Políticas de seguridad en cómputo para la Facultad de ingeniería

(Fecha de última actualización: 16 de junio 2025)

Objetivo

Establecer los lineamientos sobre los cuales se debe conducir la comunidad de la Facultad de Ingeniería de la UNAM y demás entidades que se vean involucradas con la misma o hagan uso de la infraestructura y recursos de cómputo y telecomunicaciones de dicha dependencia,

Metas

Atender a la necesidad de lineamientos que resguarden la integridad de los recursos informáticos, para su correcto uso y aprovechamiento, manteniendo un ambiente de control donde el riesgo se minimice y se cuente con una base normativa como respuesta a cualquier incidente.

Alcance

El presente documento establece un marco normativo, por el que debe conducirse todo usuario o entidad que emplee los recursos de la infraestructura informática de la Facultad de Ingeniería de la UNAM, según sea su rol y actividad que desempeñe.

Comité Asesor de Cómputo

El Comité Asesor de Cómputo de la Facultad de Ingeniería (CACFI), tiene como responsabilidad el conjuntar esfuerzos entre los representantes de todas las áreas de la Facultad para lograr un desarrollo integral en el área de computación, procurar la normatividad, la estandarización y en general, buscar mecanismos de racionalización y optimización en materia de cómputo.

Está conformado por un Comité Ejecutivo y Comité Operativo, el primero integrado por el Staff de la Facultad de Ingeniería y el segundo por los responsables de cómputo de cada División, Secretaría y Coordinación de esta Facultad.

Es el CACFI quien se encarga de establecer las estrategias de seguridad en cómputo adecuadas, disminuir la cantidad y gravedad de los problemas de seguridad informática y difundir la cultura de la seguridad en cómputo en la Facultad de Ingeniería.

1. Políticas de seguridad física

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

Políticas:

1.1 Observar las políticas de actuación de la Comisión Local de Seguridad de la Facultad de Ingeniería (http://www.administracion.ingenieria.unam.mx/CLS/) para cualquier aspecto relacionado a la seguridad física, además de acatar las siguientes:

1.2 Mantener el equipo de cómputo alejado de cualquier tipo de agente que pueda causar algún daño o interfiera con su rendimiento como son: fuego, humo, polvo, temperaturas extremas, rayos solares, vibraciones, insectos, ruido eléctrico, balastros, equipo industrial, agua, etc.

1.3 Todos los servidores deberán ubicarse en lugares de acceso físico restringido y deben tener, para acceder a ellos, puertas con cerraduras.

1.4 El lugar donde se instalen los servidores debe contar con una instalación eléctrica adecuada, entre sus características debe contar con tierra física y sistemas de alimentación ininterrumpida o de emergencia, UPS (Uninterruptible Power Supply).

1.5 El área donde se encuentren los servidores deberá cumplir con los estándares de cableado estructurado y de no ser el caso regularizar dicho cableado. Se debe conservar limpio, organizado, y despejado de objetos extraños o ajenos para el uso al cual está destinado.

1.6 Se debe contar con extintores en las salas de cómputo acorde al tipo de fuego que pudiera aparecer y el personal debe estar capacitado en el uso de estos.

1.7 Las salas de cómputo deben contar con una salida de emergencia, la cual deberá estar siempre disponible, señalada y sin ninguna obstrucción, .

1.8 Las salas donde se encuentren los equipos de cómputo deben contar con la temperatura (18oC a 21oC) y humedad (65%) adecuadas para evitar deterioro o mal funcionamiento de los equipos de cómputo.

1.9 Deben existir los controles necesarios para autorizar o no el acceso a las personas, cualesquiera que fuera su actividad o rol, a las áreas de cómputo.

1.10 Se prohíbe el acceso a las salas de cómputo con cualquier tipo de alimento o bebida y cualquier producto de tabaco y sus derivados.

1.11 Separar el centro de datos y comunicaciones (servidores, dispositivos de redes de datos y telecomunicaciones, etc.) de las salas donde se destina equipo de cómputo para préstamo.

2. Políticas de reglamentos internos

La diversidad de actividades, tareas, y trabajos en la Facultad de Ingeniería de la UNAM requieren que los distintos departamentos, áreas, laboratorios y zonas de trabajo posean dinamismo y flexibilidad en sus actividades, por lo que las políticas presentadas a continuación tienen el objetivo de promover y ratificar el uso de reglamentos internos.

Políticas:

2.1 Los departamentos, laboratorios y áreas que requieran desarrollar normas, reglamentos internos o políticas de seguridad informática adicionales o complementarias a las contenidas

en este documento son libres de hacerlo, siempre y cuando sean consideradas las actuales políticas como las prioritarias, bajo supervisión constante del CACFI.

2.2 Los reglamentos, normatividades y políticas deben buscar, perseguir y tener los mismos objetivos y metas que las Políticas de Seguridad en Cómputo de la Facultad de Ingeniería de la UNAM.

2.3 Cualquier política deberá ser publicada y difundida con frecuencia, se recomienda una vez cada dos meses, a todos aquellos que estén en el alcance de la misma.

3. Políticas referentes al perfil del administrador

El rol del administrador de sistemas se refiere al profesional que tiene la responsabilidad de mantener, operar y asegurar el correcto funcionamiento de un sistema informático y/o una red de cómputo.

Políticas:

3.1 El cargo de administrador deberá ser asignado con base a la capacidad técnica, responsabilidad, experiencia y demás cualidades que su empleador considere necesarias para desarrollar adecuadamente las tareas correspondientes, características que éste último evaluará a través de los medios que considere pertinentes previas a la toma del puesto.

3.2 Acatará en plenitud las normas publicadas por la Facultad de Ingeniería de la UNAM manteniendo un ambiente de respeto a la comunidad universitaria y demás participantes que estén involucrados con el desarrollo de su trabajo.

3.3 Además de sus capacidades técnicas, el administrador deberá reconocer la importancia de la lealtad hacia la dependencia, contar con una actitud de desempeño proactivo, trabajo en equipo, capacidad de reacción bajo presión, facilidad para la resolución de problemas y disponibilidad ante emergencias.

3.4 El administrador debe estar en constante capacitación de acuerdo a los avances tecnológicos siendo coherente al surgimiento de nuevas Tecnologías de la Información.

4. Politicas de cuentas

La dupla conformada por el nombre de usuario y contraseña, denominada cuenta, constituye el primer control de acceso lógico a los sistemas de información, por lo que a continuación se establecen las características que deben de cumplir, la forma de asignación, creación y comunicación de las mismas.

Políticas:

4.1 La longitud de una contraseña debe ser igual o mayor a ~~8~~ 12 caracteres y contar con elementos en orden aleatorio de los cuatro dominios siguientes: números, letras mayúsculas,

letras minúsculas y caracteres especiales. No se permite el uso de contraseñas que incorporen palabras en cualquier idioma, series consecutivas de números, cadenas con caracteres sucesivos del mismo dominio o la inclusión de información personal. Cualquier contraseña que no cumpla con las características de construcción antes mencionadas se define como “contraseña débil”.

4.2 Debe construirse y emplearse una contraseña diferente por cada cuenta o sistema.

4.3 La comunicación de la contraseña se realizará de manera secreta y personal vía el administrador y sin intermediarios, así mismo la cuenta entregada al usuario es intransferible y todas las acciones realizadas con ella quedan bajo la responsabilidad del mismo.

4.4 El administrador debe contar con una cuenta sin privilegios con la cual realizará sus tareas, y en el estricto caso de que lo requiera cambiará a la cuenta de administración únicamente para realizar la acción que necesita estos permisos.

4.5 Las contraseñas deben cambiarse periódicamente. El lapso máximo de tiempo de vida queda a consideración del administrador y debe ser publicado en los medios que considere pertinentes y comunicado al usuario al momento de la entrega de la cuenta.

4.6 El usuario tendrá el derecho a cambiar su contraseña siempre y cuando cumpla con las características descritas en este documento.

4.7 El administrador es responsable de activar los mecanismos nativos de los sistemas, que permitan la detección de contraseñas débiles.

4.8 Queda estrictamente prohibido prestar o transferir las cuentas.

4.9 El administrador es responsable de bloquear o dar de baja aquellas cuentas que estén inactivas por más de dos meses o de ser necesario a consideración del administrador, si representa un riesgo de seguridad, confidencialidad o de alto almacenamiento .

5. Políticas de acceso remoto

El siguiente apartado tiene la finalidad de especificar cómo será el acceso a sistemas de cómputo o informáticos de la Facultad de Ingeniería.

Políticas:

5.1 Todos los equipos que proporcionen un servicio de: acceso remoto, de administración, un formulario, terminal remota, de correo electrónico o a una aplicación que solicita o transmite información sensible; deberán contar con aplicaciones que permitan una comunicación cifrada y segura.

5.2 Las conexiones remotas hacia la red o los servicios informáticos que brinda esta entidad se deben realizar mediante servicios seguros, tal como una VPN. El acceso a distancia a equipos de cómputo con servicios de escritorio remoto (tales como Anydesk, TeamViewer, Real VNC, etc.) no podrán ser utilizados previo a la autorización del administrador.

5.3 Los sistemas deben tener la capacidad de almacenar en bitácora, los registros de las entidades que han ingresado al mismo ya sea de manera remota o local, resguardando el nombre de la cuenta, dirección IP, fecha, hora y cualquier otro dato que permita dar seguimiento sobre las acciones que se realizan.

6. Políticas de uso adecuado

Las políticas de uso adecuado especifican lo que se considera un uso apropiado y correcto de los recursos que se asignan a la comunidad que forma parte de la Facultad de Ingeniería de la UNAM.

Políticas:

Usuarios en General:

6.1 La instalación de programas y software, en caso de requerirse debe ser solicitado al administrador del sistema y en su caso a su división, para que su representante ante el CACFI realice la gestión necesaria. Para equipo de cómputo que se encuentra en aulas o laboratorios la solicitud se debe realizar a través de la división o coordinación a la cual el usuario está adscrito de tal manera que sea gestionada la instalación en horarios que el equipo esté disponible.

6.2 Queda estrictamente prohibido la instalación de software que no cuente con una licencia vigente.

6.3 Queda estrictamente prohibido la instalación de software que no cuente con una licencia vigente.

6.4 El uso del equipo es estrictamente con fines académicos y/o investigación por lo que cualquier usuario que le dé algún otro uso será sancionado.

6.5 Pueden utilizar los servicios de interconexión a la infraestructura de red de datos, siempre y cuando sólo se haga con fines académicos y tenga el acceso permitido.

6.6 Pueden utilizar software de aplicación ya instalado.

6.7 Pueden utilizar los servicios de impresión donde este se brinde.

6.8 Se deben acatar los reglamentos internos en laboratorios, aulas, auditorios, salas de videoconferencia, etc., que presten un servicio asociado a la red de datos o con equipos de cómputo.

6.9 Los equipos de cómputo, cualesquiera que estos fueran, no pueden transferirse, moverse o trasladarse a otros lugares sin el previo consentimiento del responsable de cómputo de la División, Secretaría o Coordinación a la que pertenece. En todo momento esta transferencia debe ser notificada inmediatamente a la coordinación de bienes y suministros de la Secretaría Administrativa, acatando el procedimiento para este fin. (http://www.administracion.ingenieria.unam.mx/reasignacionDeBienesInventariables.html)

Académicos, Investigadores y Administrativos.

6.8 Pueden utilizar el equipo de cómputo asignado para realizar las actividades y funciones explícitamente definidas con base en su nombramiento.

6.9 El envío y almacenamiento de todo tipo de información sensible o de carácter confidencial debe contar con las medidas apropiadas de seguridad para su protección, el usuario es responsable de habilitar estas medidas.

6.10 Es responsabilidad del dueño de la información, realizar y resguardar sus respaldos en los medios que considere pertinentes, protegiéndola de esta manera en contra de fallos que podrían traer como consecuencia la pérdida o corrupción de la misma.

6.11 Los usuarios son responsables del software que instalen en los equipos bajo su custodia, de su licenciamiento, de actualizarlos y configurarlos conforme sus necesidades.

7. Políticas de respaldos

Especifican la responsabilidad que tienen los Usuarios y Administradores de Sistemas sobre el manejo de la información de la que son responsables según sea el caso.

7.1 Es responsabilidad del usuario mantener una copia, en un medio externo o diferente del lugar en donde se procesa u opera normalmente, de la información almacenada en la computadora que le fue asignada, en bases de datos, en buzones de correos, en servidores de almacenamiento, en servidores Web y de toda aquella información propia o bajo su custodia, inclusive si esta no se encuentra en equipos que el utilice directamente.

Administradores:

7.2 El administrador del sistema es el responsable de realizar respaldos de la información y configuración residente en los sistemas a su cargo, verificando que se haya realizado correctamente y notificando previamente a los usuarios sobre la periodicidad de esta acción.

7.3 El administrador del sistema es el responsable de restaurar la información derivada de los respaldos que realiza, en caso de ser necesario.

7.4 La información respaldada debe cifrarse y almacenarse en un lugar seguro, esto implica que el respaldo no debe estar ubicado en el mismo medio en el cual está alojado, preferentemente en un equipo de computo diferente o medio extraible.

7.5 Debe mantenerse una versión reciente de los archivos más importantes del sistema, quedando a consideración del administrador la periodicidad con la que se guarda dicha información.

7.6 En el momento en que la información almacenada sea obsoleta para la dependencia, dicha información debe destruirse del medio total y de forma permanentemente. Cada División, Secretaría o Coordinación determinará cuando la información es considerada obsoleta.

7.7 En caso de ser necesario el transportar información sensible o de carácter confidencial en una unidad portátil de almacenamiento (memoria USB Flash, disco duro, laptop u otros) esta debe ir cifrada y con la autorización del responsable de cómputo de la División, Secretaría o Coordinación.

8. Políticas de correo electrónico

Establecen el uso adecuado del servicio de correo electrónico, así como los derechos y las obligaciones que el usuario debe hacer valer y cumplir al respecto.

Políticas:

8.1 El personal académico y administrativo de la Facultad de Ingeniería de la UNAM tiene la facultad de solicitar una cuenta de correo al responsable de cómputo de su área, para el uso diario de sus actividades laborales.

8.2 Queda prohibido utilizar el correo electrónico para propósitos ajenos a la dependencia.

8.3 El usuario es la única persona autorizada para administrar su propio buzón.

8.4 Cuando la cuenta se ve involucrada en algún incidente de seguridad, el administrador podrá auditar dicha cuenta, previo aviso al responsable de Cómputo del área.

8.5 Los datos adjuntos recibidos en los correos pertenecientes a servidores de la Facultad de Ingeniería de la UNAM serán filtrados para excluir extensiones como “.exe”, “.bat”, “.msi” y todas aquellas que el administrador considere de riesgo para la seguridad del sistema.

8.6 Los usuarios de los sistemas de correo electrónico deben ser conscientes de la información que se envía o se recibe, probablemente no esté cifrada y no debe ser considerada como confidencial o inalterable. Los correos que no estén cifrados no podrán ser utilizados para la transmisión de información personal o sensible.

8.7 Los mensajes con información considerada sensible, deben ser aprobados por las autoridades de su División, Secretaría o Coordinación, antes de su distribución y al enviarlos se debe de tomar las medidas pertinentes para su aseguramiento.

8.8 Anti-malware de detección y cuarentena deberán ser instalados en todos los servidores de correo electrónico. Estas herramientas deben estar actualizadas.

8.9 Toda cuenta de correo electrónico dentro de los servidores de la Facultad de Ingeniería deberán tener una cuota limitada dentro del servidor.

8.10 Cualquier acceso por medios ilegales a cuentas ajenas será considerado un ataque al servidor de correo y a la privacidad de los usuarios, por lo que el causante será sancionado.

8.11 Si se descubre a un usuario manteniendo dentro de su correo algún malware o cualquier tipo de amenaza a nuestros servidores de manera intencional este será sancionado.

8.12 Queda prohibido configurar en servidores el Relay hacia direcciones IP ajenas a la dependencia.

8.13 La publicación en medios digitales de direcciones de correo electrónico debe ser realizada a través de una imagen y no sobre texto, a menos que se separe siguiendo el siguiente formato: “usuario at servidor dot dominio”. Por ejemplo: la dirección usuario@correo.com debe ser expresada como “usuario at correo dot com”.

9. Políticas de desarrollo de software

Las políticas aquí presentadas especifican los lineamientos para el desarrollo de aplicaciones de software.

Políticas:

9.1 El desarrollo de sistemas, herramientas y software en general cuyo propósito sea el de apoyar, facilitar y agilizar las actividades académicas, de investigación o de docencia para la Facultad de Ingeniería de la UNAM, así como los distintos proyectos en colaboración con alguna otra organización interna o externa, debe de seguir los lineamientos establecidos por la UNAM, en caso que estos no existan de manera particular para alguna tecnología, se debe de seguir las metodologías internas en cada dependencia considerando la compatibilidad entre sistemas.

9.2 Es necesario el desarrollo de documentación que permita dar seguimiento a las aplicaciones de software durante todo su ciclo de vida, siguiendo la metodología que la dependencia considere adecuada para dicho fin.

9.3 La elección de la tecnología de desarrollo y bases de datos debe ser realizada en referencia a la compatibilidad con los demás sistemas con los que la aplicación pueda interactuar.

9.4 Los desarrollos deben de incluir bitácoras de uso, nativas a la aplicación e independientes a las de la plataforma de software donde resida.

9.5 Previa a la liberación de los sistemas de información debe de realizarse un análisis de seguridad en un ambiente de pruebas, corrigiendo la totalidad de los fallos que sean detectados.

9.6 Todos los desarrollos previos a su liberación y puesta en marcha, deben encontrarse en sistemas aislados de la infraestructura de datos de la Facultad de Ingeniería de la UNAM.

10. Políticas de bitácoras del sistema

Establecen los lineamientos bajo los cuales será registrada la actividad de los usuarios en los sistemas informáticos, así como la manera en que deben manejarse los registros y el propósito de los mismos.

Políticas:

10.1 El administrador del sistema debe contar con herramientas de auditoría, ya sean verificadores de integridad, detectores de intrusos de host, correlacionadores de eventos, firewalls, etc. Con el propósito de mantener evidencia ante incidentes y datos que permitan el análisis estadístico.

10.2 El CACFI es el unico organismo con la facultad de realizar y autorizar el uso de herramientas de seguridad para el análisis de tráfico y vulnerabilidades en cualquiera de las redes y equipos de cómputo de la Facultad de Ingeniería de la UNAM para la detección de posibles incidentes de seguridad o como actividad diaria de la protección de redes y sistemas.

10.3 Está prohibida la utilización de “sniffers”, “keylogguers” o cualquier otro software espía en cualquier red o sistema de cómputo de la Facultad de Ingeniería.

10.4 Los responsables de cómputo de cada área tendrán la facultad de monitorear las redes y sistemas de las áreas que administran o coordinan.

10.5 El administrador puede hacer uso de la información resguardada en las bitácoras para deslindar responsabilidades sobre el mal uso de los sistemas o para fines estadísticos, con el objetivo de implementar métricas para el conocimiento del estado actual del servicio e identificación de puntos de mejora.

11. Políticas de uso de direcciones IP

El área responsable en representar a la Facultad de Ingeniería ante la DGTIC es CACFI y/o sus representantes.

Los responsables de cómputo de cada División, Secretaría o Coordinación son los representantes de red de su área ante el Comité Asesor de Cómputo de la Facultad de Ingeniería.

Políticas:

11.1 El responsable de cómputo o administrador de red debe contar con un inventario lógico de la red a su cargo, el cual contendrá el registro de las direcciones IP, direcciones físicas (MAC) y nombre del responsable, además de otros datos que le resulten relevantes.

11.2 El uso de las direcciones IP está regulado, por lo que sólo se pueden emplear direcciones IP que hayan sido asignadas previamente por el responsable de la red.

11.3 Ningún usuario final puede hacer alguna modificación en la configuración de la dirección IP asignada al equipo bajo su responsabilidad.

11.4 En el campus de Ciudad Universitaria está prohibido el uso de servidores de DHCP con direcciones IP homologadas.

11.5 Las subredes deben emplear rangos relacionados con la zona en la que se encuentren.

11.6 Cada equipo que se incorpore a Internet debe tener la autorización del administrador de la red del área en cuestión.

11.7 Los cambios de configuración de la red, como son direcciones IP, puertas de enlace, entre otros, deben ser autorizados por el administrador de la red.

11.8 Se permiten rangos de direcciones privadas de la forma 192.168.X.X pero su asignación deberá de controlarse únicamente a los equipos asignados al área.

11.9 Las direcciones IP que pueden otorgarse son homologadas o privadas. Las homologadas sólo son otorgadas si se justifican su uso y disponibilidad.

11.10 Los administradores de la red, en cada división, secretaría y coordinación podrán realizar reasignaciones de los rangos de las direcciones IP homologadas y privadas para un mejor desempeño de la red.

11.11 El administrador de red de la división y el representante ante el CACFI son los únicos autorizados para solicitar o dar de alta nombres canónicos de hosts y alias.

12. Políticas de sitios web

Las políticas aquí contenidas son lineamientos que se deben seguir para la operación de sitos web o páginas de Internet que operen en cualquier equipo de la Facultad de Ingeniería de la UNAM.

Políticas:

12.1 Los sitios WEB deben seguir las normas, lineamientos y recomendaciones establecidas por la UNAM.

12.2 Es responsabilidad de los administradores la actualización de los certificados digitales en el caso de contar con alguno.

12.3 Los servicios que se prestan por medio de los servidores deben solo tener instalados las herramientas y aplicaciones necesarias para los servicios que proporcionan.

12.4 La configuración de los servidores es responsabilidad del administrador o encargado, quienes deben configurar dichos servidores con el principio de mínimo privilegio.

12.5 Los administradores o responsables de los servidores son los encargados de su monitoreo, actualización, evaluación e instalación de parches de seguridad.

12.6 La creación de sitios web o repositorios en servidores y equipos de la Facultad de Ingeniería de la UNAM son con fines únicamente académicos, por lo que todo material almacenado como son archivos, documentos, programas, o cualquier otro tipo de material debe contar con permiso expreso, acuerdo de colaboración o ser de dominio público.

12.7 Los administradores de servidores, deberán implementar medidas de seguridad para minimizar el riesgo de ataques o posibles infecciones por alguna especie de malware.

13. Políticas para redes inalámbricas

Previamente y durante la implementación de una red inalámbrica se deben seguir las siguientes acciones.

Políticas:

13.1 Nadie está autorizado a instalar dispositivos inalámbricos de red, sin la previa supervisión del administrador de red y previa autorización del responsable del área, coordinación, secretaría o división, dado que actualmente se cuenta con conectividad PCPUMA, en caso y de ser necesario, debe estar fundamentada académicamente.

13.2 Si se requiere una red inalámbrica para laboratorios de redes dedicadas a pruebas y experimentación de los diversos protocolos y estándares, ésta deberá instalarse de forma autónoma e independiente y totalmente desconectada de la red de la Facultad, respetando en todos los casos el espacio radioeléctrico de las redes inalámbricas ya existentes y la previa autorización del Departamento de Administración de Redes y Operación de Servidores.

13.3 La red inalambrica debe ser registrada mediante el responsable de cómputo, división, secretaría o coordinación.

13.4 Cambiar las claves por defecto cuando se instala el software del Punto de Acceso (Access Point) o AP.

13.5 La instalación y configuración de los puntos de acceso deberá ser realizada por personal capacitado con los conocimientos técnicos necesarios, además se deberán modificar los parámetros establecidos por el fabricante del dispositivo para evitar que cualquier individuo tenga acceso a los mismos.

13.6 El administrador es el encargado de cambiar el SSID que trae el equipo como predeterminado, se debe establecer un SSID que indique a qué área o proyecto pertenece el mismo.

13.7 Los dispositivos inalámbricos de red están sujetos a las mismas reglas y políticas que se aplican a otros dispositivos electrónicos de comunicación por red cableada de la Facultad de Ingeniería.

13.8 El abuso o interferencia de los canales de comunicación inalámbrica con otras actividades que no sean las establecidas es una violación al uso aceptable. La interferencia o disrupción de otras comunicaciones autorizadas o la intercepción de otros tipos de tráficos constituyen una violación a las políticas y será sancionado.

13.9 El manejo de las contraseñas es responsabilidad del administrador o responsable el cual es el encargado de la instalación de las actualizaciones, el uso de cifrado y de permitir el acceso de los usuarios al punto de acceso.

Sobre la seguridad de redes inalámbricas:

13.10 No deberán de existir redes inalámbricas que sean de tipo abiertas, es decir que no tengan un mecanismo de autenticación.

13.11 Los puntos de acceso de las redes inalámbricas deberán contar con las últimas actualizaciones de su firmware antes de ser puestos en funcionamiento. Una vez que hayan iniciado su uso, también se deberá de estar actualizando de manera constante con las últimas versiones del firmware que llegaran a liberarse.

13.12 Una vez configurado el punto de acceso se deberán deshabilitar las formas de administración que no se vayan a ocupar, por ejemplo la administración vía página Web, etc.

13.13 El SSID de la red inalámbrica deberá de estar oculto al conocimiento público (No broadcast), en caso de ser necesaria la publicación del SSID de red, esta situación se informará durante el procedimiento de registro de la red inalámbrica.

13.14 Las redes inalámbricas deberán ser implementadas en segmentos de red diferentes al de la red cableada, es decir se deberán implementar con direcciones IP no homologadas, queda prohibida la utilización de direcciones IP homologadas para asignar de manera dinámica y estática en una red inalámbrica.

13.15 Los “puntos de acceso” no podrán ser administrados por los clientes inalámbricos. Toda administración de los “puntos de acceso” se realizará por medio de la red cableada.

13.16 Cuando se cuente con una antena externa conectada al punto de acceso, se deberá reducir la potencia de transmisión para sólo cubrir el área en la cual se necesita el servicio de la red inalámbrica.

Sobre la conexión a redes inalámbricas:

13.17 Los usuarios no deben compartir su conexión a la red inalámbrica con ningún otro individuo.

13.18 El usuario que tenga una cuenta no deberá otorgarla a otra persona para que acceda a la red.

13.19 No accederá a recursos de comunicaciones sin una previa autorización.

13.20 Queda prohibido la transmisión o distribución de cualquier material en violación de cualquier ley o regulación aplicable.

13.21 Copias de programas y aplicaciones está prohibido a excepción de que exista el permiso.

13.22 Las redes inalámbricas existentes en la Facultad de Ingeniería deberán implementar como mínimo las medidas de seguridad: Cifrado en la comunicación del tipo WPA2-Enterprise con 802.1x (EAP-PEAP), habilitar políticas de firewall, así como mecanismos de prevención y detección de intrusos (WIDS/WIPS).

14. Políticas de contratación y finalización de relaciones laborales de recursos humanos en sistemas informáticos.

Son las normas referentes con la contratación y el término de las relaciones con el personal que labora para la Facultad de Ingeniería.

Políticas:

14.1 Quedan excluidos de ser contratados como administradores de sistemas o áreas de seguridad informática aquellos que hayan tenido responsabilidades en incidentes graves de seguridad.

14.2 Al finalizar una relación laboral los administradores o encargados de sistemas deberán entregar todas las cuentas de los sistemas.
14.3 Los responsables de sistemas deben cambiar todas las contraseñas cuando un administrador de su área deje de prestar sus servicios de forma inmediata.

14.4 Todo personal que termine una relación laboral, deberá entregar a la entidad correspondiente cualquier tipo de recursos que se le hayan asignado durante su estancia, ya sean materia prima, equipos, respaldos lógicos o cualquier otro tipo de información.

15. Políticas referentes a la auditoria

Establece quienes son los responsables de realizar estos procedimientos con el objetivo de proteger los bienes y los recursos en las diferentes áreas.

Políticas:

15.1 El Departamento de Seguridad en Cómputo de la Facultad de Ingeniería (DSCFI) y el administrador en cuestión tienen la autoridad de realizar auditorías internas cuando estas se requieran, contando previamente con la autorización del responsable directo, el jefe del área o división a la que está asociado el administrador.

15.2 Un jefe de área, departamento, división, administrador o responsable directo debe justificar la realización de toda auditoría y documentarla a lo largo del proceso de la misma, incluyendo los resultados, considerándolo como información confidencial y sensible.

15.3 Toda auditoría debe ser planeada y ejecutada sin afectar a los usuarios del servicio, considerando los horarios y días que el administrador considere pertinentes para minimizar el impacto de las acciones.

15.4 Los responsables de realizar la auditoría deben de tener en cuenta que la información que encuentren es confidencial, por lo que deben ser éticos, y profesionales al realizar su trabajo, manteniendo respeto absoluto y discreción. De ser considerado necesario por el jefe directo, el auditor debe firmar un acuerdo de confidencialidad.

16. Políticas sobre incidentes graves

Se considera un incidente de seguridad a cualquier falta a las políticas que dictan este documento, dándole la calificación de grave a los eventosque ponen en riesgo la información y procesos sensibles para la Facultad de Ingeniería, también cuando existen afectaciones a la red de forma generalizada, intrusiones a servicios o servidores institucionales o aquellos incidentes que ponen en riesgo la estabilidad e imagen de la Facultad de Ingeniería.

Políticas:

16.1 Queda prohibido obtener privilegios o el control de cuentas del sistema, sin que se le haya otorgado explícitamente.

16.2 Es una falta grave el difundir, copiar, o utilizar información confidencial para otro propósito ajeno al cual está destinada.

16.3 Se prohíbe cualquier tipo de ataque o intento de explotar alguna vulnerabilidad a equipos de cómputo, así mismo infectar intencionalmente cualquier punto de la infraestructura de datos de la Facultad de Ingeniería de la UNAM con algún tipo de malware o modificar las configuraciones de algún tipo de equipo de cómputo sin ser autorizado para realizar dicho cambio.

16.4 Es causa de sanción el provocar cualquier tipo de daño intencional a los medios de comunicación de la red.

16.5 Todo incidente detectado debe ser comunicado al Departamento de Seguridad en Cómputo de la Facultad de Ingeniería (DSCFI) a través de la cuenta de correo “seguridad at ingenieria dot unam dot ~~mx~~ edu” o al teléfono 56-22-09-51 ó 56-22-09-55.

16.6 Las faltas a estas políticas serán investigadas por el área involucrada y si lo solicita, será apoyada por el DSCFI.

17. Politicas para el uso de dispositivos móviles y equipos personales

El propósito principal de estas políticas es establecer un método autorizado para el control de los dispositivos móviles de cómputo o almacenamiento que contienen o acceden a los recursos de información de la Facultad de Ingeniería.

Políticas:

17.1 Todos los usuarios de dispositivos móviles de cómputo o almacenamiento privados que deseen obtener acceso a la red de la Facultad de Ingeniería, debe registrar su dispositivo previamente, para que los administradores o encargados de la red, concedan los permisos necesarios y se tenga un registro del dispositivo.

17.2 Todos los dispositivos móviles de cómputo o almacenamiento que contengan o tengan acceso a los recursos de información de la Facultad de Ingeniería, deben autenticarse antes de poder establecer una conexión a los sistemas de información de la Facultad de Ingeniería.

17.3 Si los dispositivos móviles de cómputo o almacenamiento contienen información confidencial, personal o susceptible de la Facultad de Ingeniería, deben utilizar algún tipo de cifrado o medidas igualmente fuertes de protección en los datos, mientras éstos son almacenados.

17.4 A menos que se obtenga la aprobación del administrador de los datos, bases de datos, o porciones de ellas, que residan dentro de la red de la Facultad de Ingeniería, no se puede hacer ninguna descarga de ellos a los dispositivos móviles de cómputo o almacenamiento.

17.5 Los usuarios que hayan sido víctimas de robo o extravío de dispositivos móviles de cómputo o almacenamiento, que puedan comprometer la red o los recursos de información de la Facultad de Ingeniería, deberán notificar a las autoridades responsables de cómputo de su División, Secretaría o Coordinación, para que estas actúen, y se evite el compromiso de los datos y la red de la Facultad de Ingeniería de la UNAM.

18. Politicas referentes a la comunicación en medios digitales

El uso de los medios digitales constituidos a través de Internet se utilizan de manera generalizada, estas herramientas tienen el potencial de generar un impacto significativo en la reputación organizacional y profesional.

Estas políticas tienen como objetivo indicar el buen uso de esos mecanismos, para proteger la reputación social y profesional.

Políticas:

18.1 Las cuentas en redes sociales, páginas de Internet y todas aquellas constituidas a través de Internet y soportadas por las Tecnologías de la Información y las Comunicaciones, que representen a la Facultad de Ingeniería o alguna de sus áreas, deben ser oficialmente reconocidas y aprobadas por las autoridades pertinentes según sea el caso pueden ser: el Consejo Técnico de la Facultad, el Director, los Jefes de División, Secretarios y Coordinadores.

18.2 Cada cuenta en los medios de comunicación social deberán contar con un administrador responsable.

18.3 Cada cuenta oficial deberá incluir una declaración de renuncia de responsabilidad en relación a la forma, el contenido y las opiniones contenidas en el sitio.

18.4 El contenido inapropiado, ofensivo, perjudicial e ilegal podrá ser removido por los administradores de la cuenta o bajo la dirección de personal asignado por la Facultad de Ingeniería.

18.5 Todos los sitios existentes o páginas que representen a la Facultad de Ingeniería se revisarán regularmente y pueden ser modificadas o cuando sea necesario removidas.

18.6 Se supervisará la presencia de la Facultad de Ingeniería en los principales sitios de redes sociales y se evaluará la posibilidad de lanzar una presencia en sitios nuevos a medida que estén disponibles.

18.7 La Facultad de Ingeniería no avala ni asume la responsabilidad por el contenido publicado por terceros.

18.8 La Facultad de Ingeniería de la UNAM no tolerará contenido que infrinja información confidencial, o que sea difamatorio,pornográfico, acosador o inhóspito para un ambiente de trabajo razonable.

18.9 Personal y estudiantes de la Facultad deben tomar precauciones eficaces cuando se utilizan las redes sociales para garantizar su propia seguridad y protección contra robo de identidad.

18.10 El personal y los estudiantes deben considerar los derechos de propiedad intelectual, derechos de autor y la propiedad de los datos cuando se utilizan los medios de comunicación social.

18.11 Las asociaciones, departamentos, agrupaciones y demás grupos de trabajo, pueden hacer uso de las redes sociales para maximizar la exposición de sus servicios e investigaciones, cumpliendo siempre la presente normatividad.

18.12 No se puede publicar o compartir material ajeno sin permiso del propietario.

18.13 Queda prohibido la suplantación o el robo de identidad de cualquier imagen institucional de la Facultad de Ingeniería.

19. **Politicas referentes a las plataformas educativas ó recursos académicos**

Estas políticas tienen como objetivo establecer las normas apropiadas para el uso y desarrollo de plataformas educativas que tanto académicos como estudiantes de la Facultad de Ingeniería, semestre tras semestre utilizan como recursos para fines académicos y/o administrativos.

Políticas:

19.1 Los usuarios deben utilizar el servicio de las plataformas educativas como apoyo a sus actividades académicas.

19.2 Los responsables de la plataforma educativa deberán generar las cuentas de usuario para el acceso a la plataforma, a partir de un registro de los usuarios y distribuirá las contraseñas de manera segura.

19.3 El área a cargo de la plataforma educativa deberá suspender, desactivar o cancelar definitivamente los servicios de la cuenta asociada a un usuario, cuando detecte que este realiza actividades diferentes a las permitidas en la plataforma. A juicio de esta instancia se reactivará el servicio cuando se considere que el usuario no volverá a incurrir en una conducta prohibida.

19.4 La plataforma educativa deberá estar disponible en todo momento, salvo en situaciones de fuerza mayor, o por cortes parciales o interrupciones relativas al mantenimiento preventivo o correctivo de los equipos y elementos relacionados a la prestación del servicio.

19.5 Los usuarios de la plataforma educativa son responsables de instruirse y configurar sus cuentas con los procedimientos básicos para su funcionamiento así como contar con los mecanismos de respaldo para la protección de su información.

19.6 El uso de los recursos de la plataforma educativa deberá estar relacionado con las actividades académicas que el profesor realiza ante un grupo de alumnos inscritos a la Facultad de Ingeniería.

19.7 El usuario al momento de obtener su cuenta de acceso a la plataforma educativa, deberá conocer y manifestar su consentimiento para que el administrador realice monitoreo en su conexión de acceso, cuando por la ocurrencia de incidentes de seguridad informática lo estime necesario, con el único propósito de mantener la integridad y operación efectiva del servicio como respuesta a un requerimiento de las autoridades administrativas o judiciales.

19.8 Es responsabilidad del administrador de la plataforma educativa, mantener la integridad y operación eficaz de la misma, siendo capaz de realizar acciones de actualización y mantenimiento siempre en beneficio del servicio.

19.9 Los administradores de las plataformas son responsables de confirmar que los usuarios que soliciten el servicio y adquieran contraseñas para su uso, pertenecen a la comunidad de la Facultad de Ingeniería ya sea como estudiantes, académicos o investigadores.

19.10 El usuario es responsable de la confidencialidad de sus contraseñas.

19.11 El usuario del sistema debe de contar con un respaldo de su información.

19.12 Los administradores de las plataformas educativas son responsables de mantener confidencial todo tipo de información proporcionada por los usuarios.

19.13 Los usuarios deben hacer uso adecuado de los sistemas y no realizar ninguna acción ilegal al uso de los mismos.

20. Politicas sobre el uso y operación de las salas de cómputo de la Facultad de Ingeniería

Éstas políticas tienen como objetivo dirigir el buen uso y operación de las salas de cómputo que prestan servicio a la comunidad de la Facultad de Ingeniería.

Políticas:

20.1 El área responsable, deberá tener un registro de las personas que tienen permitido el acceso a las salas de cómputo.

20.2 Los usuarios deberán identificarse para tener acceso a las salas de cómputo.

20.3 Se prohíbe a los usuarios de las salas desconectar los nodos de las computadoras.

20.4 Se permite el uso de redes sociales con motivos académicos y de comunicación. Cualquier otro uso será sancionado.

20.5 Los responsables de las salas de cómputo deberán actualizar frecuentemente el software que ofrecen a sus usuarios, con base a los recursos proporcionados para ello.

20.6 Los dispositivos de almacenamiento extraíbles deberán estar libres de software malicioso antes de ser utilizados en las salas.

20.7 Se ofrecerán asesorías sobre el uso del software instalado en las salas a quien lo requiera.

20.8 Sólo se permite un usuario por máquina, si se desea entrar con un acompañante el usuario que registro su entrada tomara responsabilidad por cualquier daño hecho por el o por su acompañante sin excusa, esto siempre y cuando el laboratorio de acceso a más de una persona.

20.9 Cualquier persona que realice algún daño a los equipos de la Facultad de Ingeniería de la UNAM será sancionado.

20.10 Tanto los responsables de las salas como los usuarios deberán conducirse con respeto y cordialidad.

Sanciones

Las sanciones a que están sujetos los administradores, responsables de sistemas o usuarios por incumplimiento de sus obligaciones e incurrir enfalta a las Políticas señaladas en este documento, son las siguientes:

I. Llamada de atención de manera verbal o escrita.
II. Suspensión desde 15 días hábiles, hasta el fin del periodo escolar de los servicios en centros y salas de cómputo.

III. Suspensión definitiva de los servicios en salas y centros de cómputo.

IV. Reposición o pago de los bienes extraviados, destruidos o deteriorados.

Adicionalmente aplicación de las sanciones que de manera interna cada División, Secretaría o Coordinación describan en sus propios reglamentos.

Glosario

CACFI: Comité Asesor de Cómputo, órgano encargado de promover y asesorar el óptimo desarrollo informático de la Facultad de Ingeniería.

URL: http://www.ingenieria.unam.mx/cacfi/paginas/presentacion.html

Contraseña débil: Se considera contraseña débil a la cadena de caracteres que se emplea como contraseña en un sistema informático y que no cumple con las características de seguridad mínimas descritas en este documento. VER POLÍTICAS DE CUENTAS.

Correlacionador de eventos: Aplicación de software o dispositivo de hardware que permite analizar los eventos registrados en bitácoras de sistemas relacionados, con la finalidad de detectar posibles intrusiones o mal funcionamiento de alguna aplicación.

DHCP: Servicio o protocolo de asignación dinámica de direcciones IP.

Dirección IP: Secuencia de caracteres empleadas por el protocolo IP (Internet Protocol), para identificar un dispositivo dentro de la red.

Dirección MAC: Secuencia de caracteres cuyo fin es identificar a un equipo de otros, por sus siglas en inglés Medium Access Control.

Dispositivo móvil: Se considera como como un dispositivo móvil a computadoras portátiles, smartphones, Asistentes Personales Digitales (PDAs), Discos Compactos (CDs), Discos Digitales Versátiles (DVDs), unidades flash, discos duros portátiles, dispositivos Bluetooth y cualquier otro dispositivo que permita la movilidad de la información, ya sea para su procesamiento o su almacenamiento, de propiedad privada o de la propiedad de la Facultad de Ingeniería.

DSCFI: Departamento de Seguridad en cómputo de la Facultad de Ingeniería. ——————————

Firewall: Aplicación de software o dispositivo de hardware que limita el acceso hacia una red, equipo de cómputo o sistema de software, en base a un criterio establecido.

Incidente: Se considera como un incidente a cualquier falta o incumplimiento a las políticas establecidas en este documento.
IP Homologada: Dirección IP cuyo segmento corresponde a las redes públicas y que son accesibles desde Internet.

IP no homologada o privada: Dirección IP cuyo segmento corresponde a las redes locales y que no son accesibles desde la Internet.
Malware: Código generado con fines maliciosos, entre los que ubicamos: virus, caballos de troya, gusanos, spyware, etc.

Punto de Acceso (Access Point) o PA: Dispositivo de red que permite la conexión de manera inalámbrica a la red.

Relay: Configuración que permite el reenvío de correo electrónico.

Sistema Detector de Intrusos: (IDS) Por sus siglas en inglés Intrusion Detector System, aplicación de software que permite la detección de agentes maliciosos a un sistema o red de cómputo.

Sniffer: Aplicación que permite el análisis de la información que transita en una red.

Tupla: Conjunto de n datos ordenados.

UPS: Por sus siglas en inglés Uninterruptible Power Supply es un dispositivo de suministro eléctrico que cuenta con una batería con la finalidad de proporcionar energía a un dispositivo en el caso de interrupción o falla del suministro principal.

Verificador de integridad: Aplicación de software que permite verificar la consistencia de la información entre dos instantes diferentes.