archivar esos medios.**
   Mediante las actividades de copia de respaldo de sistemas LMS en servidores de la División.
4. **Quién es el responsable de realizar estas operaciones.**

   Personal de la Unidad de Cómputo

IX. PLAN DE CONTINGENCIA

Se cuenta con una réplica total de la plataforma en otro servidor y en otro cuarto de telecomunicaciones, pero dentro de la misma División. Esto con la finalidad de realizar un cambio, en caso de pérdida de conexión, daño físico o fallas en el sistema operativo del servidor principal. Esta réplica es un sitio alterno

caliente y basta efectuar el redireccionamiento de la IP pública a la IP interna del sitio alterno. Este procedimiento lo realizará personal de la Unidad de Cómputo en un lapso no mayor a 24 horas.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 01 - Jefatura - 01	
(Nombre del sistema)*	**Ambiente Educativo Virtual - AEL**	
Recurso*	**Descripción***	**Control***
Bitácora del Sistema	Revisión Aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones. Responsable:Diego Ramírez Romero

7.2. Procedimiento para la revisión de las medidas de seguridad

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 01 - Jefatura - 01	
(Nombre del sistema)*	**Ambiente Educativo Virtual - AEL**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Navegación segura del sitio	Verificación y revisión de dominio del sitio.	Responsable: Diego Ramirez Romero

		Tiempo de revisión: 1 dia hábil
Prueba de servidor SSL	Verificación y revisión de tecnología implementada en el servidor.	Responsable: Diego Ramirez Romero Tiempo de revisión: 1 dia hábil
Notas de seguridad del código fuente del sitio	Determinar las vulnerabilidades de las versiones listadas en las notas de seguridad.	Responsable: Diego Ramirez Romero Tiempo de revisión: 1 dia hábil

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 01 - Jefatura - 01	
(Nombre del sistema)*	**Ambiente Educativo Virtual - AEL**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Navegación segura del sitio	Renovación automática de certificados SSL.	Responsable: Diego Ramirez Romero Tiempo de revisión: 1 día hábil
Prueba de servidor SSL	Configuración de tecnología que soporta navegadores actuales.	Responsable: Diego Ramirez Romero Tiempo de revisión: 1 día hábil
Notas de seguridad del código fuente del sitio	Se instalarán las versiones estables del código fuente del sitio.	Responsable: Diego Ramirez Romero Tiempo de revisión: 1 día hábil

7.4. Acciones para la corrección y actualización de las medidas de seguridad

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 01 - Jefatura - 01	
(Nombre del sistema)*	**Ambiente Educativo Virtual - AEL**	
Medida de seguridad*	**Acciones***	**Responsable***
Estatus de certificados SSL	Revisión de vigencia de certificados SSL	Responsable: Diego Ramirez Romero Tiempo de revisión: 1 día hábil
Tecnología implementada en el servidor WEB.	Configuración de tecnología implementada en el servidor WEB.	Responsable: Diego Ramirez Romero Tiempo de revisión: 1 día hábil

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

División de Ingenierías Civil y Geomática			
Identificador único*	DICYG - 01 - Jefatura - 01		
(Nombre del sistema)*	**Ambiente Educativo Virtual - AEL**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación en la actualización y respaldo de la plataforma.	Las actividades de actualización y respaldo se realizan	Duración 8 Horas	Prestadores de servicio social cuya vigencia es de 6 meses.

	en un servidor de pruebas.		
Capacitación en la instalación de sistema LAMP	La instalación del sistema se realiza en un entorno virtual.	Duración 24 Horas	Prestadores de servicio social cuya vigencia es de 6 meses.

8.2. Programa de difusión de la protección a los datos personales

No se cuenta con un programa de difusión de la protección de datos personales. Se siguen las políticas de tratamiento de datos personales que marque la Facultad de Ingeniería.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

División de Ingenierías Civil y Geomática			
Identificador único*	DICYG - 01 - Jefatura - 01		
(Nombre del sistema)*	**Ambiente Educativo Virtual - AEL**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Instalación de Actualizaciones a código fuente	Revisión de versión del código fuente.	1 Día hábil	BackEnd del código fuente de la plataforma.
Actualización de herramientas base del sistema operativo.	Mantener en las más recientes versiones las herramientas del sistema operativo	1 Día hábil	Herramientas mínimas para el correcto funcionamiento del sitio.
Actualización de Plugins	Revisión y actualización de Plugins	1 Día hábil	BackEnd y FrontEnd de los complementos de la plataforma.

9.2. Actualización y mantenimiento de equipo de cómputo

División de Ingenierías Civil y Geomática			
Identificador único*	DICYG - 01 - Jefatura - 01		
(Nombre del sistema)*	**Ambiente Educativo Virtual - AEL**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se han asignado recursos para la actualización del equipo de cómputo.

9.3. Procesos para la conservación, preservación y respaldos de información

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 01 - Jefatura - 01	
(Nombre del sistema)*	**Ambiente Educativo Virtual - AEL**	
Proceso*	**Descripción***	**Responsable***
Plan de respaldos de la Información	Se realiza una verificación regular de que el contenido de los respaldos de información es accesible.	Responsable: Diego Ramirez Romero Tiempo de revisión: 1 día hábil

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Ingenierías Civil y Geomática	
Identificador único*	DICYG - 01 - Jefatura - 01
(Nombre del sistema)*	**Ambiente Educativo Virtual - AEL**

Proceso*	Descripción*	Responsable*
Validación de usuarios y aulas.	Se verifica el tiempo inactivo del usuario y/o de un aula. El tiempo mínimo para su eliminación es de mayor igual a un año de inactividad.	Responsable: Diego Ramirez Romero Tiempo de revisión: 1 día hábil

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

1. El jefe de la División deberá solicitar la cancelación por escrito al responsable del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.
2. El responsable del sistema deberá realizar la suspensión de las credenciales de acceso al sistema o en su caso, bloquear el apartado de inicio de sesión del mismo.
3. El responsable del sistema deberá notificar al Jefe de la División de las acciones realizadas para lograr la cancelación temporal del sistema.
4. Una vez transcurrida la temporalidad en que el sistema quedó bloqueado, el encargado del sistema iniciará la eliminación segura del mismo.

Sistema de Horarios

Este sistema se ha venido utilizando desde hace aproximadamente 8 años, para hacer la carga académica del semestre y obtener un reporte en Excel para ser enviado a la Secretaría de Servicios Académicos de la Facultad y de esta forma programar los grupos y salones que se utilizarán durante el semestre.

Durante este periodo fue sometido a una actualización tanto de *front* como de *back end*. En el aspecto visual fue implementado con diseño responsivo, además se incluyeron *banners* y *plugins* para mejorar la interacción del usuario con el sistema.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingenierías Civil y Geomática	
Identificador único*	DICYG - 02 - Jefatura - 02
(Nombre del sistema) *	**Sistema de Horarios**
Datos personales (sensibles o no) contenidos en el sistema*:	Grado Académico, Nombre, Apellido Paterno, Apellido Materno, RFC, Homoclave, Folio, Número de trabajador, CURP.
Responsable*:	Jefatura DICyG
Nombre*:	**M.I. Marco Tulio Mendoza Rosas**
Cargo*:	**Jefe de la División de Ingenierías Civil y Geomática**
Funciones*:	Tomar las decisiones adecuadas sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, académicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	**M.I. Tanya Itzel Arteaga Ricci**
Cargo*:	**Jefa de la Unidad de Cómputo**
Funciones*:	Dar soporte al desarrollo en cómputo necesaria en la División de Ingenierías Civil y Geomática para atender las actividades académico-administrativas para las carreras de licenciatura,

	especialidad y posgrado a cargo de la misma.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias
	Usuarios:
(Nombre del Usuario 1*)	Secretaría Académica
Cargo*:	Secretaría Académica
Funciones*:	Tomar las decisiones adecuadas sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	Decidir a qué usuarios se les da acceso al sistema con privilegios administrativos. Decidir sobre la incorporación de nuevas funcionalidades en el sistema. Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, académicas, físicas y administrativas.
(Nombre del Usuario 2*)	Secretaría Técnica
Cargo*:	Secretaría Técnica
Funciones*:	Establecer las condiciones óptimas de operación para que las actividades académico–administrativas de la División se desarrollen conforme a lo establecido en el proyecto académico-administrativo de la Facultad.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias
(Nombre del Usuario 3*)	Ing. Victor Manuel Martínez
Cargo*:	Jefe del Departamento de Construcción
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de construcción
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 4*)	M.I. Octavio García Domínguez
Cargo*:	Jefe del Departamento de Estructuras

Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de estructuras
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 5*)	M.I. Adolfo Reyes Pizano
Cargo*:	Jefe del Departamento de Geodesia y Cartografía
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de Geodesia y Cartografía
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 6*)	M.I. Juan Luis Umaña Romero
Cargo*:	Jefe del Departamento de Geotecnia
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de Geotecnia
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 7*)	Ing. Jesús Gallegos Silva
Cargo*:	Jefe del Departamento de Hidráulica
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de Hidráulica
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 8*)	Dr. Enrique César Valdéz
Cargo*:	Jefe del Departamento de Sanitaria y Ambiental
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de sanitaria y ambiental
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.

(Nombre del Usuario 9*)	Ing. Heriberto Esquivel Castellanos
Cargo*:	Jefe del Departamento de Ingeniería de Sistemas, Planeación y Transporte
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de Ingeniería de Sistemas, Planeación y Transporte
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 10*)	Jefe del Departamento de Topografía
Cargo*:	Jefe del Departamento de Topografía
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de Topografía
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingenierías Civil y Geomática	
Identificador único¨*	DICYG - 02 - Jefatura - 02
(Nombre del sistema *)	Sistema de Horarios
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Servidores de la División

3. ANÁLISIS DE RIESGOS

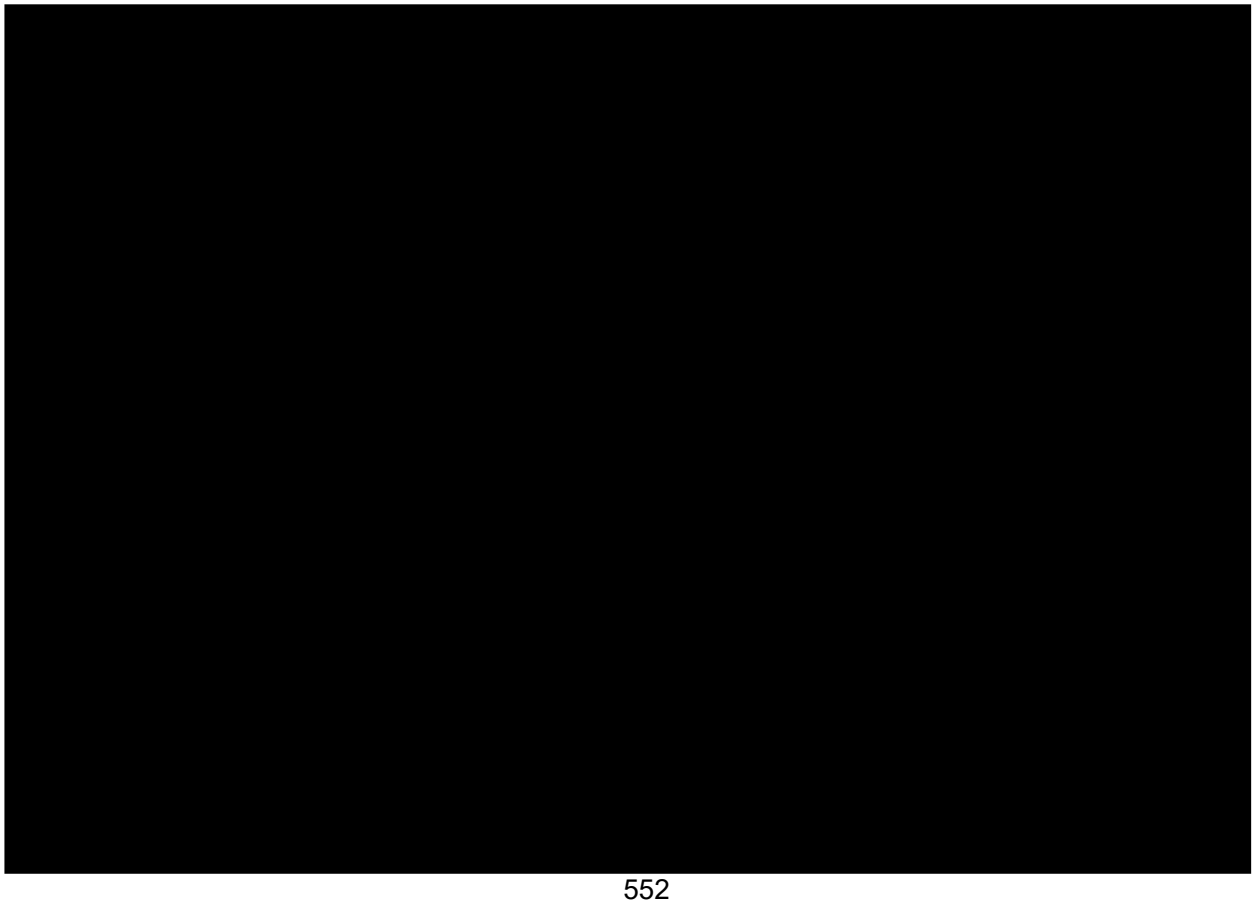
[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 551 a 553.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

División de Ingenierías Civil y Geomática	
Identificador único*	DICYG - 02 - Jefatura - 02
(Nombre del sistema)*	**Sistema de Horarios**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	Se descarga la información procesada del sistema y se carga en el sistema de escolar-ti de la Facultad de Ingeniería
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema de horarios no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Los datos que se registran en las bitácoras:

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema en el servidor.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

La división cuenta con un CCTV, 24 horas, ya que para acceder al edificio solo se cuenta con una reja y una puerta de cristal las cuales se encuentran abierta para el ingreso de personal académico, administrativo, y alumnos de 07:00 am a 21:00 pm

2. **Seguridad perimetral interior**

Para el acceso a la oficina se requiere identificarse en un biométrico y posteriormente presentarse en el cubículo mencionado, con una identificación oficial.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los usuarios que deseen realizar la actualización de sus datos personales deberán acudir con el responsable del sistema.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

Está basado en roles

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?

SI

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
SI

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
SI

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
SI

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
SI

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El responsable del sistema

b) ¿Quién autoriza la creación de nuevos perfiles?
El jefe de la División

c) ¿Se lleva registro de la creación de nuevos perfiles?
Desde el sistema es posible visualizar la creación de perfiles

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema desde cualquier dispositivo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
SI

c) ¿Cómo se evita el acceso remoto no autorizado?
Se tiene un control de acceso basado en llaves cifradas

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos: X, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual _X__,
   c) Periodicidad con que los realiza: Semestral _____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad. **Disco Duro Mecánico**
3. Cómo y dónde archiva esos medios, **NAS de la División**
4. Quién es el responsable de realizar estas operaciones **El área universitaria**

IX. PLAN DE CONTINGENCIA

Se cuenta con algunas medidas de seguridad que se especifican en este documento, se está trabajando en un nuevo esquema y planes de seguridad.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 02 - Jefatura - 02	
(Nombre del sistema)*	Sistema de Horarios	
Recurso*	**Descripción***	**Control***
Bitácora del Sistema	Revisión Aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones. Responsable:M.I. Tanya Itzel Arteaga Ricci

7.2 Procedimiento para la revisión de las medidas de seguridad

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 02 - Jefatura - 02	
(Nombre del sistema)*	**Sistemas de Horarios**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Plan de respaldos de la Información	Verificación y revisión de respaldos del Sistema	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil

Actualización de Software	Revisión y actualización de Software	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil
Instalación de Actualizaciones a Software antimalware	Revisión del software antimalware	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 02 - Jefatura - 02	
(Nombre del sistema)*	**Sistema de Horarios**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Plan de respaldos de la Información	Verificación y revisión de respaldos del Sistema	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil
Instalación de Actualizaciones a Software antimalware	Revisión del software antimalware	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil
Actualización de Software	Revisión y actualización de Software	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil

7.4 Acciones para la corrección y actualización de las medidas de seguridad

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 02 - Jefatura - 02	
(Nombre del sistema)*	**Sistema de Horarios**	
Medida de seguridad*	**Acciones***	**Responsable***
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la última versión estable disponible a petición del responsable del sistema.	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

No se cuenta con un programa de capacitación para los responsables, se toma como un área de oportunidad.

División de Ingenierías Civil y Geomática			
Identificador único*	DICYG - 02 - Jefatura - 02		
(Nombre del sistema)*	**Sistema de Horarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No aplica para los usuarios, ya que no se han realizado capacitaciones del sistema

8.2. Programa de difusión de la protección a los datos personales

División de Ingenierías Civil y Geomática

Identificador único*	DICYG - 02 - Jefatura - 02
(Nombre del sistema)*	**Sistema de inscripciones al Laboratorio de Hidráulica**

Actividad*	Descripción*	Duración*	Cobertura*

Se siguen las políticas de tratamiento de datos personales que marque la Facultad de Ingeniería.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

División de Ingenierías Civil y Geomática	
Identificador único*	DICYG - 02 - Jefatura - 02
(Nombre del sistema)*	**Sistema de Horarios**

Actividad*	Descripción*	Duración*	Cobertura*
Revisión, actualización y mantenimiento del sistema de horarios	1. Actualización de la base de datos 2. Realizar pruebas de funcionalidad en busca de errores, bugs o problemas de compatibilidad como consecuencia de las actualizaciones anteriores 3. Corregir y/o refactorizar características del sistema.	3 meses	BackEnd de la aplicación: tecnologías de desarrollo.

	4. Aplicar modificaciones solicitadas y verificar el correcto funcionamiento		

9.2. Actualización y mantenimiento de equipo de cómputo

División de Ingenierías Civil y Geomática			
Identificador único*	DICYG - 02 - Jefatura - 02		
(Nombre del sistema)*	**Sistema de Horarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se han asignado recursos para la actualización del equipo de cómputo.

9.3. Procesos para la conservación, preservación y respaldos de información

Jefatura		
Identificador único*	DICYG - 02 - Jefatura - 02	
(Nombre del sistema)*	**Sistema de Horarios**	
Proceso*	**Descripción***	**Responsable***
El formato de los archivos de respaldo de información corresponde a información en texto plano.	Se realiza una verificación regular de que el contenido de los respaldos de información es accesible.	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 02 - Jefatura - 02	
(Nombre del sistema)*	**Sistema de Horarios**	
Proceso*	**Descripción***	**Responsable***

No se cuenta con un proceso para borrados seguro y disposición final de equipos

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

1. El Jefe de la División deberá solicitar la cancelación por escrito al encargado del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.
2. El responsable del sistema deberá realizar la suspensión de las credenciales de acceso al sistema o en su caso, bloquear el apartado inicio de sesión del mismo.
3. El responsable del sistema deberá notificar al Jefe de la División de las acciones realizadas para lograr la cancelación temporal del sistema.
4. El responsable del sistema notificará al Jefe de la División de que el sistema ha sido cancelado.

SISTEMA DE CONTRATACIONES

Este sistema es utilizado para capturar la información de los trabajadores académicos y sus contrataciones. De esta manera se tiene un mejor control de la información actual e histórica del personal académico y se identifica de manera más sencilla si hay algún problema con alguna contratación para poder corregirse.

El sistema fue sometido a varias mejoras de *back end* y *front end* respecto al año anterior que se encontraba en desarrollo, incluso fue rebautizado de “Sistema de Contrataciones” a “SIPAC”.

Actualmente el sistema ya está siendo funcional al 100% y es adaptado por todos los jefes de departamento de la División.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingenierías Civil y Geomática	
Identificador único*	DICYG - 03 - Jefatura - 03
(Nombre del sistema) *	**Sistema de Contrataciones**
Datos personales (sensibles o no) contenidos en el sistema*:	RFC, CURP, Nombre, Apellido Paterno, Apellido Materno, Sexo, Estado Civil, Nacionalidad, Calle, Número, Colonia, Alcaldía Ciudad, Código Postal, Teléfono de casa, Teléfono Celular, Teléfono de Oficina, Correo Electrónico.
Responsable*:	Jefatura DICyG
Nombre*:	**M.I. Marco Tulio Mendoza Rosas**
Cargo*:	Jefe de la División de Ingenierías Civil y Geomática
Funciones*:	Tomar las decisiones adecuadas sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, académicas, físicas y administrativas.
	Encargado:
(Nombre del Encargado 1*)	**M.I. Tanya Itzel Arteaga Ricci**
Cargo*:	**Jefa de la Unidad de Cómputo**

Funciones*:	Dar soporte al desarrollo en cómputo necesario en la División de Ingenierías Civil y Geomática para atender las actividades académico-administrativas para las carreras de licenciatura, especialidad y posgrado a cargo de la misma.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias.
	Usuarios:
(Nombre del Usuario 1*)	Secretaría Académica
Cargo*:	Secretaría Académica
Funciones*:	Tomar las decisiones adecuadas sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	Decidir a qué usuarios se les da acceso al sistema con privilegios administrativos. Decidir sobre la incorporación de nuevas funcionalidades en el sistema. Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, académicas, físicas y administrativas.
(Nombre del Usuario 2*)	Secretaría Técnica
Cargo*:	Secretaría Técnica
Funciones*:	Establecer las condiciones óptimas de operación para que las actividades académico–administrativas de la División se desarrollen conforme a lo establecido en el proyecto académico-administrativo de la Facultad.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias
(Nombre del Usuario 3*)	Ing. Victor Manuel Martínez
Cargo*:	Jefe del Departamento de Construcción
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de construcción
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.

(Nombre del Usuario 4*)	M.I. Octavio García Domínguez
Cargo*:	Jefe del Departamento de Estructuras
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de estructuras
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 5*)	M.I. Adolfo Reyes Pizano
Cargo*:	Jefe del Departamento de Geodesia y Cartografía
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de Geodesia y Cartografía
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 6*)	M.I. Juan Luis Umaña Romero
Cargo*:	Jefe del Departamento de Geotecnia
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de Geotecnia
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 7*)	Ing. Jesús Gallegos Silva
Cargo*:	Jefe del Departamento de Hidráulica
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de Hidráulica
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 8*)	Dr. Enrique César Valdéz
Cargo*:	Jefe del Departamento de Sanitaria y Ambiental
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de sanitaria y ambiental

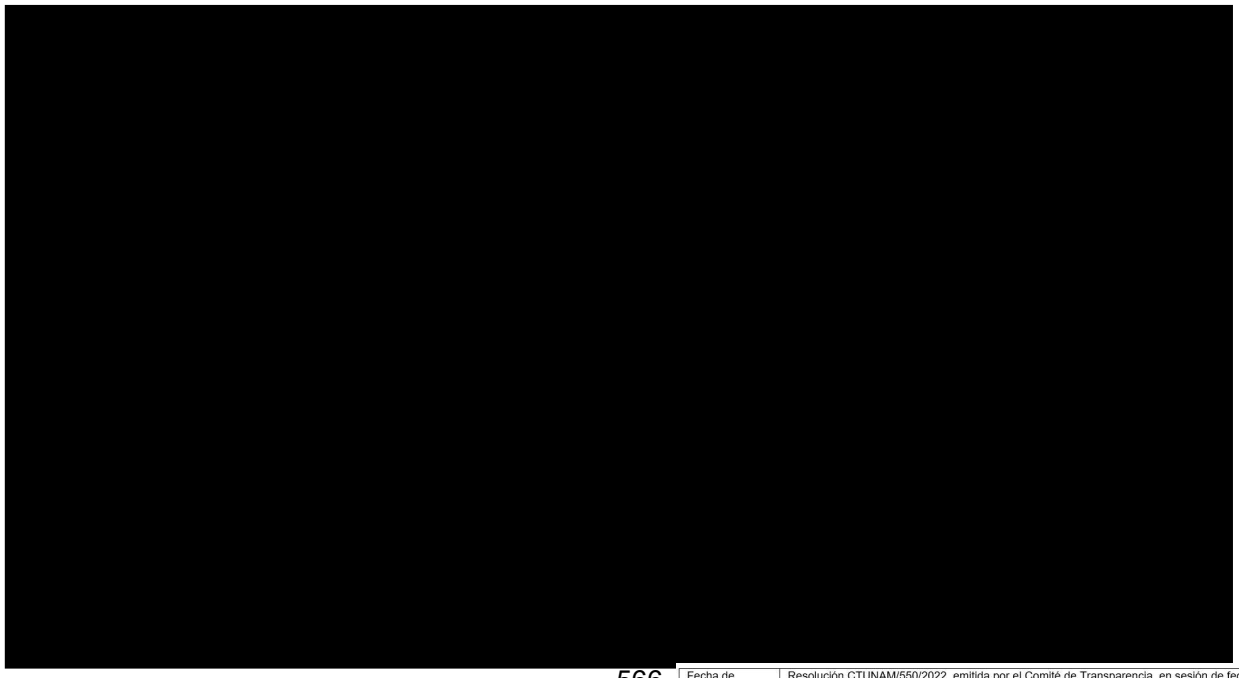
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 9*)	Ing. Heriberto Esquivel Castellanos
Cargo*:	Jefe del Departamento de Ingeniería de Sistemas, Planeación y Transporte
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de Ingeniería de Sistemas, Planeación y Transporte
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 10*)	Jefe del Departamento de Topografía
Cargo*:	Jefe del Departamento de Topografía
Funciones*:	Brindar seguimiento a los procesos de registro de asignaturas del departamento de Topografía
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingenierías Civil y Geomática	
Identificador único¨*	DICYG - 03 - Jefatura - 03
(Nombre del sistema *)	**Sistema de Contrataciones**
Tipo de soporte:*	Electrónico.
Descripción:*	Base de datos.
Características del lugar donde se resguardan los soportes:*	Servidores de la División

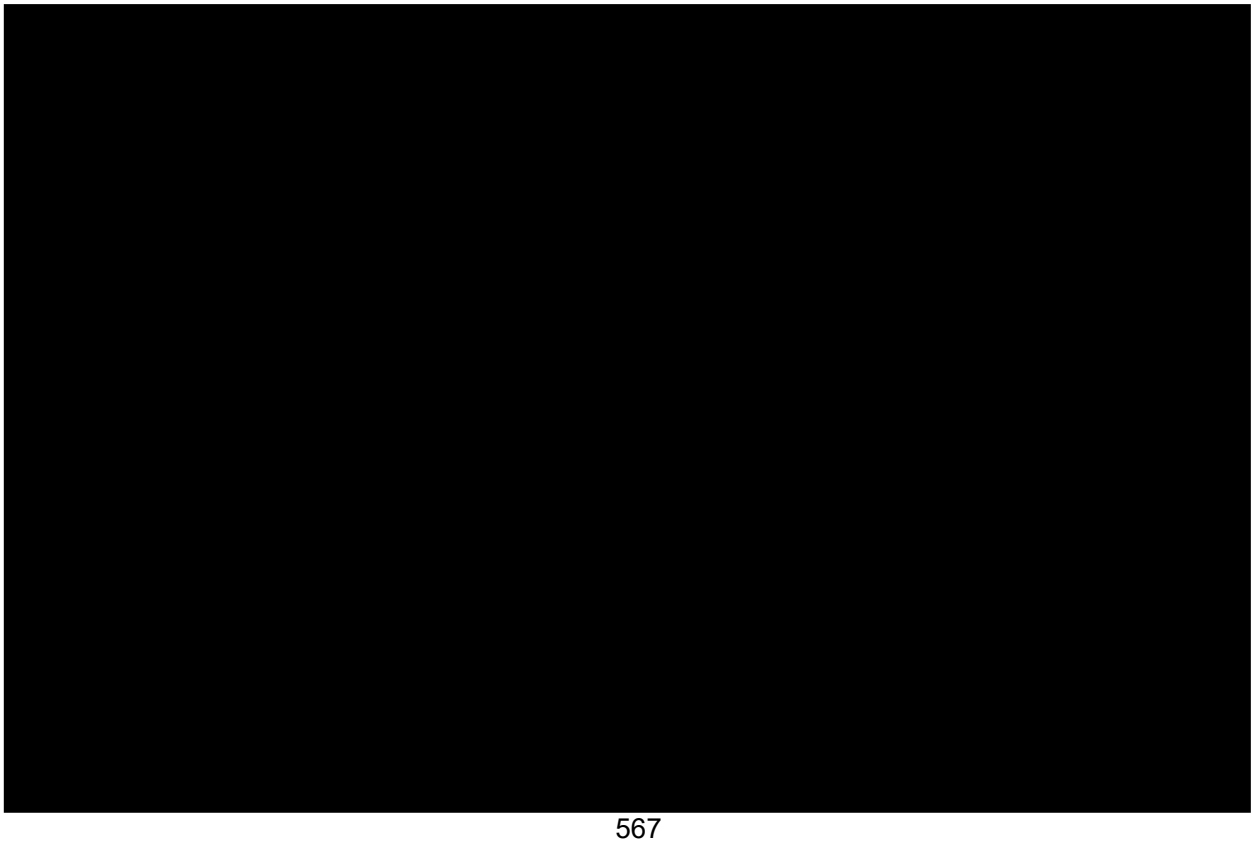
3. ANÁLISIS DE RIESGOS

4. ANÁLISIS DE BRECHA



Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 566 a 568.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO



[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

División de Ingenierías Civil y Geomática	
Identificador único*	DICYG - 03 - Jefatura - 03
(Nombre del sistema)*	**Sistema de Contrataciones**

TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

En el Sistema de Horarios no se realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Los datos que se registran en las bitácoras:

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema en el servidor.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes. se considerará como área de oportunidad

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

La división cuenta con un CCTV, 24 horas, ya que para acceder al edificio solo se cuenta con una reja y una puerta de cristal las cuales se encuentran abierta para el ingreso de personal académico, administrativo, y alumnos de 07:00 am a 21:00 pm

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para el acceso a la oficina se requiere identificarse en un biométrico y posteriormente presentarse en el cubículo mencionado, ya que el acceso además incluye llaves físicas.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los usuarios que deseen realizar la actualización de sus datos personales deberán acudir con el responsable del sistema.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso:

Basado en roles.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Si

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?

El responsable del sistema

b) ¿Quién autoriza la creación de nuevos perfiles?

El jefe de la División

c) ¿Se lleva registro de la creación de nuevos perfiles?

Desde el sistema es posible visualizar la creación de perfiles

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?

No, cada usuario puede acceder al sistema desde cualquier dispositivo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?

SI

c) ¿Cómo se evita el acceso remoto no autorizado?

Se tiene un control de acceso basado en llaves cifradas

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   Se realizan respaldos completos de forma manual semestralmente.
2. El tipo de medios que utiliza para almacenar las copias de seguridad
   El volcado de las copias de seguridad se realiza en los servidores de la División.
3. Cómo y dónde archiva esos medios.
   NAS de la División
4. Quién es el responsable de realizar estas operaciones.

   Personal de la Unidad de Cómputo

IX. PLAN DE CONTINGENCIA

Se cuenta con algunas medidas de seguridad que se especifican en este documento, se está trabajando en un nuevo esquema y planes de seguridad.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

División de Ingenierías Civil y Geomática	
Identificador único*	DICYG - 03 - Jefatura - 03

(Nombre del sistema)*	Sistema de Contrataciones	
Recurso*	**Descripción***	**Control***
Bitácora del Sistema	Revisión Aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones. Responsable:M.I. Tanya Itzel Arteaga Ricci

7.2. Procedimiento para la revisión de las medidas de seguridad

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 03 - Jefatura - 03	
(Nombre del sistema)*	**Sistema de Contrataciones**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Plan de respaldos de la Información	Verificación y revisión de respaldos del Sistema	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 dia hábil
Actualización de Software	Revisión y actualización de Software	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 dia hábil
Instalación de Actualizaciones a Software antimalware	Revisión del software antimalware	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 dia hábil

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 03 - Jefatura - 03	
(Nombre del sistema)*	**Sistema de Contrataciones**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Plan de respaldos de la Información	Verificación y revisión de respaldos del Sistema	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil
Instalación de Actualizaciones a Software antimalware	Revisión del software antimalware	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil
Actualización de Software	Revisión y actualización de Software	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil

7.4. Acciones para la corrección y actualización de las medidas de seguridad

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 03 - Jefatura - 03	
(Nombre del sistema)*	**Sistema de Contrataciones**	
Medida de seguridad*	**Acciones***	**Responsable***
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la última versión	Responsable: M.I. Tanya Itzel Arteaga Ricci

	estable disponible a petición del responsable del sistema	Tiempo de revisión: 1 día hábil

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

División de Ingenierías Civil y Geomática			
Identificador único*	DICYG - 03 - Jefatura - 03		
(Nombre del sistema)*	**Sistema de Contrataciones**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación	Capacitación a todos los jefes de la División sobre el uso correcto del sistema	10 horas	Jefes de la División de Ingenierías Civil y Geomática

8.2. Programa de difusión de la protección a los datos personales

División de Ingenierías Civil y Geomática			
Identificador único*	DICYG - 03 - Jefatura - 03		
(Nombre del sistema)*	**Sistema de Contrataciones**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Se siguen las políticas de tratamiento de datos personales que marque la Facultad de Ingeniería.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

División de Ingenierías Civil y Geomática			
Identificador único*	DICYG - 03 - Jefatura - 03		
(Nombre del sistema)*	**Sistema de Contrataciones**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Revisión, actualización y mantenimiento del sistema de contrataciones	1. Actualización de la base de datos 2. Realizar pruebas de funcionalidad en busca de errores, bugs o problemas de compatibilidad como consecuencia de las actualizaciones anteriores 3. Corregir y/o refactorizar características del sistema. 4. Aplicar modificaciones solicitadas y verificar el correcto funcionamiento	3 meses	BackEnd de la aplicación: tecnologías de desarrollo.

9.2. Actualización y mantenimiento de equipo de cómputo

División de Ingenierías Civil y Geomática			
Identificador único*	DICYG - 03 - Jefatura - 03		
(Nombre del sistema)*	**Sistema de Contrataciones**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se han asignado recursos para la actualización del equipo de cómputo.

9.3. Procesos para la conservación, preservación y respaldos de información

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 03 - Jefatura - 03	
(Nombre del sistema)*	**Sistema de Contrataciones**	
Proceso*	**Descripción***	**Responsable***
El formato de los archivos de respaldo de información corresponde a información en texto plano.	Se realiza una verificación regular de que el contenido de los respaldos de información es accesible.	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Ingenierías Civil y Geomática		
Identificador único*	DICYG - 03 - Jefatura - 03	
(Nombre del sistema)*	**Sistema de Contrataciones**	
Proceso*	**Descripción***	**Responsable***

No se cuenta con un proceso para borrados seguro y disposición final de equipos

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

5. El Jefe de la División deberá solicitar la cancelación por escrito al encargado del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.
6. El responsable del sistema deberá realizar la suspensión de las credenciales de acceso al sistema o en su caso, bloquear el apartado inicio de sesión del mismo.
7. El responsable del sistema deberá notificar al Jefe de la División de las acciones realizadas para lograr la cancelación temporal del sistema.
8. El responsable del sistema notificará al Jefe de la División de que el sistema ha sido cancelado.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Diego Ramírez Romero Ayudante de profesor diego.ramirezr@ingenieria.unam.edu Héctor Alejandro Martínez Garduño Ayudante de profesor hector.martinez@ingenieria.unam.edu M.I. Tanya I. Arteaga Ricci Jefa de la Unidad de Cómputo tanya.arteaga@ingenieria.unam.edu	
Revisó:	M.I. Marco Tulio Mendoza Rosas Jefe de la División de Ingenierías Civil y Geomática rockmarc@unam.mx	
Autorizó:	M.I. Marco Tulio Mendoza Rosas Jefe de la División de Ingenierías Civil y Geomática rockmarc@unam.mx	
Fecha de aprobación:	Agosto 17, 2022	
Fecha de actualización:	Agosto 17, 2022	

DIVISIÓN DE INGENIERÍA ELÉCTRICA

ÍNDICE

DIVISIÓN DE INGENIERÍA ELÉCTRICA

La División de Ingeniería Eléctrica de la Facultad de Ingeniería de la UNAM, responsable de las carreras de Ingeniería en Computación, Ingeniería Eléctrica Electrónica e Ingeniería en Telecomunicaciones; debe enfrentar retos que la sociedad demanda en beneficio del país mediante su objetivo fundamental de formar profesionales íntegros, altamente competitivos, capaces de generar y aplicar nuevos conocimientos en beneficio de la humanidad.

Proporcionando a los egresados conocimientos y una educación de alto nivel académico para poder realizar docencia, investigación de vanguardia y difusión de la cultura; todas comprometidas con las necesidades del país y en particular con los sectores industrial, empresarial y gubernamental.

SISTEMA CV

El sistema C.V. reúne el Curriculum Vitae de los académicos que imparten asignaturas correspondientes a los planes de estudio de las carreras de la División de Ingeniería Eléctrica adscritos a esta división.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingeniería Eléctrica	
Identificador único*	DIE-01-DC-01
(Nombre del sistema) *	**C.V.**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre completo, RFC con homoclave, Sexo, Estado civil, Correo electrónico personal, Correo electrónico laboral, Teléfono personal, Teléfono laboral. Domicilio (Ingrese calle, número externo y/o interno, colonia, delegación o municipio y entidad federativa). Número de horas en la UNAM, Número de trabajador, Puesto en la UNAM, Antigüedad, División y Departamento de adscripción, Página web del profesor, Página web institucional, SNI, PRIDE. Trayectoria educativa, títulos, premios, distinciones, superación y actualización académica. Experiencia profesional.
Responsable*:	Facultad de Ingeniería
Nombre*:	Ing. Alberto Templos Carbajal
Cargo*:	Jefe del Departamento de Computación de la División de Ingeniería Eléctrica
Funciones*:	Se decidió la creación y uso del sistema (para CACEI y ANECA), así como la automatización, finalidad y uso de los datos personales.
Obligaciones*:	Establecer usuarios con privilegios de administrador del sistema. Actualizar el sistema para nuevos requerimientos. Resguardar que el sistema formalice todas las medidas de seguridad técnicas físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	Guadalupe Lizeth Parrales Romay
Cargo*:	Profesor de Asignatura A, Ayudante de Profesor A
Funciones*:	Realizar y mantener actualizado el sistema de Curriculum Vitae (C. V.) para el personal académico de la DIE, con la finalidad de apoyar en los procesos de acreditación de CACEI y ANECA.
Obligaciones*:	Proporcionar protección de datos personales de los académicos que resguarda el sistema de C. V. mediante desarrollo y mantenimiento de estrategias de seguridad de software.

	Dar de alta usuarios del sistema C.V. Desarrollar nuevas funcionalidades requeridas para cubrir las solicitudes de procesos de acreditación.
	Usuarios:
(Nombre del Usuario 1*)	Luis Sergio Valencia Castro
Cargo*:	Coordinador de la Carrera de Ingeniería en Computación
Funciones*:	Revisar el registro de los datos del sistema
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 2*)	Alberto Templos Carbajal
Cargo*:	Jefe del Departamento de Computación
Funciones*:	Revisar el registro de los datos del sistema
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
(Nombre del Usuario 3*)	Todos los profesores de la División de Ingeniería Eléctrica
Cargo*:	Profesores de Asignatura y Profesores de Carrera de Tiempo Completo
Funciones*:	Impartir docencia de las asignaturas del Plan de estudios.
Obligaciones*:	Impartir docencia y cumplir con legislación universitaria.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

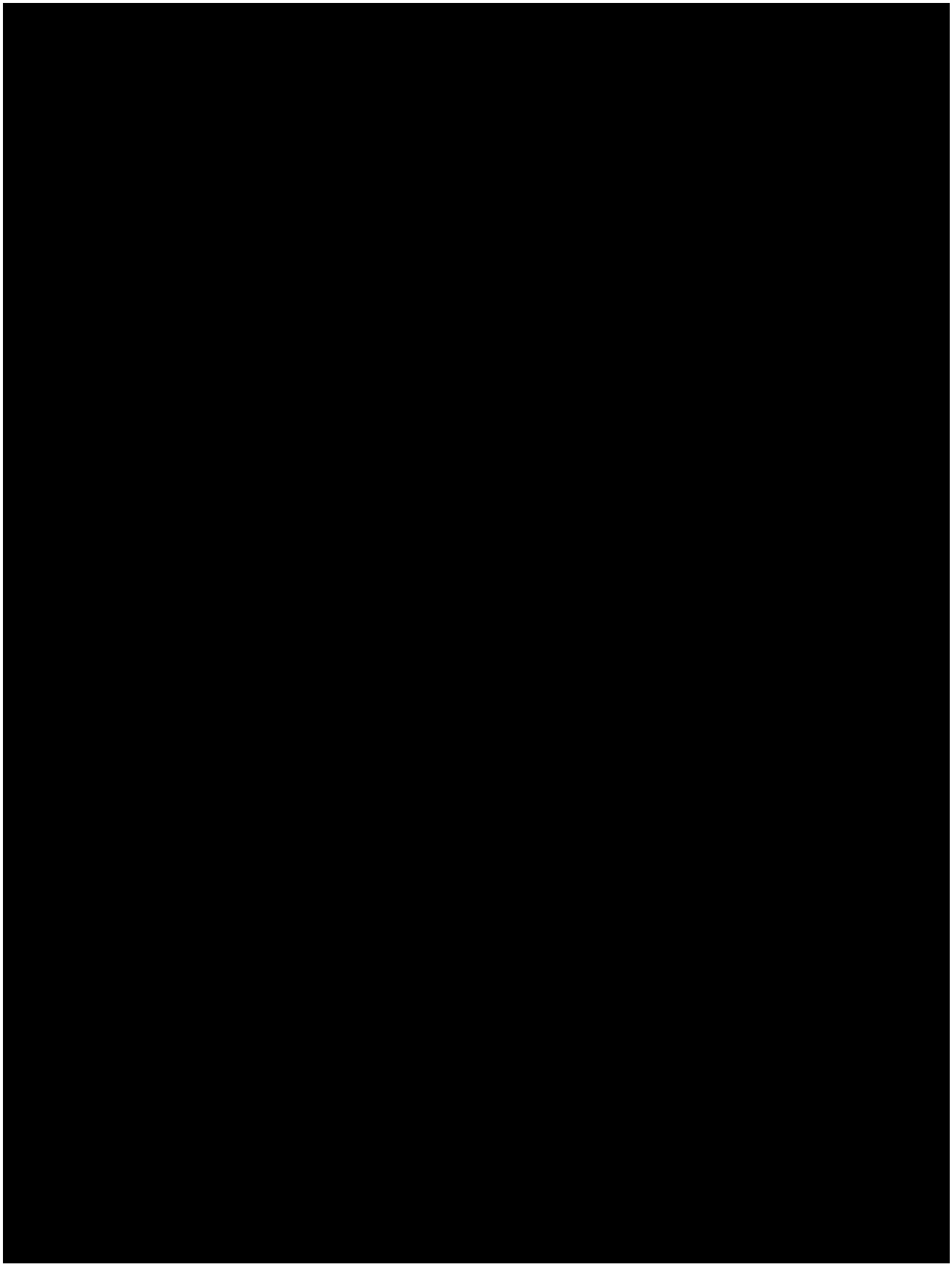
División de Ingeniería Eléctrica*	
Identificador único¨*	DIE-01-DC-01
(Nombre del sistema *)	**C.V.**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Dos Servidores del Departamento de Computación

3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

División de Ingeniería Eléctrica*	
Identificador único*	DIE-01-DC-01
(Nombre del sistema)*	**C.V.**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	Se le proporciona información al área solicitante de las entidades como CACEI y ANECA de manera electrónica mediante un formato específico que brindan las entidades. No se cifra la información. Existe formalidad en las transferencias de datos personales mediante instrumento jurídico, que brinda la acreditación de las carreras por parte de las instituciones CACEI y ANECA.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema de C. V. (Curriculum Vitae) no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos en dos servidores.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No se realizan bitácoras.

IV. REGISTRO DE INCIDENTES:

Procedimiento: Se realiza un respaldo mensual del sistema para permitir la recuperación de los datos del sistema.

1. Los datos que registra:

a) La persona que resolvió el incidente;

El administrador del sistema resuelve el incidente; la solicitud se atiende mediante correo electrónico en el cual el usuario proporciona sus credenciales de acceso o en su defecto una captura de pantalla que muestre el problema**.**

b) La metodología aplicada

Verificar el correcto funcionamiento e integridad de la bases de datos y del sistema web. Determinando si el problema es general o de forma particular.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Se cuenta con un punto de control de acceso al edificio mediante un vigilante para llegar al laboratorio donde se encuentran los servidores, que contienen el sistema de C.V., el laboratorio cuenta con un administrador y ayudantes.

Se cuenta con cámaras de vigilancia.

Sólo personal autorizado e identificado tiene acceso al área de los servidores que contiene el sistema C.V.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Se tienen instalados controles biométricos, el tipo de cerradura es de seguridad, cerradura de pasador, de picaporte y ectópica. Se cuenta con cámaras de vigilancia

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización de los datos contenidos en el sistema de C.V. se realiza cada semestre, mediante solicitud en una junta de departamento. No se validan los datos.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?
c) ¿Está basado en roles (perfiles) o grupos?
d) ¿Está basado en reglas?

El usuario del sistema debe ser un académico que labore en nuestra institución. Se da acceso mediante su número de trabajador y RFC.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Si
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
La administradora del sistema de C.V.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Jefe del Departamento de Computación

c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema con su usuario y contraseña desde cualquier equipo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si

c) ¿Cómo se evita el acceso remoto no autorizado?
El acceso remoto al sistema es mediante usuario y contraseña y perfil de administración.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   - **c)** Completos_X_, diferenciales ___ o incrementales___;
   - **d)** De forma automática ____ o Manual _X____,
   - **e)** Periodicidad con que los realiza: _semestral_____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Se respalda en los discos duros de los servidores, y en el equipo de la administradora del sistema (disco duro y de estado sólido).
3. Cómo y dónde archiva esos medios, y
   En los servidores y en la PC de la administradora del sistema
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   El área responsable es el Departamento de Computación; la administradora del sistema de C.V. Ing. Guadalupe Lizeth Parrales Romay

IX. PLAN DE CONTINGENCIA

No se ha contemplado; se planea realizarlo.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

No existe ningún dispositivo alterno que garantice la disponibilidad del sistema.

División de Ingeniería Eléctrica		
Identificador único*	DIE-01-DC-01	
(Nombre del sistema)*	**C.V.**	
Recurso*	**Descripción***	**Control***
No existe recurso de monitoreo	No hay recurso para revisiones aleatorias y/o pruebas de penetración, etc.	No existe.

7.2. Procedimiento para la revisión de las medidas de seguridad

División de Ingeniería Eléctrica		
Identificador único*	DIE-01-DC-01	
(Nombre del sistema)*	**C.V.**	
Medida de seguridad*	**Procedimiento***	**Responsable***
No existe	No existe	No existe.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

División de Ingeniería Eléctrica		
Identificador único*	DIE-01-DC-01	
(Nombre del sistema)*	**C.V.**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No existe	No existe	No existe.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

División de Ingeniería Eléctrica	
Identificador único*	DIE-01-DC-01

(Nombre del sistema)*	C.V.	
Medida de seguridad*	**Acciones***	**Responsable***
No se ha llevado a cabo	No se ha llevado a cabo	No existe.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

División de Ingeniería Eléctrica			
Identificador único*	DIE-01-DC-01		
(Nombre del sistema)*	C.V.		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No existe	No existe	No existe.	No existe.

8.2. Programa de difusión de la protección a los datos personales

División de Ingeniería Eléctrica			
Identificador único*	DIE-01-DC-01		
(Nombre del sistema)*	C.V.		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se ha implementado	No se ha implementado	No existe.	No existe.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

División de Ingeniería Eléctrica	
Identificador único*	DIE-01-DC-01

(Nombre del sistema)*	C.V.		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Se lleva a cabo el respaldo de la base de datos.	Para el respaldo de la base de datos; se realiza una conexión al servidor de base de datos para descargar la información actualizada.	Semestralmente: un día.	Tener actualizada la experiencia, la formación, aptitudes, y los datos de contacto del académico.
Se lleva a cabo el respaldo del sistema Web.	Se realiza una conexión al servidor web y se realiza una copia de la última versión del sistema.	En la última semana del semestre	Tener actualizada la experiencia, la formación, aptitudes, y los datos de contacto del académico.

9.2. Actualización y mantenimiento de equipo de cómputo

División de Ingeniería Eléctrica			
Identificador único*	DIE-01-DC-01		
(Nombre del sistema)*	C.V.		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Se realiza el cambio cuando es necesario debido a que el hardware ya no cubre con los requerimientos para el correcto funcionamiento del sistema; como puede ser espacio en DD, memoria RAM, conexión de red, sistema operativo, etc.	Mejora la calidad en el servicio de captura de C.V. de académicos. El mantenimiento es menos demandante.	Tres semanas: En el intersemestre.	La funcionalidad como mayor velocidad en el acceso de los datos y carga de los mismos.

9.3. Procesos para la conservación, preservación y respaldos de información

División de Ingeniería Eléctrica		
Identificador único*	DIE-01-DC-01	
(Nombre del sistema)*	**C.V.**	
Proceso*	**Descripción***	**Responsable***
No contamos con documentación del proceso de respaldo.	No existe.	No existe.

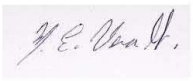
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Ingeniería Eléctrica		
Identificador único*	DIE-01-DC-01	
(Nombre del sistema)*	**C.V.**	
Proceso*	**Descripción***	**Responsable***
No contamos por escrito con el proceso para este punto.	No existe.	No existe.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No tenemos implementado este tratamiento de datos personales.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	María Elena Vera García, Ayudante de Prof. B, 56-22-30-53, vera@fi-b.unam.mx	
Revisó:	María Jaquelina López Barrientos, Prof. de Carrera Titular A, 56-22-30-66, jaqui.lopez963@gmail.com	
Autorizó:	Orlando Zaldívar Zamorategui, Jefe de la DIE, 56-22-31-16, 56-22-31-28, zazor1@fi-b.unam.mx	
Fecha de aprobación:	17 de agosto del 2022	
Fecha de actualización:	17 de agosto del 2022	

DIVISIÓN DE INGENIERÍA MECÁNICA E INDUSTRIAL

-

ÍNDICE

DIVISIÓN DE INGENIERÍA MECÁNICA E INDUSTRIAL

La División de Ingeniería Mecánica e Industrial tiene como funciones sustantivas la docencia, la generación del conocimiento y su difusión. Para cubrir la primera de ellas cuenta con cuatro carreas: Ingeniería Mecánica, Ingeniería Industrial, Ingeniería Mecatrónica e Ingeniería en Sistemas Biomédicos. Además, participa de manera directa en el Programa de Posgrado en Ingeniería de la UNAM, en los campos de conocimiento en Ingeniería Mecánica y en Ingeniería de Sistemas, y en menor medida en el Programa de Posgrado en Ciencia e Ingeniería de Materiales. En cuanto a la generación del conocimiento, en la División existe desde hace más de cuatro décadas la tradición por el desarrollo de proyectos de investigación básica y de desarrollo tecnológico, así como de la difusión de los resultados en congresos nacionales e internacionales y en revistas arbitradas.

Este documento tiene el objetivo de documentar las actividades realizadas para formar parte del Sistema de Gestión de Seguridad de Datos Personales de la DIMEI, y que a su vez es revisado y controlado por la UNAM. Se trata de una primera versión del documento, que se enriquecerá conforme se vayan cumpliendo las tareas necesarias y acordes con la reglamentación establecida, también se actualizará conforme se agreguen, editen o termine su tiempo de vida de los desarrollos o procesos mencionados en el presente documento y que se tengan claras las ediciones o modificaciones del tratamiento de datos personales.

El alcance de este sistema se centra en proteger “Todos los datos personales y datos personales sensibles que recabe y trate la DIMEI” de accesos no autorizados de tratamientos distintos a los fines para los que fueron recabados.

Sistemas de Tratamiento de Datos Personales

La División de Ingeniería Mecánica e Industrial cuenta con diferentes Sistemas y Aplicaciones que facilitan la ejecución de los procesos de las diferentes áreas académico-administrativas, algunos de los cuales hacen tratamiento de datos personales de alumnos, profesores y trabajadores.

A continuación se enlistan los sistemas que hacen tratamiento de datos personales en la DIMEI:

- Sistema de calificaciones de laboratorios

- Sistema de atención personalizada DIMEI

- Sistema de préstamo de herramientas

SISTEMA DE CALIFICACIONES DE LABORATORIOS

Sistema encargado de llevar el control de las reuniones de las distintas Academias de la Facultad de Ingeniería, permitiéndoles a los presidentes programar reuniones, permite dar de alta a sus miembros y administrar a los mismos (modificar y eliminar datos personales), realizar minutas, hacer seguimiento a los acuerdos producto de las reuniones, reprogramar reuniones, enviar por correo las minutas. Así mismo, los jefes de departamento pueden consultar todas las academias pertenecientes a dicho departamento, y a su vez, los jefes de división pueden consultar todos sus departamentos. Adicionalmente también los presidentes pueden editar minutas y bloquear la edición una vez que lo decidan. Por último, en el sistema se pueden consultar minutas, documentos y evidencias de reuniones anteriores.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingeniería Mecánica e Industrial – Secretaría Académica	
Identificador único*	DIMEI - 01 - SA - 01
Nombre del sistema *	**Sistema de calificaciones de laboratorios**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, apellido paterno, apellido materno, número de cuenta
Responsable*:	Secretaría Académica
Nombre*:	**Ing. Miriam Mendoza Cano**
Cargo*:	Secretaria Académica
Funciones*:	Decidir el funcionamiento del contenido, finalidad y uso del sistema.
Obligaciones*:	Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, académicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	**Ing. Cynthia Nelly Peña Belmont**
Cargo*:	**Técnico Académico**
Funciones*:	Dar soporte al desarrollo en cómputo necesaria en la División para atender las actividades académico-administrativas.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias.
(Nombre del Encargado 2*)	David Suárez Esteves
Cargo*:	Ayudante de Profesor
Funciones*:	Brindar apoyo al registro de los grupos y efectuar los mantenimientos adecuados y necesarios al sistema.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
	Usuarios:
(Nombre del Usuario 1*)	Académicos activos en la DIMEI
Cargo*:	Profesores de asignatura y tiempo completo
Funciones*:	Revisión y consultas en el sistema
Obligaciones*:	

	Cumplir con la obligación legal del manejo de los datos personales de alumnos inscritos en su curso.
(Nombre del Usuario 2*)	Funcionarios activos de la DIMEI
Cargo*:	Jefes de Departamento
Funciones*:	Revisión y consultas en el sistema.
Obligaciones*:	Cumplir con la obligación legal del manejo de los datos personales

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingeniería Mecánica e Industrial – Secretaría Académica	
Identificador único¨*	DIMEI - 01 - SA - 01
Nombre del sistema*	**Sistema de calificaciones de laboratorios**
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos.
Características del lugar donde se resguardan los soportes: *	Servidores de la División

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 595 a 597.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

División de Ingeniería Mecánica e Industrial – Secretaría Académica	
Identificador único*	DIMEI - 01 - SA - 01
Nombre del sistema*	**Sistema de calificaciones de laboratorios**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema de calificaciones de laboratorios no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Los datos que se registran en las bitácoras: La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema en el servidor.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

La división cuenta con un CCTV, 24 horas, ya que para acceder al edificio solo se cuenta con una puerta de cristal las cuales se encuentran abierta para el ingreso de personal académico, administrativo, y alumnos de 07:00 am a 21:00 pm

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para el acceso a la oficina se requiere identificarse en un biométrico y posteriormente presentarse en el cubículo mencionado, ya que el acceso además incluye llaves físicas.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se hace la actualización de los datos manualmente cotejando la información de que dispone la Secretaría Académica.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:
Basado en roles

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Si

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles? El sistema tiene la capacidad de que los nuevos usuarios creen su propio usuario, pero también el administrador puede dar de alta a uno o más usuarios.

b) ¿Quién autoriza la creación de nuevos perfiles? La secretaría Académica.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Se tiene un control de los creados masivamente o por petición de profesor. En el caso de un autorregistro el control lo tienen los logs del sistema.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si

c) ¿Cómo se evita el acceso remoto no autorizado?
Mediante la implementación de llaves en la conexión ssh.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
Se realizan respaldos completos de forma manual semestralmente.

2. El tipo de medios que utiliza para almacenar las copias de seguridad

El volcado de las copias de seguridad se realiza en los servidores de la División

3. Cómo y dónde archiva esos medios:
   Mediante las actividades de copia de respaldo del sistema en servidores de la División
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Personal de la Coordinación de Cómputo.

IX. PLAN DE CONTINGENCIA

Se cuenta con una réplica total de la plataforma en otro servidor y en otro cuarto de telecomunicaciones, pero dentro de la misma División. Esto con la finalidad de realizar un cambio, en caso de pérdida de conexión, daño físico o fallas en el sistema operativo del servidor principal. Esta réplica es un sitio alterno caliente y basta efectuar el redireccionamiento de la IP pública a la IP interna del sitio alterno. Este procedimiento lo realizará personal de la Coordinación de Cómputo en un lapso no mayor a 24 horas.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

División de Ingeniería Mecánica e Industrial – Secretaría Académica		
Identificador único*	DIMEI - 01 - SA - 01	
Nombre del sistema*	**Sistema de calificaciones de laboratorios**	
Recurso*	**Descripción***	**Control***
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Las herramientas utilizadas están bajo el control y operación de personal de UNAM CERT. Responsables: Personal de la Coordinación de Seguridad de la Información - UNAM CERT.
Bitácora del Sistema	Revisión Aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones. Responsable: Personal de la Coordinación de Cómputo

7.2. Procedimiento para la revisión de las medidas de seguridad

División de Ingeniería Mecánica e Industrial – Secretaría Académica		
Identificador único*	DIMEI - 01 - SA - 01	
Nombre del sistema*	**Sistema de calificaciones de laboratorios**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Plan de respaldos de la Información	Verificación y revisión de respaldos del Sistema	*a)* Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Actualización de Software	Revisión y actualización de Software	Responsable: Ing. Cynthia Nelly Peña Belmont
Instalación de Actualizaciones a Software antimalware	Revisión del software antimalware	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 dia hábil

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

División de Ingeniería Mecánica e Industrial – Secretaría Académica		
Identificador único*	DIMEI - 01 - SA - 01	
(Nombre del sistema)*	**Sistema de calificaciones de laboratorios**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Plan de respaldos de la Información	Verificación y revisión de respaldos del Sistema	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Instalación de Actualizaciones a código fuente	Revisión de versión del código fuente.	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Actualización de Plugins	Revisión y actualización de Plugins	Responsable: Ing. Cynthia Nelly Peña Belmont

		Tiempo de revisión: 1 día hábil

7.4. Acciones para la corrección y actualización de las medidas de seguridad

División de Ingeniería Mecánica e Industrial – Secretaría Académica		
Identificador único*	DIMEI - 01 - SA - 01	
Nombre del sistema*	**Sistema de calificaciones de laboratorios**	
Medida de seguridad*	**Acciones***	**Responsable***
Estatus de certificados SSL	Revisión de vigencia de certificados SSL	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

División de Ingeniería Mecánica e Industrial – Secretaría Académica			
Identificador único*	DIMEI - 01 - SA - 01		
(Nombre del sistema)*	**Sistema de calificaciones de laboratorios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se cuenta con un programa de capacitación de la protección de datos personales

8.2. Programa de difusión de la protección a los datos personales

No se cuenta con un programa de difusión de la protección de datos personales, para este sistema en particular. Se siguen las políticas de tratamiento de datos personales que marque la Facultad de Ingeniería.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

División de Ingeniería Mecánica e Industrial – Secretaría Académica			
Identificador único*	DIMEI - 01 - SA - 01		
Nombre del sistema*	**Sistema de calificaciones de laboratorios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Instalación de Actualizaciones a código fuente	Revisión de versión del código fuente.	1 Día hábil	BackEnd del código fuente de la plataforma.
Actualización de Plugins	Revisión y actualización de Plugins	1 Día hábil	BackEnd y FrontEnd de los complementos de la plataforma.

9.2. Actualización y mantenimiento de equipo de cómputo

División de Ingeniería Mecánica e Industrial – Secretaría Académica			
Identificador único*	DIMEI - 01 - SA - 01		
Nombre del sistema*	**Sistema de calificaciones de laboratorios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento	Revisión física periódica del equipo	12 hrs	Limpieza total del equipo

No se han asignado recursos para la actualización del equipo de cómputo

9.3. Procesos para la conservación, preservación y respaldos de información

División de Ingeniería Mecánica e Industrial – Secretaría Académica		
Identificador único*	DIMEI - 01 - SA - 01	
Nombre del sistema*	**Sistema de calificaciones de laboratorios**	
Proceso*	**Descripción***	**Responsable***
Plan de respaldos de la Información	Se realiza una verificación regular de que el contenido de los respaldos de información es accesible.	Responsable: David Suárez Esteves Tiempo de revisión: 1 día hábil

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Ingeniería Mecánica e Industrial – Secretaría Académica		
Identificador único*	DIMEI - 01 - SA - 01	
Nombre del sistema*	**Sistema de calificaciones de laboratorios**	
Proceso*	**Descripción***	**Responsable***
Validación de usuarios	Se verifica con Secretaría Académica si algún usuario ya no está activo	Responsable: David Suárez Esteves Tiempo de revisión: 1 día hábil
Borrado de final	Se formatea el servidor para borrar todo rastro de información del sistema	Responsable: Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Baja del equipo	Se solicita la baja del equipo por obsolescencia	Responsable: Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

1. El jefe de la División deberá solicitar la cancelación por escrito al responsable del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.
2. El responsable del sistema deberá realizar la suspensión de las credenciales de acceso al sistema o en su caso, bloquear el apartado de inicio de sesión del mismo.
3. El responsable del sistema deberá notificar al Jefe de la División de la acciones realizadas para lograr la cancelación temporal del sistema.
4. Una vez transcurrida la temporalidad en que el sistema quedó bloqueado, el encargado del sistema iniciará la eliminación segura del mismo.

SISTEMA DE ATENCIÓN PERSONALIZADA

Los alumnos que no alcanzan grupo en las asignaturas que solicitan mediante el proceso de inscripciones que lleva a cabo la Facultad, realizan la petición de sus opciones de grupos en este sistema, el cual requiere a los alumnos indiquen los motivos por los cuales están llevando a cabo la petición. En el caso de que los alumnos trabajen o estén en último semestre, deben proporcionar vía el sistema, la carta laboral y/o su historial académico. Los jefes de Departamento analizan las solicitudes y en base al número de vacantes de los grupos realizan o no la inscripción del alumno en alguna de las opciones solicitadas.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingeniería Mecánica e Industrial – Secretaría Académica	
Identificador único*	DIMEI - 02 - SA - 02
(Nombre del sistema)*	**Sistema de atención personalizada**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, Apellido Paterno, Apellido Materno, Número de cuenta, correo electrónico..
Responsable*:	Secretaría Académica
Nombre*:	**Ing. Miriam Mendoza Cano**
Cargo*:	Secretaria académica
Funciones*:	Tomar las decisiones adecuadas sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, académicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	**Ing. Cynthia Nelly Peña Belmont**
Cargo*:	**Coordinación de Cómputo**
Funciones*:	Dar soporte al desarrollo en cómputo necesaria en la DIMEI para atender las actividades académico-administrativas.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias
(Nombre del Encargado 2*)	David Suárez Esteves
Cargo*:	Ayudante de Profesor
Funciones*:	Brindar apoyo al registro de los grupos y efectuar los mantenimientos adecuados y necesarios al sistema.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
	Usuarios:
(Nombre del Usuario 1*)	Secretaría Académica
Cargo*:	Secretaría Académica
Funciones*:	Tomar las decisiones adecuadas sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	Decidir a qué usuarios se les da acceso al sistema con privilegios administrativos. Vigilar que el sistema cumpla con todas las medidas de

	seguridad técnicas, académicas, físicas y administrativas.
(Nombre del Usuario 2*)	Funcionarios activos de la DIMEI
Cargo*:	Jefes de Departamento
Funciones*:	Establecer las condiciones óptimas de operación para que las actividades académico–administrativas de la División se desarrollen conforme a lo establecido en el proyecto académico-administrativo de la Facultad.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingeniería Mecánica e Industrial – Secretaría Académica	
Identificador único¨*	DIMEI - 02 - SA - 02
(Nombre del sistema)*	**Sistema de atención personalizada**
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos relacional
Características del lugar donde se resguardan los soportes: *	Servidores de la División

3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 605 a 606.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

[redacted]

5. PLAN DE TRABAJO

[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

División de Ingeniería Mecánica e Industrial – Secretaría Académica	
Identificador único*	DIMEI - 02 - SA - 02
(Nombre del sistema)*	**Sistema de atención personalizada**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado de sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema de atención personalizada no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos..

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Los datos que se registran en las bitácoras:

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema en el servidor.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

La división cuenta con un CCTV, 24 horas, ya que para acceder al edificio solo se cuenta con una puerta de cristal las cuales se encuentran abierta para el ingreso de personal académico, administrativo, y alumnos de 06:30 am a 21:00 pm.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para el acceso a la oficina se requiere identificarse en un biométrico y posteriormente presentarse en el cubículo mencionado, ya que el acceso además incluye llaves físicas.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se hace la actualización de los datos manualmente cotejando la información de que dispone la Secretaría Académica.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso: Está basado en roles

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos? Sí
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Sí
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Sí

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Sí
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Sí

4. Administración de perfiles de usuario y contraseñas:

- **a)** ¿Quién da de alta nuevos perfiles?
  El encargado del sistema
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
  El jefe de la División
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?
  No, ya que sólo los autoriza el jefe de la División

5. Acceso remoto al sistema de tratamiento de datos personales:

- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
  No, cada usuario puede acceder al sistema desde cualquier dispositivo con conexión a internet.
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Sí
- **c)** ¿Cómo se evita el acceso remoto no autorizado?
  Mediante la implementación de llaves en la conexión ssh.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   Se realizan respaldos completos de forma manual semestralmente.
2. El tipo de medios que utiliza para almacenar las copias de seguridad.
   El volcado de las copias de seguridad se realiza en los servidores de la División.
3. Cómo y dónde archiva esos medios

Mediante las actividades de copia de respaldo del sistema en servidores de la División.

4. Quién es el responsable de realizar estas operaciones.
   Personal de la Coordinación de Cómputo

IX. PLAN DE CONTINGENCIA

Se cuenta con una réplica total de la plataforma en otro servidor y en otro cuarto de telecomunicaciones, pero dentro de la misma División. Esto con la finalidad de realizar un cambio, en caso de pérdida de conexión, daño físico o fallas en el sistema operativo del servidor principal. Esta réplica es un sitio alterno caliente y basta efectuar el redireccionamiento de la IP pública a la IP interna del sitio alterno. Este procedimiento lo realizará personal de la Coordinación de Cómputo en un lapso no mayor a 24 horas.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

División de Ingeniería Mecánica e Industrial – Secretaría Académica		
Identificador único*	DIMEI - 02 - SA - 02	
(Nombre del sistema)*	**Sistema de atención personalizada**	
Recurso*	**Descripción***	**Control***
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Las herramientas utilizadas están bajo el control y operación de personal de UNAM CERT. Responsables: Personal de la Coordinación de Seguridad de la Información - UNAM CERT.
Bitácora del Sistema	Revisión Aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones. Responsable: Personal de la Coordinación de Cómputo

7.2. Procedimiento para la revisión de las medidas de seguridad

División de Ingeniería Mecánica e Industrial – Secretaría Académica		
Identificador único*	DIMEI - 02 - SA - 02	
(Nombre del sistema)*	**Sistema de atención personalizada**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Plan de respaldos de la Información	Verificación y revisión de respaldos del Sistema	Responsable: Ing. Cynthia Nelly Peña Belmont

		Tiempo de revisión: 1 día hábil
Actualización de Software	Revisión y actualización de Software	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Instalación de Actualizaciones a Software antimalware	Revisión del software antimalware	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

División de Ingeniería Mecánica e Industrial – Secretaría Académica		
Identificador único*	DIMEI - 02 - SA - 02	
(Nombre del sistema)*	**Sistema de atención personalizada**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Plan de respaldos de la Información	Verificación y revisión de respaldos del Sistema	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Instalación de Actualizaciones a código fuente	Revisión de versión del código fuente.	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Actualización de Plugins	Revisión y actualización de Plugins	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil

7.4. Acciones para la corrección y actualización de las medidas de seguridad

División de Ingeniería Mecánica e Industrial – Secretaría Académica		
Identificador único*	DIMEI - 02 - SA - 02	
(Nombre del sistema)*	**Sistema de atención personalizada**	
Medida de seguridad*	**Acciones***	**Responsable***
Estatus de certificados SSL	Revisión de vigencia de certificados SSL	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

División de Ingeniería Mecánica e Industrial – Secretaría Académica			
Identificador único*	DIMEI - 02 - SA - 02		
(Nombre del sistema)*	**Sistema de atención personalizada**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se cuenta con un programa de capacitación de la protección de datos personales.

8.2. Programa de difusión de la protección a los datos personales

No se cuenta con un programa de difusión de la protección de datos personales, para este sistema en particular. Se siguen las políticas de tratamiento de datos personales que marque la Facultad de Ingeniería.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

División de Ingeniería Mecánica e Industrial – Secretaría Académica			
Identificador único*	DIMEI - 02 - SA - 02		
(Nombre del sistema)*	**Sistema de atención personalizada**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Instalación de Actualizaciones a código fuente	Revisión de versión del código fuente.	1 Día hábil	BackEnd del código fuente de la plataforma.
Actualización de Plugins	Revisión y actualización de Plugins	1 Día hábil	BackEnd y FrontEnd de los complementos de la plataforma.

9.2. Actualización y mantenimiento de equipo de cómputo

División de Ingeniería Mecánica e Industrial – Secretaría Académica	
Identificador único*	DIMEI - 02 - SA - 02

(Nombre del sistema)*	Sistema de atención personalizada		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento	Revisión física periódica del equipo	12 hrs	Limpieza total del equipo

No se han asignado recursos para la actualización del equipo de cómputo.

9.3. Procesos para la conservación, preservación y respaldos de información

División de Ingeniería Mecánica e Industrial – Secretaría Académica		
Identificador único*	DIMEI - 02 - SA - 02	
(Nombre del sistema)*	Sistema de atención personalizada	
Proceso*	**Descripción***	**Responsable***
El formato de los archivos de respaldo de información corresponde a información en texto plano.	Se realiza una verificación regular de que el contenido de los respaldos de información es accesible.	Responsable: M.I. Tanya Itzel Arteaga Ricci Tiempo de revisión: 1 día hábil

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Ingeniería Mecánica e Industrial – Secretaría Académica		
Identificador único*	DIMEI - 02 - SA - 02	
(Nombre del sistema)*	Sistema de atención personalizada	
Proceso*	**Descripción***	**Responsable***
Validación de usuarios	Se verifica con Secretaría Académica si algún usuario ya no está activo	Responsable: David Suárez Esteves Tiempo de revisión: 1 día hábil
Borrado de final	Se formatea el servidor para borrar todo rastro de información del sistema	Responsable: Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Baja del equipo	Se solicita la baja del equipo por obsolescencia	Responsable: Cynthia Nelly Peña Belmont

		Tiempo de revisión: 1 día hábil

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

1. El jefe de la División deberá solicitar la cancelación por escrito al responsable del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.
2. El responsable del sistema deberá realizar la suspensión de las credenciales de acceso al sistema o en su caso, bloquear el apartado de inicio de sesión del mismo.
3. El responsable del sistema deberá notificar al Jefe de la División de la acciones realizadas para lograr la cancelación temporal del sistema.
4. Una vez transcurrida la temporalidad en que el sistema quedó bloqueado, el encargado del sistema iniciará la eliminación segura del mismo.

SISTEMA DE PRÉSTAMO DE HERRAMIENTAS

Sistema desarrollado para el almacén, actualizando un sistema que se manejaba en ACCESS para el llenado de vales de préstamo de herramientas para alumnos, pero debido a las limitantes del software se decidió pasarlo a aplicación web, dando como resultado un sistema más eficiente en el registro de los préstamos como en la generación de reportes.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**	
Identificador único*	DIMEI - 03 - DIDM - 01
(Nombre del sistema)*	**Sistema de préstamo de herramientas**
Datos personales (sensibles o no) contenidos en el sistema*:	Número de cuenta, nombre, apellido paterno y apellido materno.
Responsable*:	Jefe del Departamento
Nombre*:	**Dr. Adrián Espinosa Bautista**
Cargo*:	**Jefe del Departamento de Ingeniería de Diseño y Manufactura**
Funciones*:	Tomar las decisiones adecuadas sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, académicas, físicas y administrativas.
	Encargados:
(Nombre del Encargado 1*)	**Ing. Cynthia Nelly Peña Belmont**
Cargo*:	**Técnico Académico**
Funciones*:	Dar soporte al desarrollo en cómputo necesaria en la División para atender las actividades académico-administrativas.
Obligaciones*:	Procurar la protección de datos personales contenidos en el sistema mediante la implementación de estrategias
(Nombre del Encargado 2*)	Erika López López
Cargo*:	Ayudante de profesor
Funciones*:	Brindar apoyo al registro de los grupos y efectuar los mantenimientos adecuados y necesarios al sistema.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales.
	Usuarios:
(Nombre del Usuario 1*)	Fabricio Quiñones Palacios
Cargo*:	Laboratorista
Funciones*:	Registrar cada préstamo de herramientas
Obligaciones*:	Decidir sobre la incorporación de nuevas funcionalidades en el sistema. Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, académicas, físicas y administrativas.

(Nombre del Usuario 2*)	Alberto González Morales
Cargo*:	Laboratorista
Funciones*:	Registrar cada préstamo de herramientas.
Obligaciones*:	Decidir sobre la incorporación de nuevas funcionalidades en el sistema. Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, académicas, físicas y administrativas.
(Nombre del Usuario 3*)	Dr. Adrián Espinosa Bautista
Cargo*:	Jefe de Departamento
Funciones*:	Decidir a quién se le da acceso al sistema y como se manejará la información.
Obligaciones*:	Decidir sobre la incorporación de nuevas funcionalidades en el sistema. Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, académicas, físicas y administrativas.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**	
Identificador único¨*	DIMEI - 03 - DIDM - 01
(Nombre del sistema)*	**Sistema de préstamo de herramientas**
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos
Características del lugar donde se resguardan los soportes: *	Servidores de la División

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 615 a 616.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**	
Identificador único*	DIMEI - 03 - DIDM - 01

Registro de Equipos de Cómputo de la Facultad de Ingeniería (RECFI)	**Sistema de préstamo de herramientas**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema de préstamo de herramientas no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El sistema cuenta con una bitácora interna que registra los ingresos y las actividades en general que realiza el usuario, incluyendo fecha y hora.

IV. REGISTRO DE INCIDENTES:

Los datos que se registran en las bitácoras:
La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema en el servidor.
.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

   La división cuenta con un CCTV, 24 horas, ya que para acceder al edificio solo se cuenta con una puerta de cristal las cuales se encuentran abierta para el ingreso de personal académico, administrativo, y alumnos de 06:30 am a 21:00 pm

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

   Para el acceso al almacén solo se accede con llave física.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se hace la actualización de los datos manualmente cotejando la información de que dispone la Secretaría Académica.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes): Basado en roles

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Sólo los encargados pueden dar de alta nuevos perfiles.
b) ¿Quién autoriza la creación de nuevos perfiles? El jefe del departamento
c) ¿Se lleva registro de la creación de nuevos perfiles?
No, por que solo el jefe del departamento autoriza los nuevos perfiles

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si
c) ¿Cómo se evita el acceso remoto no autorizado?
Mediante la implementación de llaves en la conexión ssh.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

Se realizan respaldos completos de forma manual semestralmente.

2. El tipo de medios que utiliza para almacenar las copias de seguridad

El volcado de las copias de seguridad se realiza en los servidores de la División.

3. Cómo y dónde archiva esos medios.

Mediante las actividades de copia de respaldo del sistema en servidores de la División.

4. Quién es el responsable de realizar estas operaciones.

Personal de la Coordinación de Cómputo

IX. PLAN DE CONTINGENCIA

Se cuenta con una réplica total de la plataforma en otro servidor y en otro cuarto de telecomunicaciones, pero dentro de la misma División. Esto con la finalidad de realizar un cambio, en caso de pérdida de conexión, daño físico o fallas en el sistema operativo del servidor principal. Esta réplica es un sitio alterno caliente y basta efectuar el redireccionamiento de la IP pública a la IP interna del sitio alterno. Este procedimiento lo realizará personal de la Coordinación de Cómputo en un lapso no mayor a 24 horas.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**		
Identificador único*	DIMEI - 03 - DIDM - 01	
(Nombre del sistema)*	*Sistema de préstamo de herramientas*	
Recurso*	**Descripción***	**Control***
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Las herramientas utilizadas están bajo el control y operación de personal de UNAM CERT. Responsables: Personal de la Coordinación de Seguridad de la Información - UNAM CERT.
Bitácora del Sistema	Revisión Aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones. Responsable: Personal de la Coordinación de Cómputo

7.2. Procedimiento para la revisión de las medidas de seguridad

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**	
Identificador único*	DIMEI - 03 - DIDM - 01

(Nombre del sistema)*	*Sistema de préstamo de herramientas*	
Medida de seguridad*	**Procedimiento***	**Responsable***
Plan de respaldos de la Información	Verificación y revisión de respaldos del Sistema	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Actualización de Software	Revisión y actualización de Software	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Instalación de Actualizaciones a Software antimalware	Revisión del software antimalware	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**		
Identificador único*	DIMEI - 03 - DIDM - 01	
(Nombre del sistema)*	*Sistema de préstamo de herramientas*	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Plan de respaldos de la Información	Verificación y revisión de respaldos del Sistema	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Instalación de Actualizaciones a código fuente	Revisión de versión del código fuente.	Responsable: Ing. Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Actualización de Plugins	Revisión y actualización de Plugins	Responsable: Ing. Cynthia Nelly Peña Belmont

		Tiempo de revisión: 1 día hábil

7.4. Acciones para la corrección y actualización de las medidas de seguridad

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**		
Identificador único*	DIMEI - 03 - DIDM - 01	
(Nombre del sistema)*	*Sistema de préstamo de herramientas*	
Medida de seguridad*	**Acciones***	**Responsable***
Estatus de certificados SSL	Revisión de vigencia de certificados SSL	Responsable: Ing. Cynthia Nelly Peña Belmont a) Tiempo de revisión: 1 día hábil

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**			
Identificador único*	DIMEI - 03 - DIDM - 01		
(Nombre del sistema)*	*Sistema de préstamo de herramientas*		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se cuenta con un programa de capacitación de la protección de datos personales.

8.2. Programa de difusión de la protección a los datos personales

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**	
Identificador único*	DIMEI - 03 - DIDM - 01
(Nombre del sistema)*	*Sistema de préstamo de herramientas*

Actividad*	Descripción*	Duración*	Cobertura*

No se cuenta con un programa de difusión de la protección de datos personales, para este sistema en particular. Se siguen las políticas de tratamiento de datos personales que marque la Facultad de Ingeniería.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**			
Identificador único*	DIMEI - 03 - DIDM - 01		
(Nombre del sistema)*	*Sistema de préstamo de herramientas*		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Instalación de Actualizaciones a código fuente	Revisión de versión del código fuente.	1 Día hábil	BackEnd del código fuente de la plataforma.
Actualización de Plugins	Revisión y actualización de Plugins	1 Día hábil	BackEnd y FrontEnd de los complementos de la plataforma.

9.2. Actualización y mantenimiento de equipo de cómputo

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**			
Identificador único*	DIMEI - 03 - DIDM - 01		
(Nombre del sistema)*	*Sistema de préstamo de herramientas*		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento	Revisión física periódica del equipo	12 hrs	Limpieza total del equipo

No se han asignado recursos para la actualización del equipo de cómputo.

9.3. Procesos para la conservación, preservación y respaldos de información

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**		
Identificador único*	DIMEI - 03 - DIDM - 01	
(Nombre del sistema)*	*Sistema de préstamo de herramientas*	
Proceso*	**Descripción***	**Responsable***
Respaldo de la Información	Se realiza una verificación regular de que el contenido de los respaldos de información es accesible.	Responsable: Erika López López Tiempo de revisión: 1 día hábil

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Ingeniería Mecánica e Industrial **Departamento de Ingeniería de Diseño y Manufactura**		
Identificador único*	DIMEI - 03 - DIDM - 01	
(Nombre del sistema)*	*Sistema de préstamo de herramientas*	
Proceso*	**Descripción***	**Responsable***
Validación de usuarios	Se verifica con Secretaría Académica si algún usuario ya no está activo	Responsable: Erika López López Tiempo de revisión: 1 día hábil
Borrado de final	Se formatea el servidor para borrar todo rastro de información del sistema	Responsable: Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Baja del equipo	Se solicita la baja del equipo por obsolescencia	Responsable: Cynthia Nelly Peña Belmont Tiempo de revisión: 1 día hábil
Validación de usuarios	Se verifica con Secretaría Académica si algún usuario ya no está activo	Responsable: Erika López López Tiempo de revisión: 1 día hábil

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

1. El jefe de la División deberá solicitar la cancelación por escrito al responsable del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.
2. El responsable del sistema deberá realizar la suspensión de las credenciales de acceso al sistema o en su caso, bloquear el apartado de inicio de sesión del mismo.
3. El responsable del sistema deberá notificar al Jefe de la División de la acciones realizadas para lograr la cancelación temporal del sistema.
4. Una vez transcurrida la temporalidad en que el sistema quedó bloqueado, el encargado del sistema iniciará la eliminación segura del mismo.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo	Cynthia Nelly Peña Belmont Coordinación de Cómputo Tel. 5556229981 ext. 509 cynelly@comunidad.unam.mx	 Cynthia Nelly Peña Belmont
Revisó:	Miriam Mendoza Cano Secretaria Académica Tel. 5556229981 ext. 517 mir_g_menca@unam.mx	 Miriam Graciela Mendoza Cano
Autorizó:	Francisco Javier Solorio Ordaz Jefe de la División de Ingeniería Mecánica e Industrial Tel. 5556229981 ext. 518 fjso@unam.mx	 Francisco Javier Solorio Ordaz
Fecha de aprobación:		17 – agosto - 2022
Fecha de actualización:		17 – agosto - 2022

DIVISIÓN DE EDUCACIÓN CONTINUA Y A DISTANCIA

ÍNDICE

DIVISIÓN DE EDUCACIÓN CONTINUA Y A DISTANCIA (DECD)

La División de Educación Continua y a Distancia (DECD) de la Facultad de Ingeniería, es la encargada de proporcionar educación a los ingenieros egresados de la facultad, de otras instituciones, y al público en general, conocimientos actualizados en las diferentes áreas. Esto lo realizamos ofreciéndoles a los participantes una variedad de cursos, diplomados y talleres, tanto presenciales como en línea y ahora también híbridos.

En concordancia con una de las actividades sustantivas de la Universidad, el aspecto cultural también es parte importante del quehacer de la División, al tener la sede en uno de los edificios más representativos de la época colonial el “Palacio de Minería”, este se presta para llevar a cabo diferentes actividades, exposiciones, conciertos, visitas guiadas y una amplia gama de actividades culturales.

La división también tiene a su cargo la oficina de egresados de la facultad, con ella, se pretende estar en contacto con los exalumnos para poder ofrecerles la oferta académica de la División y mantener un enlace entre ambas partes.

INTRANET

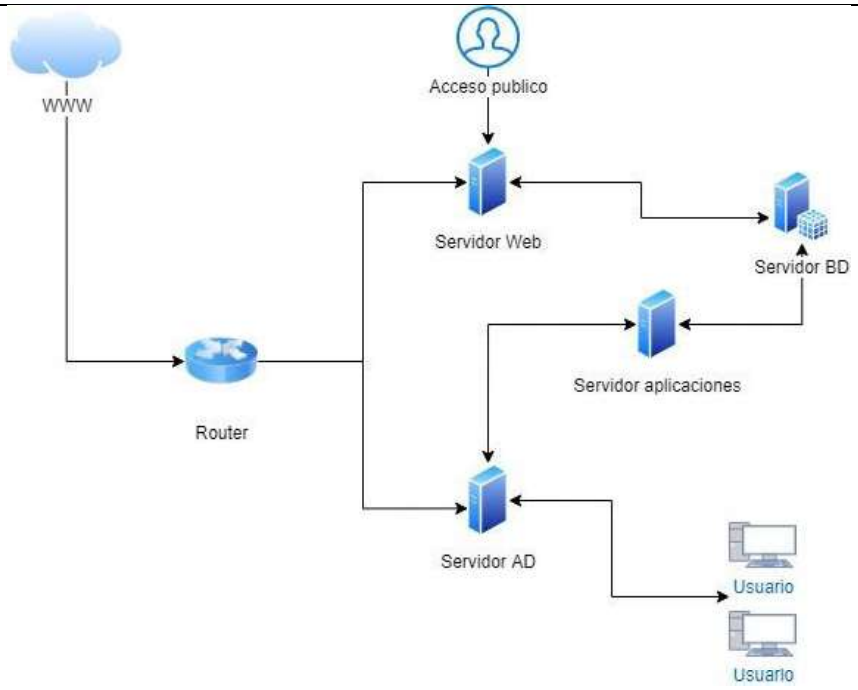
La División cuenta con un sistema interno, mediante el cual se administran los datos de los participantes a los diferentes cursos, los egresados y el personal por honorarios. A este sistema se le llama **"INTRANET"**.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Educación Continua y a Distancia	
Identificador único*	DECD-01-TIC-01
Nombre del sistema *	INTRANET
Datos personales (sensibles o no) contenidos en el sistema*:	PARTICIPANTES Nombre, Sexo, Teléfonos, RFC, correo electrónico, país, código postal, estado, municipio, colonia, calle, numero exterior, número interior, nivel de estudios, Titulado, institución de procedencia, carrera, nombre de la empresa donde labora, teléfono de empresa, razón social de la empresa, dirección de la empresa, RFC de la empresa EGRESADOS Número de cuenta UNAM, nombre, RFC, CURP, genero, nacionalidad, calle, colonia código postal, delegación, ciudad, estado, teléfono de casa, estado, teléfono del trabajo, extensión, fecha de nacimiento, correo electrónico, clave de carrera UNAM, nombre de la carrera, clave del módulo, nombre del módulo, año de ingreso, semestre de ingreso, año de egreso, semestre de egreso, promedio, clave de modalidad, nombre de la modalidad, presentación, título de trabajo escrito, tipo, fecha de registro, fecha de titulación, hora de titulación, recinto, RFC presidente, Nombre presidente, presidente asistencia, RFC vocal, nombre vocal, vocal asistencia, RFC secretario, nombre secretario, secretario asistencia, RFC primer suplente, nombre primer suplente, primer suplente asistencia, RFC segundo suplente, nombre segundo suplente, segundo suplente asistencia, Director, resultado. PROFESORES Nombre, teléfono particular, teléfono de oficina, teléfono celular, correo electrónico personal, correo electrónico de oficina, país, código postal, calle, numero interior, número exterior, colonia, delegación o municipio, estado, número de cedula profesional, RFC, Empresa donde labora, extracto de curriculum, archivo del curriculum. PERSONAL DE HONORARIOS Nombre, Monto del contrato, Actividades a desarrollar, tipo de honorario.
Responsable*:	División de Educación Continua y a Distancia de la Facultad de Ingeniería

Nombre*:	**Mtro. Arturo López Cardiel**
Cargo*:	**Coordinador de Tecnologías de la Información y Telecomunicaciones**
Funciones*:	Mantener los datos personales a disposición de los usuarios, y que se les dé el uso para el cual han sido solicitados.
Obligaciones*:	Mantener la funcionalidad requerida del sistema e incorporar las nuevas funcionalidades solicitadas por los usuarios. Aplicar políticas de seguridad para los usuarios. Implementar medidas para resguardar la seguridad de los datos, tanto física como técnica.
	Encargados:
(Nombre del Encargado 1*)	**Kevin David Espinoza Flores**
Cargo*:	**Administrador de Bases de datos y servidores**
Funciones*:	Aplicar las políticas de seguridad para los datos personales. Actualización de los servidores. Dar de alta, baja y actualización de usuarios del sistema.
Obligaciones*:	Mantener los servidores actualizados, verificar la integridad de las bases de datos, mantener los permisos de los usuarios de acuerdo a su rol, verificar que el funcionamiento de los programas de seguridad se encuentren actualizados, mantener los certificados de seguridad vigentes.
(Nombre del Encargado 2*)	Miguel Angel Leyva Bejarano
Cargo*:	Programador
Funciones*:	Desarrollar el software solicitado por las diferentes áreas de la División, y actualizarlas derivado de las nuevas solicitudes.
Obligaciones*:	Verificar el buen funcionamiento del sistema. Asegurarse de la integridad de los datos al realizar las transacciones. Desarrollar los sistemas en base a políticas y estándares de la División. Brindar apoyo a los usuarios en la utilización del sistema.
	Usuarios:
(Nombre del Usuario 1*)	Lic. Anabell Branch Ramos
Cargo*:	Secretaria Académica de la División
Funciones*:	Dar seguimiento al registro de los participantes y los profesores
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales
(Nombre del Usuario 2*)	Nora Jimena Jarillo Aguilar
Cargo*:	Jefa de la Oficina de egresados de la Facultad de Ingeniería
Funciones*:	Dar seguimiento al registro de los egresados
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales
(Nombre del Usuario 3*)	Eric Antonio Aguilar Olivares
Cargo*:	Jefe de la Unidad Administrativa de la División
Funciones*:	Dar seguimiento al registro de los participantes, profesores y personal de honorarios
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

División de Educación Continua y a Distancia	
Identificador único¨*	DECD-01-TIC-01
Nombre del sistema*	INTRANET
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos
Características del lugar donde se resguardan los soportes: *	 Alojado en los servidores de la DECD.

3. ANÁLISIS DE RIESGOS

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las paginas 629 a 631.
Periodo de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

División de Educación Continua y a Distancia de la Facultad de Ingeniería	
Identificador único*	DECD-01-TIC-01
Nombre del sistema*	INTRANET
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan trasferencias de datos mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan trasferencias de datos mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan trasferencias de datos mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

INTRANET no realiza tratamiento de datos personales con soportes físicos, ya que se encuentran en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado se encuentra en un archivo *.log almacenado en ubicación del sistema en el servidor.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
Se les pide su identificación oficial: credencial del INE O Pasaporte.

b) ¿Cómo las autentifica?
Mediante su fotografía en su identificación

c) ¿Cómo les autoriza el acceso?
Avisando a la persona que van a visitar.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   La persona a la que van a visitar tiene que corroborar que son las personas que espera.

2. ¿Cómo las autentifica?
   Mediante su fotografía en la identificación.

3. ¿Cómo les autoriza el acceso?
   Permitiendo su acceso a las zonas controladas.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

PARTICIPANTES
El participante solicita la actualización de datos a través de la página web, se le envía a su correo registrado una clave para validar que se trata de dicho participante con la cual se le permitirá actualizar sus datos personales. La frecuencia con la que se realiza este proceso depende de cada participante.

EGRESADOS
El egresado solo podrá actualizar su información laboral y de contacto ya que toda la

información relevante a su persona no se podrá modificar. La frecuencia con la que se realiza este proceso depende de cada egresado.

PROFESORES
El área encargada de la coordinación de la oferta académica será la responsable de actualizar sus datos personales. La frecuencia con la que se realiza este proceso depende de la coordinación de la oferta académica.

PERSONAL DE HONORARIOS
El área encargada de la tramitación de los honorarios será la responsable de actualizar sus datos personales. La frecuencia con la que se realiza este proceso depende de la tramitación de los honorarios.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):
Está basado en roles (perfiles) o grupos

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  Si.
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  Si.
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Si.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
  Si
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  Si

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles?
  El Administrador de Bases de datos y servidores.
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
  El Coordinador de Tecnologías de la Información y Telecomunicaciones.
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?
  Si.

5. Acceso remoto al sistema de tratamiento de datos personales:
- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
  Si.
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
  Si
- **c)** ¿Cómo se evita el acceso remoto no autorizado?
  Mediante usuario y contraseña.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos **X**, diferenciales **X** o incrementales **X**;
   b) De forma automática **X** o Manual __,
   c) Periodicidad con que los realiza: Diario
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;[11]

Disco Duro.

3. Cómo y dónde archiva esos medios, y

En un disco duro externo localizado en el mismo cuarto de servidores.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

El Administrador de Bases de datos y servidores.

IX. PLAN DE CONTINGENCIA

No se cuenta con el plan de contingencia, pero se encuentra en desarrollo.
No se cuenta con sitio redundante.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

División de Educación Continua y a Distancia		
Identificador único*	DECD-01-TIC-01	
Nombre del sistema*	INTRANET	
Recurso*	**Descripción***	**Control***
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones. Responsable: El Administrador de Bases de datos y servidores.

Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Las herramientas utilizadas están bajo el control y operación de personal de UNAM CERT. Responsables: Personal de la Coordinación de Seguridad de la Información - UNAM CERT.

7.2. Procedimiento para la revisión de las medidas de seguridad

División de Educación Continua y a Distancia		
Identificador único*	DECD-01-TIC-01	
Nombre del sistema*	INTRANET	
Medida de seguridad*	**Procedimiento***	**Responsable***
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	El responsable de realizar la revisión es el Administrador de Bases de datos y servidores. La duración de la revisión es de 30 minutos.
Plan de respaldos de información	Revisión y validación del historial de respaldos del sistema.	El responsable de realizar la revisión es el Administrador de Bases de datos y servidores. La duración de la revisión es de 30 minutos.
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	El responsable de realizar la revisión es el Administrador de Bases de datos y servidores. La duración de la revisión es de 2 horas.
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	El responsable de realizar la revisión es el Administrador de Bases de datos y servidores. La duración de la revisión es un día hábil.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

División de Educación Continua y a Distancia		
Identificador único*	DECD-01-TIC-01	
(Nombre del sistema)*	INTRANET	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	El responsable de realizar la revisión es el Administrador de Bases de datos y servidores.
Plan de respaldos de información	Se cuenta con respaldos actualizados de la información del sistema.	El responsable de realizar la revisión es el Administrador de Bases de datos y servidores.
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	El responsable de realizar la revisión es el Administrador de Bases de datos y servidores.
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	El responsable de realizar la revisión es el Administrador de Bases de datos y servidores.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

División de Educación Continua y a Distancia		
Identificador único*	DECD-01-TIC-01	
Nombre del sistema*	INTRANET	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Realizar la renovación anual del certificado SSL para el subdominio donde se encuentra el sistema.	El responsable de realizar la revisión es el Administrador de Bases de datos y servidores.
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la última versión estable disponible a petición del responsable del sistema.	El responsable de realizar la revisión es el Programador.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

División de Educación Continua y a Distancia			
Identificador único*	DECD-01-TIC-01		
(Nombre del sistema)*	INTRANET		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Curso en línea	25 horas. Del 9 de agosto al 12 de septiembre.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.

8.2. Programa de difusión de la protección a los datos personales

División de Educación Continua y a Distancia			
Identificador único*	DECD-01-TIC-01		
(Nombre del sistema)*	INTRANET		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se cuenta con un programa de difusión de la protección de datos personales.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

División de Educación Continua y a Distancia	
Identificador único*	DECD-01-TIC-01

Nombre del sistema*	INTRANET		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de tecnologías de desarrollo	1. Solicitar la Actualización del Lenguaje de programación en el servidor de pruebas. 2 Actualizar el framework de desarrollo de la aplicación y sus dependencias. 3. Realizar exhaustivas pruebas de funcionalidad en busca de errores, bugs o problemas de compatibilidad como consecuencia de las actualizaciones anteriores. 4. Corregir y/o refactorizar características del sistema. 5. Aplicar modificaciones realizadas en el servidor de pruebas y verificar el correcto funcionamiento. 6. Llevar a cabo todas las actualizaciones anteriores en el servidor de producción.	12 meses	BackEnd de la aplicación: tecnologías de desarrollo.

9.2. Actualización y mantenimiento de equipo de cómputo

División de Educación Continua y a Distancia	
Identificador único*	DECD-01-TIC-01

Nombre del sistema*	INTRANET		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento de servidores	Limpieza preventiva. Revisión de condiciones de desempeño.	Un día hábil, cada 6 meses.	Evita sobrecalentamientos y desgaste de componentes internos de los servidores.

9.3. Procesos para la conservación, preservación y respaldos de información

División de Educación Continua y a Distancia		
Identificador único*	DECD-01-TIC-01	
Nombre del sistema*	INTRANET	
Proceso*	**Descripción***	**Responsable***
El responsable de realizar la revisión es el Administrador de Bases de datos y servidores.	El responsable de realizar la revisión es el Administrador de Bases de datos y servidores.	El responsable de realizar la revisión es el Administrador de Bases de datos y servidores.

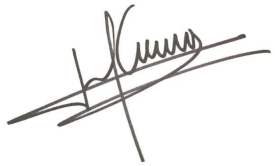
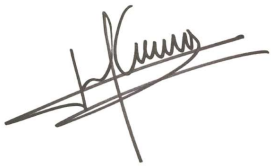
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

División de Educación Continua y a Distancia		
Identificador único*	DECD-01-TIC-01	
Nombre del sistema*	INTRANET	
Proceso*	**Descripción***	**Responsable***
Borrado seguro y disposición de componentes informáticos	El borrado seguro de la Información se realiza con herramientas que permiten el formateo a bajo nivel de los medios magnéticos que lo contienen. Una vez realizado el proceso los componentes informáticos son enviados para su disposición final a la dirección general de obras y servicios mediante los programas de recolección de desechos electrónicos.	El responsable de realizar la revisión es el Administrador de Bases de datos y servidores.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Por el momento no se tiene contemplada la cancelación de este sistema ya que es la columna vertebral de las operaciones diarias de la División **.**

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Mtro. Arturo López Cardiel Coordinador de Tecnologías de la Información y Telecomunicaciones. Tel. 5556232940 arturo.lopez@mineria.unam.mx	
Revisó:	Mtro. Víctor Manuel Rivera Romay Jefe de la División de Educación Continua y a Distancia de la Facultad de Ingeniería. Tel. 5556232900 victor.rivera@mineria.unam.mx	
Autorizó:	Mtro. Víctor Manuel Rivera Romay Jefe de la División de Educación Continua y a Distancia de la Facultad de Ingeniería. Tel. 5556232900 victor.rivera@mineria.unam.mx	
Fecha de aprobación:	17/08/2022	
Fecha de actualización:	17/08/2022	

UNIDAD DE ALTA TECNOLOGÍA

ÍNDICE

Unidad de Alta Tecnología

La Facultad de Ingeniería de la UNAM fundó la Unidad de Alta Tecnología como unidad de posgrado y vinculación industrial para apoyar el desarrollo de las áreas estratégicas para la industria nacional.

En la Unidad de Alta Tecnología se llevan a cabo proyectos con las empresas que generan prototipos de máquinas, procesos y productos de alta tecnología.

Se ofrecen posgrados en los cuáles los estudiantes aprenden a trabajar en proyectos de innovación tecnológica industrial.

Se satisfacen las necesidades de la industria de la región por medio de proyectos de investigación y desarrollo en conjunto con empresas y programas académicos en ingeniería mecánica y en ingeniería aeroespacial.

Sistema de software de Control de Acceso Biométrico

El sistema de software de control de acceso biométrico permite controlar el acceso a las diferentes áreas de la Unidad.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología	
Identificador único*	UAT-01-DA-01
(Nombre del sistema) *	**Control de Acceso Biométrico**
Datos personales (sensibles o no) contenidos en el sistema*:	El sistema contiene datos personales en general. Nombre completo, número de cuenta UNAM o número de trabajador UNAM o número de matrícula o de identificación en el caso de alumnos o académicos provenientes de otras instituciones y huella dactilar.
Responsable*:	Delegado Administrativo de la UAT
Nombre*:	**Diego Valadez Rodríguez**
Cargo*:	**Delegado Administrativo de la UAT**
Funciones*:	- Resguardar el equipo donde reside el software y base de datos del sistema de control de acceso biométrico. - Resguardar la integridad física y operativa de los biométricos.
Obligaciones*:	- Recibir las solicitudes de alta, baja o modificación de datos.
	Encargados:
(Nombre del Encargado 1*)	**Diego Valadez Rodríguez**
Cargo*:	**Delegado Administrativo de la UAT**
Funciones*:	- Comprobar la identidad de la persona
Obligaciones*:	- Dar de alta en la base de datos general de los biométricos la información de los usuarios (datos generales y huella dactilar). - Pasar la información de los usuarios de la base de datos general a los biométricos en donde se requiere el acceso. - Borrar de los biométricos y de la base de datos general los datos de los usuarios que dejan de colaborar en la UAT. - Modificar en caso de requerirlo, alguno de los datos de los usuarios.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología	
Identificador único¨*	UAT-01-DA-01
(Nombre del sistema *)	Control de Acceso Biométrico
Tipo de soporte:*	Electrónico

Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Oficina. Área con control de acceso.

3. ANÁLISIS DE RIESGOS

4. ANÁLISIS DE BRECHA

5. PLAN DE TRABAJO

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología	
Identificador único*	UAT-01-DA-01
(Nombre del sistema)*	**Control de Acceso Biométrico**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se lleva a cabo transmisión de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se lleva a cabo transmisión de datos personales mediante el traslado de soportes electrónicos.

Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de datos personales se realiza en una red privada independiente y sin difusión (no se puede ver, no tiene acceso a internet). El sistema envía una notificación cuando establece o no comunicación con el biométrico, así mismo indica si los datos son enviados correctamente o si hubo alguna falla, y cuando los datos son modificados o eliminados también envía una notificación.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema de Control de Acceso Biométrico no cuenta con soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Sistema de Control de Acceso Biométrico

La UAT no llevan bitácoras de operación cotidiana, el acceso al software del control de acceso solo se lleva a cabo para realizar un nuevo registro o dar de baja un registro o realizar alguna modificación, normalmente se realizan a inicio y fin de cada semestre. Estas acciones las lleva a cabo el responsable a solicitud del jefe de la Unidad y jefes de Departamento. Los dispositivos biométricos almacenan registro de acceso al área donde están colocados, y se va sobre escribiendo. El registro de cada biométrico puede ser consultado desde el equipo que alberga el software y base de datos del Sistema de Control de Acceso. El único que puede hacer consultas es el responsable del Sistema de Control de Acceso Biométrico.

IV. REGISTRO DE INCIDENTES:

La UAT no cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

- Hay un punto de acceso principal en donde se cuenta con vigilancia las 24 hrs. Se puede ingresar a pie o en automóvil.
- Se debe identificar con el personal de vigilancia, quien cuenta con una relación de personal autorizado para ingresar a las instalaciones o un aviso en caso de ser visitantes, y la persona que los atenderá.
- Se autentifican con credencial de estudiante o académico, y los académicos además tienen un tag que les da acceso para ingresar en su vehículo.
- Para ingresar dentro de la Unidad se tienen dos accesos principales controlados por biométricos, y solo pueden ingresar quienes han sido registrados en ellos.
- No existe un sistema de tratamiento de datos personales de videovigilancia, pero se cuenta con cámaras de CCTV que cubren el pasillo donde se encuentran los accesos principales.

- Los alumnos son registrados en los biométricos de acceso principal y en los biométricos de los laboratorios o áreas en donde desarrollarán sus actividades, el acceso es solicitado por el profesor con el que estarán colaborando quien informa al jefe de la Unidad y al responsable del sistema de control de acceso biométrico.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
2. ¿Cómo las autentifica?
3. ¿Cómo les autoriza el acceso?

- No existe un sistema de tratamiento de datos personales de videovigilancia, pero se cuenta con cámaras de CCTV que cubren el pasillo donde se encuentra el acceso al área donde se tiene el equipo que alberga el sistema de control de acceso biométrico.
- El primer acceso es una puerta con cerradura y posteriormente un biométrico.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El sistema de Control de Acceso Biométrico almacena datos generales y una huella dactilar, que antes de guardar en la base de datos se verifican con el usuario, en caso de que tenga problemas al utilizar los biométricos se acude directamente con el responsable del sistema. No es frecuente registrar, dar de baja o modificar un registro, ya que solo se modifica la huella o se da de alta un PIN en caso de tener algún daño en la huella registrada.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?
c) ¿Está basado en roles (perfiles) o grupos? **Está basado en roles (perfiles)**
d) ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? **No**
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **No**
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **No**

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles?
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?

No se pueden dar de alta perfiles de usuario en el sofware del Sistema de Control de Acceso, es un único administrador.

5. Acceso remoto al sistema de tratamiento de datos personales:
- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? **No**
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? **No**
- **c)** ¿Cómo se evita el acceso remoto no autorizado? **No está configurado el acceso remoto, el equipo opera en una red de datos independiente.**

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

No se llevan a cabo respaldos.

IX. PLAN DE CONTINGENCIA

Actualmente no se cuenta con un plan de contingencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología		
Identificador único*	UAT-01-DA-01	
(Nombre del sistema)*	**Control de Acceso Biométrico**	
Recurso*	**Descripción***	**Control***

No se cuenta con herramientas o recursos para monitorear la protección de datos personales.

7.2. Procedimiento para la revisión de las medidas de seguridad

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología	
Identificador único*	UAT-01-DA-01
(Nombre del sistema)*	**Control de Acceso Biométrico**

Medida de seguridad*	Procedimiento*	Responsable*
Actualizaciones de seguridad	Revisar e instalar las actualizaciones del sistema operativo	a) Se llevan a cabo por el responsable del sistema de control de acceso biométrico. b) Un día.
Actualización del software antivirus	Revisar y mantener el software antivirus actualizado.	a) Se llevan a cabo por el responsable del sistema de control de acceso biométrico. b) Un día.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología		
Identificador único*	UAT-01-DA-01	
(Nombre del sistema)*	**Control de Acceso Biométrico**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Actualizaciones de seguridad	El sistema operativo cuenta con las actualizaciones más recientes.	El responsable de llevar a cabo las actualizaciones es el Lic. Diego Valadez Rodríguez, la responsable de verificar que el sistema este actualizado es la MI Ma del Socorro Armenta
Actualización del software antivirus	El equipo cuenta con software antivirus actualizado.	El responsable de llevar a cabo las actualizaciones es el Lic. Diego Valadez Rodríguez, la responsable de verificar que el antivirus este actualizado es la MI Ma del Socorro Armenta

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología	
Identificador único*	UAT-01-DA-01
(Nombre del sistema)*	**Control de Acceso Biométrico**

Medida de seguridad*	Acciones*	Responsable*
Revisar que herramientas pueden ayudar a proteger la base de datos donde se almacena la información de datos personales.	a) Familiarizarse con el sistema y la forma en que almacena la información. b) Buscar las herramientas.	a) Responsable de las acciones: MI Ma del Socorro Armenta Servín b) Fecha límite de conclusión: noviembre de 2022.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología			
Identificador único*	UAT-01-DA-01		
(Nombre del sistema)*	**Control de Acceso Biométrico**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se han recibido cursos de capacitación.

8.2. Programa de difusión de la protección a los datos personales

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología			
Identificador único*	UAT-01-DA-01		
(Nombre del sistema)*	**Control de Acceso Biométrico**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se cuenta con un programa de difusión de la protección de datos personales**.**

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología			
Identificador único*	UAT-01-DA-01		
(Nombre del sistema)*	**Control de Acceso Biométrico**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

La versión del sistema de Control de Acceso Biométrico depende del modelo de los biométricos que va a administrar. Si los modelos no cambian, la versión de software se mantiene y solo se van aplicando los parches de seguridad que correspondan si se proporcionan por el proveedor.

9.2. Actualización y mantenimiento de equipo de cómputo

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología			
Identificador único*	UAT-01-DA-01		
(Nombre del sistema)*	**Control de Acceso Biométrico**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del equipo de cómputo	A finales del 2021 se pudo actualizar el equipo de cómputo.	Poner a punto de operación el equipo, incluyendo la instalación de actualizaciones y configuraciones de seguridad, así como la instalación de todos los aplicativos se llevó a cabo en tres días.	Se cuenta con un equipo de mejores características para llevar a cabo las actividades.

9.3. Procesos para la conservación, preservación y respaldos de información

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología		
Identificador único*	UAT-01-DA-01	
(Nombre del sistema)*	**Control de Acceso Biométrico**	
Proceso*	**Descripción***	**Responsable***

No se han llevado a cabo respaldos.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Unidad de Alta Tecnología - Delegación Administrativa de la Unidad de Alta Tecnología		
Identificador único*	UAT-01-DA-01	
(Nombre del sistema)*	**Control de Acceso Biométrico**	
Proceso*	**Descripción***	**Responsable***
Borrado seguro	Formato a bajo nivel del disco duro del equipo.	Responsable de TICs de la UAT MI Ma del Socorro Armenta Servín
Disposición final de	Se siguen las disposiciones	Responsable de TICs de la

equipos y componentes informáticos	institucionales para dar de baja un equipo o componente.	UAT y delegado Administrativo de la UAT MI Ma del Socorro Armenta Servín Lic. Diego Valadez Rodríguez

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Actualmente no se cuenta con un procedimiento para la cancelación de un sistema de tratamiento de datos personales, ni se ha llevado a cabo la cancelación de alguno.

Sistema de Atención

El sistema de atención personalizada brinda atención a los alumnos de la licenciatura de la carrera de Ingeniería Aeroespacial en las asignaturas que administra la UAT. Este sistema entra en operación una vez que la Facultad ha concluido el proceso de cambios de grupo, altas y bajas.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz	
Identificador único*	UAT-02-DIAuto-01
(Nombre del sistema) *	**Sistema de Atención**
Datos personales (sensibles o no) contenidos en el sistema*:	El sistema contiene datos personales en general. Datos de los alumnos: Nombre completo, número de cuenta, número de inscripción, correo electrónico, fecha y hora de ingreso al sistema, carrera, asignatura(s) solicitada(s), clave(s) de asignatura(s), grupo(s) solicitado(s), Departamento que administra(s) la asignatura(s), comentarios, probatorios (historial académico, constancia de trabajo). Datos del Departamento: Nombre del Departamento, clave de Departamento. Datos de las asignaturas: Nombre y clave de asignatura. Datos de los administradores del sistema: Nombre completo, RFC, Departamento.
Responsable*:	Jefe de Departamento
Nombre*:	**MI Osiris Ricardo Torres**
Cargo*:	**Jefe del Departamento de Ingeniería Automotriz**
Funciones*:	Analizar y decidir sobre las solicitudes ingresadas por los alumnos al sistema.
Obligaciones*:	Atender las solicitudes que puedan proceder en base al cupo que haya en los grupos solicitados por los alumnos, tomando en cuenta los comentarios y probatorios que proporcionaron.
	Encargados:
(Nombre del Encargado 1*)	**MI Ma del Socorro Armenta Servín**
Cargo*:	**Responsable de TICs de la UAT**
Funciones*:	- Vigilar que el sistema opere y almacene la información adecuadamente y que cumpla con las medidas de seguridad.
Obligaciones*:	- Generar un respaldo de la base de datos y borrar los datos cada semestre una vez que finaliza el proceso.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz	
Identificador único¨*	UAT-02-DIAuto-01
(Nombre del sistema *)	Sistema de Atención
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar	Sala de servidores. Área restringida.

donde se resguardan los soportes:*	

3. ANÁLISIS DE RIESGOS

[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

5. PLAN DE TRABAJO

[redacted]

Fecha de clasificación:	Resolución CTUNAM/550/2022, emitida por el Comité de Transparencia, en sesión de fecha 2 de septiembre de 2022.
Información reservada:	Apartados identificados como "3. ANÁLISIS DE RIESGOS", "4. ANÁLISIS DE BRECHA" Y "5. PLAN DE TRABAJO", contenidos en las páginas 654 a 655.
Período de reserva:	5 años
Fundamento legal:	De conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz	
Identificador único*	UAT-02-DIAuto-01
(Nombre del sistema)*	**Sistema de Atención**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se lleva a cabo transmisión de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se lleva a cabo transmisión de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La conexión con la base de datos se lleva a cabo mediante el uso de una red privada virtual, y de la interfaz gráfica oficial de la base de datos, mediante la cual se puede administrar y llevar a cabo todas las tareas, entre ellas la exportación de esta, la cual se hace en el formato nativo de la base de datos.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Sistema de Atención
No cuenta con soporte físico.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Sistema de Atención
La UAT no lleva bitácoras como tal, el sistema solo funciona por unos días al inicio de cada semestre. Al responsable se le muestra la información ingresada por los alumnos.
El acceso a la base de datos solo lo puede llevar a cabo el encargado y es mediante uso de VPN y el manejo de la base de datos mediante la interfaz gráfica oficial del manejador.
El servidor que aloja el sistema de atención y la base de datos son institucionales y pertenecen a la Facultad, las bitácoras que puedan tener en los servidores quedan fuera del alcance y conocimiento de la UAT.

IV. REGISTRO DE INCIDENTES:

La UAT no cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

- Hay un punto de acceso principal en donde se cuenta con vigilancia las 24 hrs. Se puede ingresar a pie o en automóvil.
- Se debe identificar con el personal de vigilancia, quien cuenta con una relación de personal autorizado para ingresar a las instalaciones o un aviso en caso de ser visitantes, y la persona que los atenderá.
- Se autentifican con credencial de estudiante o académico, y los académicos además tienen un tag que les da acceso para ingresar en su vehículo.
- Para ingresar dentro de la Unidad se tienen dos accesos principales controlados por biométricos, y solo pueden ingresar quienes han sido registrados en ellos.
- No existe un sistema de tratamiento de datos personales de videovigilancia, pero se cuenta con cámaras de CCTV que cubren el pasillo donde se encuentran los accesos principales.
- Los alumnos son registrados en los biométricos de acceso principal y en los biométricos de los laboratorios o áreas en donde desarrollarán sus actividades, el acceso es solicitado por el profesor con el que estarán colaborando quien informa al jefe de la Unidad y al responsable del sistema de control de acceso biométrico.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
2. ¿Cómo las autentifica?
3. ¿Cómo les autoriza el acceso?

- No existe un sistema de tratamiento de datos personales de videovigilancia, pero se cuenta con cámaras de CCTV que cubren el pasillo donde se encuentra el acceso a las áreas donde se tiene el equipo activo de red y servidores.
- El site principal cuenta con puerta y cámara de cctv

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El sistema de Atención registra la información proporcionada por los alumnos cada semestre.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?
c) ¿Está basado en roles (perfiles) o grupos? **Está basado en roles (perfiles)**
d) ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? **No**
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **Si**
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **No**

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles? **El encargado del sistema**
b) ¿Quién autoriza la creación de nuevos perfiles? **El responsable del sistema**
c) ¿Se lleva registro de la creación de nuevos perfiles? **No**

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? **No**
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? **Se utiliza una conexión por VPN.**
c) ¿Cómo se evita el acceso remoto no autorizado? **Se deben tener credenciales para la VPN.**

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos **** Se van a comenzar a realizar**
   a) Completos_**x**_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __**x**___,
   c) Periodicidad con que los realiza: ___**cada semestre**____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: **Disco Duro Externo**

3. Cómo y dónde archiva esos medios: **El disco duro externo se encuentra en un archivero con llave**.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). **El área universitaria**.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz		
Identificador único*	UAT-02-DIAuto-01	
(Nombre del sistema)*	**Sistema de Atención**	
Recurso*	**Descripción***	**Control***

Actualmente no se cuenta con herramientas o recursos para monitorear la protección de datos personales, pero de acuerdo con el análisis de riesgos y el análisis de brecha, se estableció el plan de trabajo, con lo cual se pretende proteger los datos personales. Se buscarán las herramientas adecuadas para monitorear el sistema y la seguridad de los datos personales.

7.2. Procedimiento para la revisión de las medidas de seguridad

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz		
Identificador único*	UAT-02-DIAuto-01	
(Nombre del sistema)*	**Sistema de Atención**	
Medida de seguridad*	**Procedimiento***	**Responsable***

Actualmente no se cuenta con un procedimiento para revisar las medidas de seguridad, sin embargo, se empezará a trabajar en este.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz		
Identificador único*	UAT-02-DIAuto-01	
(Nombre del sistema)*	**Sistema de Atención**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Respaldo de la base de datos del sistema de atención	Restauración de la base de datos.	Responsable de TICs de la UAT MI Ma del Socorro Armenta Servín

Actualmente solo se ha llevado a cabo la prueba de restauración de respaldo de la base de datos.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz		
Identificador único*	UAT-02-DIAuto-01	
(Nombre del sistema)*	**Sistema de Atención**	
Medida de seguridad*	**Acciones***	**Responsable***
Revisar que mecanismos pueden brindar mayor seguridad.	Buscar los mecanismos de seguridad que puedan adecuarse al sistema de atención.	Responsable de las acciones: MI Ma del Socorro Armenta Servín

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz			
Identificador único*	UAT-02-DIAuto-01		
(Nombre del sistema)*	**Sistema de Atención**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se han recibido cursos de capacitación.

8.2. Programa de difusión de la protección a los datos personales

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz			
Identificador único*	UAT-02-DIAuto-01		
(Nombre del sistema)*	**Sistema de Atención**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

No se cuenta con un programa de difusión de la protección de datos personales**.**

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz			
Identificador único*	UAT-02-DIAuto-01		
(Nombre del sistema)*	**Sistema de Atención**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización y mantenimiento del sistema de atención	Revisar las actualizaciones o notificaciones de seguridad del sistema. Modificar las características del sistema de acuerdo a las necesidades o	Revisar cada fin de semestre si hay algo que pueda hacer vulnerable al sistema. Tres días. Llevar a cabo las modificaciones en caso de	Todo el sistema.

	situaciones que puedan presentarse.	necesitarse. El tiempo dependerá de la modificación a realizar.	

9.2. Actualización y mantenimiento de equipo de cómputo

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz			
Identificador único*	UAT-02-DIAuto-01		
(Nombre del sistema)*	**Sistema de Atención**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Los servidores donde residen los sistemas de la UAT son institucionales y pertenecen a la Facultad. La actualización y mantenimiento quedan fuera del alcance de la Unidad.

9.3. Procesos para la conservación, preservación y respaldos de información

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz		
Identificador único*	UAT-02-DIAuto-01	
(Nombre del sistema)*	**Sistema de Atención**	
Proceso*	**Descripción***	**Responsable***
Exportación de la base de datos	Se lleva a cabo utilizando la interfaz gráfica de la base de datos utilizando el formato nativo, y se almacenará en disco duro externo.	Responsable del proceso: MI Ma del Socorro Armenta Servín. Tiempo máximo de ejecución: 1 hr.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Unidad de Alta Tecnología - Departamento de Posgrado en Ingeniería Automotriz		
Identificador único*	UAT-02-DIAuto-01	
(Nombre del sistema)*	**Sistema de Atención**	
Proceso*	**Descripción***	**Responsable***
Realizar solicitud de borrado seguro de la base de datos.	Solicitar al área responsable de servidores institucionales el borrado seguro de la base de datos del sistema de atención.	Responsable de realizar la solicitud: MI Ma del Socorro Armenta Servin.

Al ser un servidor institucional el que alberga la base de datos del sistema de atención de la UAT, la disposición final de equipos y componentes informáticos queda fuera del alcance de la UAT.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Actualmente no se cuenta con un procedimiento para la cancelación de un sistema de tratamiento de datos personales, ni se ha llevado a cabo la cancelación de alguno.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	MI Ma del Socorro Armenta Servín Responsable de TICs de la Unidad de Alta Tecnología Tel. 4421926252 Ext UNAM 34352 msoco@comunidad.unam.mx msoco.armenta@ingenieria.unam.edu	
Revisó:	Dr. Marcelo López Parra Jefe de la Unidad de Alta Tecnología Tel. 4421926253 Ext UNAM 34353 lopezp@unam.mx	
Autorizó:	Dr. Marcelo López Parra Jefe de la Unidad de Alta Tecnología Tel. 4421926253 Ext UNAM 34353 lopezp@unam.mx	
Fecha de aprobación:	17/08/2022	
Fecha de actualización:	19/08/2022	