POLÍTICAS DE SEGURIDAD EN CÓMPUTO PARA LA FACULTAD DE INGENIERÍA SUBCOMITÉ DE ADMINISTRADORES DE RED

MARZO DEL 2003

CONTENIDO

I. INTRODUCCIÓN

Este documento presenta las políticas de alcance institucional que permite crear y establecer una educación y una filosofía sobre la postura que en materia de seguridad en cómputo debe tener la institución respecto a los riesgos que la rodean.

Las políticas define ciertos lineamientos que establecen un límite entre lo que está permitido a los usuarios dentro de la institución y fuera de ella y lo que no está, esto es con el propósito de proteger la información almacenada en los sistemas y el acceso a éstos.

Para ello para la institución, el principio básico de seguridad es "Lo que no se permite expresamente, está prohibido".

La tecnología tiene la capacidad para abrir las puertas a un vasto mundo de recursos de información, así como de personas, a cualquier estudiante o miembro de la comunidad universitaria con una conexión a Internet. Las oportunidades que tenemos con esta conectividad son casi ilimitadas, mas no así, los recursos computacionales y de conectividad disponibles. Este nuevo mundo virtual al que tenemos acceso requiere de reglas y precauciones, para asegurar un uso óptimo y correcto de los recursos. En este sentido, la Facultad de Ingeniería cree firmemente en que el desarrollo de políticas que sean bien entendidas, que circulen ampliamente y que sean efectivamente implementadas, conllevará a hacer de la red de cómputo de la Facultad y el Internet un ambiente más seguro y productivo para estudiantes y miembros en general de la comunidad universitaria.

Las políticas de seguridad son los documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos que tanto usuarios como administradores tienen y qué hacer ante un incidente de seguridad.

Mientras las políticas indican el “qué”, los procedimientos indican el “cómo”. Los procedimientos son los que nos permiten llevar a cabo las políticas. Ejemplos que requieren la creación de un procedimiento son los siguientes:

- Otorgar una cuenta.
- Dar de alta a un usuario.
- Conectar una computadora a la red.
- Localizar una computadora.
- Actualizar el sistema operativo.
- Instalar software localmente o vía red.
- Actualizar software crítico.
- Exportar sistemas de archivos.
- Respaldar y restaurar información.
- Manejar un incidente de seguridad.

Para que esto sirva de algo, las políticas deben ser:

- Apoyadas por los directivos.

- Únicas.
- Claras (explícitas).
- Concisas (breves).
- Bien estructuradas.
- Servir de referencia.
- Escritas.
- Dadas a conocer.
- Entendidas por los usuarios.
- Firmadas por los usuarios.
- Mantenerse actualizadas.

Las políticas son parte fundamental de cualquier esquema de seguridad eficiente. Como administradores, nos aminoran los riesgos, y nos permiten actuar de manera rápida y acertada en caso de haber una emergencia de cómputo. Como usuarios, nos indican la manera adecuada de usar un sistema, indicando lo que puede hacerse y lo que debe evitarse en un sistema de cómputo, contribuyendo a que no seamos "malos vecinos" de la red sin saberlo. El tener un esquema de políticas facilita grandemente la introducción de nuevo personal, teniendo ya una base escrita y clara para capacitación; dan una imagen profesional a la organización y facilitan una auditoría.

Los principales puntos que deben contener las políticas de seguridad son los siguientes:

- Ámbito de aplicación.
- Análisis de riesgos.
- Enunciados de políticas.
- Sanciones.
- Sección de uso ético de los recursos de cómputo.
- Sección de procedimientos para el manejo de incidentes.

Al diseñar un esquema de políticas de seguridad, conviene que dividamos nuestro trabajo en varias diferentes políticas específicas: cuentas, contraseñas, control de acceso, uso adecuado, respaldos, correo electrónico, contabilidad del sistema, seguridad física, etc.

II. SEGURIDAD EN CÓMPUTO

Es un conjunto de recursos destinados a lograr que los activos de una organización sean confidenciales, íntegros, consistentes y disponibles a sus usuarios, autentificados por mecanismos de control de acceso y sujetos a auditoría.

- Confidencial. La información debe ser leída por su propietario o por alguien explícitamente autorizado para hacerlo.
- Íntegro. La información no debe ser borrada ni modificada por alguien que carezca de autorización para hacerlo.
- Consistente. El sistema, al igual que los datos, debe comportarse como uno espera que lo haga.

- Disponible. La información debe estar siempre disponible en el lugar y cantidad de tiempo requeridos.
- Autentificado. Únicamente deben ingresar al sistema personas autorizadas, siempre y cuando comprueben que son usuarios legítimos.
- Control de acceso. Debe conocerse en todo momento quién entra al sistema y de dónde procede.
- Auditoría. Deben conocerse en cada momento las actividades de los usuarios dentro del sistema.

Las políticas del presente documento tienen como alcance a la Facultad de Ingeniería de la UNAM.

Factores Críticos

Es necesario hacer énfasis en que el apoyo por parte de la gente con el poder de decisión (cuerpo directivo) es fundamental para el éxito de un esquema de seguridad, ya que sin él, algunos elementos de dicho esquema no tendrían validez. Es vital mantener en constante capacitación al personal mediante cursos, seminarios, congresos, etc. La mejor defensa es el conocimiento. Los usuarios deben conocer el uso adecuado de los sistemas de cómputo y saber cómo protegerse a sí mismos de accesos no autorizados. Debe crearse una cultura de seguridad, haciendo ver a la gente involucrada los peligros a los que se está expuesto en un ambiente tan hostil como el que ha generado la evolución de las actuales redes de computadoras.

Políticas De Seguridad

La política que seguiremos será prohibitiva: "Lo que no esté explícitamente permitido queda prohibido."

III. POLÍTICAS DE SEGURIDAD FISICA

El primer paso a considerar en un esquema de seguridad, que muchas veces no recibe suficiente atención, es la seguridad física; las medidas que se usan para proteger las instalaciones en las que reside un sistema de cómputo: llaves, candados, tarjetas de acceso, puertas, ventanas, alarmas, vigilancia, etc.

Políticas respecto a la seguridad física:

- Mantener las computadoras alejadas del fuego, humo, polvo y temperaturas extremas.
- Colocarlas fuera del alcance de rayos solares, vibraciones, insectos, ruido eléctrico (balastras, equipo industrial, etc.), agua, etc.
- Todos los servidores deberán ubicarse en lugares de acceso físico restringido y deberán contar para acceder a ellos con puertas con chapas.
- El lugar donde se instalen los servidores contarán con una instalación eléctrica adecuada, entre sus características con tierra física. Y dichos equipos deberán contar con NO-BREAKS.
- En los lugares donde se encuentren equipo de cómputo queda prohibido el consumo de bebidas y alimentos.
- El lugar donde se encuentre los servidores mantendrán condiciones de higiene.
- Deberá contarse con extintores en las salas de cómputo. El personal deberá estar capacitado en el uso de extintores.
- Las salas de cómputo deberán contar con una salida de emergencia.

IV. POLÍTICAS DE CUENTAS

Establecen qué es una cuenta de usuario de un sistema de cómputo, cómo está conformada, a quién puede serle otorgada, quién es el encargado de asignarlas, cómo deben ser creadas y comunicadas.

Políticas:

Las cuentas deben ser otorgadas exclusivamente a usuarios legítimos. Se consideran usuarios legítimos aquellos usuarios quienes hayan realizado su tramite de registro de cuenta y que:

1. Sean miembros vigentes de la comunidad de la Facultad de Ingeniería.
2. Participen en proyectos especiales y tenga la autorización del jefe del área.
3. Una cuenta deberá estar conformada por un nombre de usuario y su respectiva contraseña.
4. La asignación de cuentas la hará el administrador del servidor del área en cuestión y al usuario sólo le dará derecho de acceder a los recursos al servidor donde se realiza el registro.
5. El administrador podrá deshabilitar las cuentas que no sean vigentes.
6. La cuenta y contraseña personales son intransferibles.

V. POLÍTICAS DE CONTRASEÑAS

Son una de las políticas más importantes, ya que por lo general, las contraseñas constituyen la primera y tal vez única manera de autenticación y, por tanto, la única línea de defensa contra ataques. Éstas establecen quién asignará la contraseña, qué longitud debe tener, a qué formato deberá apegarse, cómo será comunicada.

Políticas:

- El administrador del servidor será el responsable de asignar las contraseñas.
- El administrador deberá contar con herramientas de detección de contraseña débiles.
- La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el administrador/usuario. Todas las contraseñas deberán contar con al menos seis caracteres.
- Todas las contraseñas elegidas por los usuarios deben ser difíciles de adivinar. No deben ser utilizadas palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.
- Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar.
- Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores.
- La comunicación de la contraseña se realizará de manera personal y no se podrá informar a otra persona que no sea el interesado.
- No se podrán informar contraseñas por vía telefónica.
- Las contraseñas deberán cambiarse máximo cada seis meses.

VI. POLÍTICAS DE CONTROL DE ACCESO

Especifican cómo deben los usuarios acceder al sistema, desde dónde y de qué manera deben autentificarse.

Políticas:

- Todos lo administradores que den un servicio de acceso remoto deberán contar con aplicaciones que permitan una comunicación segura y encriptada.
- Todos los usuarios deberán autentificarse con su cuenta y no podrán hacer uso de sesiones activas de otros usuarios.
- Todos los usuarios deberán acceder al sistema utilizando algún programa que permita una comunicación segura y encriptada.
- Está prohibido acceder al sistema con una cuenta diferente de la propia, aún con la autorización del dueño de dicha cuenta.
- Si un usuario está fuera del sitio de trabajo, debe conectarse a una máquina pública del sitio y, únicamente desde ésta, hacer la conexión a la computadora deseada.
- Al momento de ingresar a un sistema UNIX, cada usuario deberá ser notificado de la fecha, hora y dirección desde la que se conectó al sistema por última vez, lo cual permitirá detectar fácilmente el uso no autorizado del sistema.
- El usuario tendrá el derecho a cambiar su contraseña.
- El usuario podrá utilizar los servicios de sesiones remotas si se brinda.

VII. POLÍTICAS DE USO ADECUADO

Especifican lo que se considera un uso adecuado o inadecuado del sistema por parte de los usuarios, así como lo que está permitido y lo que está prohibido dentro del sistema de cómputo.

Existen dos enfoques: permisivo (todo lo que no esté explícitamente prohibido está permitido) y prohibitivo (todo lo que no esté explícitamente permitido está prohibido). Cuál de estas elegir dependerá del tipo de organización y el nivel de seguridad que esta requiera.

Permitido
Alumnos:

- Realizar sus tareas con fines académicos y asociadas con los programas académicos de Ingeniería.
- Utilizar los servicios de Internet donde se brinden, con fines académicos.
- Utilizar software de aplicación ya instalado.
- Utilizar los servicios de impresión donde se brinden.

Académicos, Investigadores y Administrativos.

- Utilizar el equipo de cómputo asignado para realizar sus actividades y funciones explícitamente definidas de su plaza.

- Las áreas de Investigación de Seguridad en Cómputo de la Facultad de Ingeniería (AISCFI), serán autorizadas en el subcomité de administradores de red, dichas áreas serán las únicas a las que se permitirán realizar pruebas e investigación de seguridad informática, en ambientes controlados. Las AISCFI deberán solicitar permiso e informarán de dichas pruebas al subcomité de administradores, donde se describirán del tipo de pruebas, lugar de las pruebas, fechas y horas. Cómo requisito deberán realizarse en lugares aislados (redes internas), que no comprometan la operación de las demás áreas.

Prohibido

- Está terminantemente prohibido ejecutar programas que intenten adivinar las contraseñas alojadas en las tablas de usuarios de máquinas locales o remotas.
- La cuenta de un usuario es personal e intransferible, por lo cual no se permite que este comparta su cuenta ni su contraseña con persona alguna, aún si ésta acredita la confianza del usuario.
- Está estrictamente prohibido hacer uso de herramientas propias de delincuentes informáticos, tales como: programas que rastrean vulnerabilidades en sistemas de cómputo propios o ajenos.
- Está estrictamente prohibido hacer uso de programas que explotan alguna vulnerabilidad de un sistema para proporcionar privilegios no otorgados explícitamente por el administrador .
- No se permite instalar programas y software propio, en caso de requerirse deberá solicitarlo al administrador del sistema.
- No se permite bajo ninguna circunstancia el uso de cualquiera de las computadoras con propósitos de ocio o lucro. Por lo cual se prohíbe descargar (o proveer) música, imágenes, videos, chatear, etc., con fines de ocio.

VIII. POLÍTICAS DE RESPALDOS

Para el usuario

- Será responsabilidad del usuario mantener una copia de la información de su cuenta.

Para el administrador del sistema

- El administrador del sistema es el responsable de realizar respaldos de la información crítica, siempre que tenga los medios físicos para realizarla. Cada treinta días deberá efectuarse un respaldo completo del sistema. y deberá verificar que se haya realizado correctamente.
- El administrador del sistema es el responsable de restaurar la información.
- La información respaldada deberá ser almacenada en un lugar seguro.
- Deberá mantenerse una versión reciente de los archivos más importantes del sistema.
- En el momento en que la información respaldada deje de ser útil a la organización, dicha información deberá ser borrada antes de deshacerse del medio.

IX. POLÍTICAS DE CORREO ELECTRÓNICO

Establece tanto el uso adecuado como inadecuado del servicio de correo electrónico, los derechos y obligaciones que el usuario debe hacer valer y cumplir al respecto.

Políticas:

- El usuario es la única persona autorizada para leer su propio correo, a menos que él mismo autorice explícitamente a otra persona para hacerlo, o bien, que su cuenta esté involucrada en un incidente de seguridad de cómputo, donde el administrador del sistema podrá auditar dicha cuenta.
- Está estrictamente prohibido usar la cuenta de correo electrónico proporcionada por la organización para propósitos ajenos a sus actividades académicos o laborales según sea el caso.
- Está prohibido enviar correos conteniendo injurias, falsedades y malas palabras.
- Está prohibido enviar correos sin remitente y sin asuntos.
- Está prohibido enviar por correo virus, archivos o información que ponga en peligro la seguridad del sistema.
- Está prohibido enviar correos SPAM.
- Está prohibido enviar correos de publicidad personal o con intereses personales.
- Está prohibido enviar correos haciéndose pasar por otra persona.
- Está prohibido reenviar cadenas, chistes y toda clase de información intrascendente, ajena a la actividad académica o laboral del usuario.

X. POLÍTICAS DE CONTABILIDAD DEL SISTEMA

Establecen los lineamientos bajo los cuales pueden ser monitoreadas las actividades de los usuarios del sistema de cómputo, así como la manera en que debe manejarse la contabilidad del sistema y el propósito de la misma.

Políticas.

- El administrador del sistema deberá contar con herramientas de auditoria en el sistema.
- El administrador de red de la división o secretaría podrá realizar un monitoreo de su red, o de toda en caso de un incidente de seguridad y cuando necesite estadísticas para rediseñar su red.
- Los usuarios finales en ninguna situación podrá realizar monitoreos de la red.
- Los responsables de cómputo y el administrador general de la red tienen la autoridad de realizar auditorías internas permanentemente.

XI. POLÍTICAS DE USO DE DIRECCIONES IP

El área responsable en representar a la Facultad de Ingeniería ante DGSCA es Secretaría General.

- El administrador de red deberá contar con un registro de sus direcciones IP utilizadas.
- El formato que utilizará para registrar su información esta contenido en el Apéndice A.
- Ningún área puede hacer uso de una dirección IP que no le corresponda, sin autorización expresa y escrita del administrador del área en cuestión.

- Ningún usuario final podrá hacer modificación en la configuración de su dirección IP asignada al equipo de su responsabilidad.
- En el campus de C.U. No se permiten el uso de servidores de DHCP con Direcciones IP homologadas.
- No se permiten utilizar en subredes de una zona, rangos de otras zonas. Por ejemplo de la en la zona A, utilizar, rangos de la zona C.
- Cada equipo que se incorpore a la red Internet deberá tener autorización del administrador de red del área en cuestión.
- Si se realiza un cambio de tarjeta de red se deberá de informar del reemplazo y de la dirección física asociada a la IP al administrador de red.
- Se permite rangos de direcciones privadas 192.168.X.X pero su asignación deberá de controlarse únicamente a los equipos asignados al área.
- Las direcciones IP que podrán otorgarse serán homologadas o privadas. Las homologadas sólo serán otorgadas si se justifican su uso y disponibilidad. Para asignar una dirección IP deberá justificarse su utilización y solicitarla al administrador o responsable de cómputo para su autorización.
- El administrador de red podrá realizar reasignaciones de los rangos de la direcciones IP homologadas y privadas para un mejor desempeño de la red.
- El administrador de red y el representante ante comité de cómputo son los únicos autorizados en solicitar dar de alta nombres canónicos de hosts, alias, mail Exchangers al Administrador General de la Red.

XII. POLÍTICAS DE WEB.

Véase LA Normatividad del Web.

XIII. POLÍTICAS DE CONTRATACIÓN Y FINALIZACIÓN DE RELACIONES LABORALES DE RECURSOS HUMANOS EN SISTEMAS INFORMÁTICOS.

Políticas

- No podrán ser contratados personas como administradores de sistemas o en áreas de seguridad informática que hayan tenido responsabilidades en incidentes graves de seguridad.
- Al finalizar una relación laboral los administradores o encargados de sistemas deberán entregar todas las cuentas y contraseñas de los sistemas críticos.
- Los responsables de sistemas deberán cambiar todos las contraseñas críticas cuando un administrador de su área deje de prestar sus servicios.

XIV. SANCIONES

Al crear nuestras políticas es necesario contemplar diferentes escenarios.

Tarde o temprano, todas las políticas serán violadas. ¿Qué puede llevar a que una política sea violada?

- Negligencia.
- Error accidental.
- Desconocimiento de la misma.
- Falta de entendimiento de la misma.

¿Qué debemos hacer si una política es violada?

- Investigar quién llevó a cabo esta violación.
- Investigar cómo y por qué ocurrió esta violación.
- Aplicar una acción correctiva (disciplinaria).

¿Qué sucede si un usuario local viola las políticas de un sitio remoto?

- Debe haber acciones a seguir bien definidas con respecto a los usuarios locales.
- Debe estarse bien protegido en contra de posibles acciones desde el sitio remoto.

¿Cómo reaccionar ante un incidente de seguridad? Hay dos estrategias básicas:

- Proteger y perseguir
    - Su principal objetivo es proteger y preservar los servicios del sitio, y restablecerlos lo más rápido posible.
    - Se realizan acciones drásticas, tales como dar de baja los servicios, desconectar el sistema de la red, apagarlo, etc.
    - Lo utilizamos cuando:
    - Los activos están bien protegidos
- Se correo un gran riesgo debido a la intrusión.
- No existe la posibilidad o disposición para enjuiciar.
- Se desconoce la base del intruso.
- Los usuarios son poco sofisticados y su trabajo es vulnerable.
- Los recursos de los usuarios son minados.
- Perseguir y enjuiciar
    - Su objetivo principal es permitir que los intrusos continúen con sus actividades en el sistema hasta que pueda identificarse a los responsables.
    - Lo utilizamos cuando:
        - Los recursos están bien protegidos.
        - Se dispone de respaldos confiables.
        - El riesgo para los activos es mayor que el daño de esta y futuras intrusiones.
        - El ataque proviene de un sitio con el que guardamos cierta relación, y ocurre con cierta frecuencia e intensidad.
        - El sitio posee cierta atracción para los intrusos.
        - El sitio está dispuesto a correr el riesgo a que se exponen los activos al permitir que el ataque continúe.
        - Puede controlarse el acceso al intruso.
        - Se cuenta con herramientas de seguridad confiables.

- El personal técnico conoce a profundidad el sistema operativo y sus utilerías.
- Existe disposición para la persecución por parte de los directivos.
- Existen leyes al respecto.
- En el sitio existe alguien que conozca sobre cuestiones legales.

Políticas de sanciones

En caso de un incidente de seguridad grave (Un evento que pone en riesgo la seguridad de un sistema de cómputo).

Tales como:

- Obtener el privilegio de root o administrador del sistema, sin que se le haya otorgado explícitamente.
- Borrar, modificar Información.
- Difundir información confidencial.
- Copiar Información confidencial.
- Ataques maliciosos a equipos de cómputo.
- Ejecución de Programas para obtener privilegios y que sean exitosos
- Violar correos de cuentas ajenas.
- Un incidente donde esté involucrado un administrador de sistema u trabajador de la UNAM.
- Infectar intencionalmente un servidor con virus.
- Modificar Configuraciones de Switches y ruteadores sin ser responsables del equipo.
- Daño físico intencional a los medios de comunicación de la red, como fibra óptica, UTP, Switches, hubs, ruteadores, transceivers.

Si se llegase a ocurrir un incidente grave se reportará al Departamento de Seguridad de la DGSCA y se seguirán los procedimientos establecidos por ellos. Como medida precautoria y teniendo como prioridad el mantener la seguridad de los sistemas, las cuentas involucradas se deshabilitarán en toda la Facultad hasta que se deslinden las responsabilidades del incidente.

Sanciones

Se darán las siguientes sanciones a los usuarios:

ACTIVIDAD NO LÍCITA	**SANCIÓN**
Consumo de alimentos, bebidas, utilización de los servicios por ocio.	Suspensión del servicio por un día. **Reincidencia.** Cancelación de los servicios por un mes en todas las áreas de la Facultad de Ingeniería.
Utilizar una sesión activa ajena	Suspensión por un día su cuenta. **Reincidencia.** Suspensión de los servicios por un mes en todas las áreas de la Facultad de Ingeniería
Acceso con una cuenta diferente a la propia, con permiso del propietario	Suspensión por un mes de los servicios en la Facultad de Ingeniería, del que presta y del que usa la cuenta. **Reincidencia.** Suspensión por un semestre.
Ejecución de programas que intenten adivinar cuentas y contraseñas locales o remotos	Suspensión de los servicios por un año en todas las áreas de la Facultad. **Reincidencia.** Cese definitivo de los servicios de cómputo, durante toda su carrera.
Ejecución de herramientas para rastrear vulnerabilidades en sistemas de cómputo propios o ajenos.	Suspensión de los servicios por un año en todas las áreas de la Facultad. **Reincidencia.** Cese definitivo de los servicios de cómputo, durante toda su carrera.
Hacer uso de programas que explotan alguna vulnerabilidad del sistema.	Suspensión de los servicios por un año en todas las áreas de la Facultad. **Reincidencia.** Cese definitivo de los servicios de cómputo, durante toda su carrera.
Instalación de software externo al oficial	Suspensión del servicio por una semana.

	Reincidencia. Suspensión por un mes.
Cambio de la configuración de los Equipos y que afecte el funcionamiento del equipo.	Suspensión del servicio por un mes.
Envíos de falsas alarmas o mensajes que atenten contra la integridad física o moral de las personas.	Suspensión de los servicios por un año en todas las áreas de la Facultad. **Reincidencia.** Cese definitivo de los servicios de cómputo, durante toda su carrera.
Cualquier violación por parte de algún administrador de red, académico u investigador en la política de uso de direcciones IP.	Carta de "extrañamiento" dirigida al Jefe de División o Secretaría.
Violación de las políticas por parte de un académico, investigador, trabajador, en un incidente no grave.	Carta de "extrañamiento" dirigida al Jefe de División o Secretaría.
Utilización de los servicios con fines no acordes a las funciones de su plaza en caso de ser empleado.	Carta de "extrañamiento" dirigida al Jefe de División o Secretaría.
Utilización de los servicios con fines no académicos u de ocio.	Suspensión del servicio por un día. **Reincidencia.** Cancelación de los servicios por un mes en todas las áreas de la Facultad de Ingeniería.

En caso de robo y daño físico de equipo y material de forma intencional, el responsable tendrá que resarcir los daños.

La carta de extrañamiento la podrá realizar el área afectada o el subcomité de administradores de red.

XV. PLAN DE CONTINGENCIAS

Al hablar de políticas de seguridad hay que contemplar tanto la prevención como la recuperación. Sin embargo, ningún sistema es completamente seguro, ya que pese a todas las medidas de seguridad puede ocurrir un desastre. De hecho los expertos en seguridad afirman "sutilmente" que hay que definir un Plan de Contingencias para "cuando falle el sistema", no "por si falla el sistema".

Políticas del Plan de Contingencias:

Todas las áreas deberán contar con un plan de contingencias para sus equipos o servicios críticos de cómputo.

A continuación mencionaremos de manera breve como realizar un plan de contingencias.

Definición de un Plan de Contingencias

Algunas definiciones de Plan de Contingencias.

- "El plan de contingencias es una estrategia constituida por un conjunto de recursos ideados con el propósito de servir de respaldo, contando con una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio efectuados por una paralización total o parcial de la capacidad operativa de la empresa.
- Tal estrategia, puntualizada en un manual, es resultado de todo un proceso de análisis y definiciones que dan lugar a las metodologías. A su vez las metodologías existentes versan sobre el proceso necesario para obtener dicho plan."
- "Un Plan de Contingencia de Seguridad Informática consiste en los pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del sistema aunque, y por lo general, constan de reemplazos de dichos sistemas."

La primera definición menciona que cualquier empresa debe tener una estrategia en caso de una paralización operativa; mientras que la segunda definición es más particular, debido a que se enfoca a la Seguridad Informática, que en nuestro caso es la que nos interesa.

Pero ambas definiciones coinciden que un Plan de Contingencias debe ser capaz de reestablecer el correcto funcionamiento de la empresa o sistema y minimizar los daños.

De acuerdo con lo anterior podemos definir un Plan de Contingencias como:

"Conjunto de procedimientos que permiten recuperar y reestablecer el correcto funcionamiento del sistema en un tiempo mínimo después de que se haya producido el problema; considerando las acciones que se llevarán a cabo antes, durante y después del desastre, para tener el mínimo de pérdidas posibles."

El Plan de Contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento.
Pese a todas las medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible.

Se pueden analizar dos ámbitos: el primero abarca las actividades que se deben realizar y los grupos de trabajo o responsables de operarlas; y el segundo, el control, esto es, las pruebas y verificaciones periódicas de que el Plan de Contingencias está operativo y actualizado.

Fases de un Plan de Contingencia

Fase I. Análisis y Diseño

Estudia la problemática, las necesidades de recursos, las alternativas de respaldo, y se analiza el costo/beneficio de las mismas. Ésta es la fase más importante, pudiendo llegarse al final de la misma incluso a la conclusión de que no es viable o es muy costoso su seguimiento. En la forma de desarrollar esta fase, se diferencian las dos familias metodológicas. Estas son llamadas Risk Analysis y Business Impact.

Las Risk Analysis se basan en el estudio de los posibles riesgos desde el punto de vista de probabilidad de que los mismos sucedan. Aunque los registros de incidentes son escasos y poco fiables, aún así es más fácil encontrar este tipo de metodologías que las segundas.

Las Business Impact, se basan en el estudio del impacto (pérdida económica o de imagen que ocasiona la falta de algún recurso de los que soporta la actividad del negocio). Estas metodologías son más escasas, pero tienen grandes ventajas como es el mejor entendimiento del proceso o el menor empleo de tiempo de trabajo por ir más directamente al problema

Las tareas de esta fase en las distintas metodologías planteadas son las siguientes:

Risk Analysis Business Impact

1. Identificación de amenazas.
2. Análisis de la probabilidad de materialización de la amenaza
3. Selección de amenazas.
4. Identificación de entornos amenazados.
5. Identificación de servicios afectados.
6. Estimación del impacto económico por paralización de cada servicio.
7. Selección de los servicios a cubrir.
8. Selección final del ámbito del plan.
9. Identificación de alternativas para los entornos.
10. Selección de alternativas.
11. Diseño de estrategias de respaldo.
12. Selección de la estrategia de respaldo.
13. Identificación de servicios finales.
14. Análisis del impacto. En estas metodologías se evalúan los daños económicos y de imagen y otros aspectos no económicos.
15. Selección de servicios críticos.
16. Determinación de recursos de soporte.
17. Identificación de alternativas paraentornos.
18. Selección de alternativas.
19. Diseño de estrategias globales de respaldo

20. Selección de la estrategia global de respaldo.

Hay un factor importante a determinar en esta fase que es el Time Frame o tiempo que la organización puede asumir con paralización de la actividad operativa antes de incurrir en pérdidas significativas. Este factor marcará las estrategias de recuperación y se extraerá del análisis del impacto.

Fase II. Desarrollo de un plan.
Esta fase y la tercera son similares en todas las metodologías. En ella se desarrolla la estrategia seleccionada, implantándose hasta el final todas las acciones previstas. Se definen las distintas organizaciones de emergencia y se desarrollan los procedimientos de actuación generando así la documentación del plan.

Es en esta fase cuando se analiza la vuelta a la normalidad, dado que pasar de la situación normal a la alternativa debe concluirse con la reconstrucción de la situación inicial antes de la contingencia.

Fase III. Pruebas y mantenimiento.
En esta fase se definen las pruebas, sus características y sus ciclos, y se realiza la primera prueba como comprobación de todo el trabajo realizado, así como concientizar al personal implicado.

Asimismo se define la estrategia de mantenimiento, la organización destinada a ello, y las normas y procedimientos necesarios para llevarlo a cabo.

Características de un Plan de Contingencias
Un plan de contingencia debería de:

- Tener la aprobación de los integrantes.
- Ser flexible.
- Contener un proceso de mantenimiento.
- Tener un costo efectivo.
- Enfatizar en la continuidad del negocio
- Asignar responsabilidades específicas.
- Incluir un programa de prueba.

Aprobación El plan debe de ser aceptable para auditores internos; fuera de auditores, el director, clientes y proveedores.
Flexibilidad El plan deberá ser especificado en guías, en lugar de relacionar los detalles a situaciones individuales del desastre.
Mantenimiento Eludir detalles innecesarios de manera que el plan pueda ser fácilmente actualizado.
Costo-Efectividad La planeación del proyecto deberá enfatizar en la necesidad de minimizar los costos del desarrollo del plan, respaldo redundante del procesamiento de la suscripción de honorarios, mantenimiento y costo de pruebas.
Continuidad de la empresa. El plan debe de asegurar la continuidad, durante un periodo de recuperación de desastres.

Respuesta organizada. El plan debe proporcionar una lista de verificación de salidas que necesitan atención inmediata que sigue al desastre. Así mismo incluirá listas de números de teléfono y las direcciones de individuos para conectarlos.

Responsabilidad. A individuos específicos deberá asignárseles la responsabilidad de cada salida que requiera atención durante la Respuesta de Emergencia y el tiempo del periodo del procesamiento interno.

Prueba. La prueba con los usuarios para revisar los procedimientos de verificación de respaldo debe de realizar algo específico en los intervalos de tiempo. De tal forma que el plan cuente con un estado de frecuencias de prueba y documente la metodología de prueba.

Características de un buen Plan de Contingencias.

- Funcional.- Desarrollado por los supervisores de primera línea.
- Costo – Efectividad.- En relación con baja probabilidad.
- Flexibilidad.- El mismo plan puede ser utilizado para cualquier desastre.
- Fácil de mantener.- Mantenerlo simple.

Pero no basta con tener un manual cuyo título sea Plan de Contingencia o denominación similar, sino que es imprescindible conocer si funcionará con las garantías necesarias y cubre los requerimientos en un tiempo inferior al fijado y con una duración suficiente. El plan de contingencia inexcusablemente debe:

- Realizar un análisis de Riesgos de Sistemas Críticos que determine la tolerancia de los sistemas.
- Establecer un Periodo Crítico de Recuperación en el cual los procesos deben ser reanudados antes de sufrir pérdidas significativas o irrecuperables.
- Realizar un Análisis de Aplicaciones Críticas por el que se establezcan las prioridades de Proceso.
- Determinar las prioridades de Proceso, por días del año, que indiquen cuáles son las Aplicaciones y Sistemas Críticos en el momento de ocurrir el desastre y el orden de proceso correcto.
- Establecer Objetivos de Recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración de Desastre y el momento en que el Centro Alternativo puede procesar las Aplicaciones Críticas.
- Designar, entre los distintos tipos existentes, un Centro Alternativo de Proceso de Datos.
- Asegurar la Capacidad de Comunicaciones.
- Asegurar la Capacidad de los Servicios de respaldos.

Algunas de las preguntas que pueden formularse al realizar una auditoria sobre este tipo de planes es:

- ¿Cómo está estructurado el Plan?
- ¿Es fácil de seguir el Plan en el caso de un desastre?
- ¿Indica el Plan quién es el responsable de desarrollar tareas específicas?
- ¿Cómo se activa el plan en caso de un desastre?
- ¿Cómo están contenidos estos procedimientos de activación en los procedimientos de emergencia normales de la organización?
- ¿Han sido probados estos procedimientos en un test de desastre simulado?

- ¿Contiene el Plan procedimientos que fijen los daños en las etapas iniciales de las Operaciones de Recuperación?
- ¿Incluye el Plan procedimientos para trasladar el proceso desde el Centro Alternativo al Centro Restaurado o Nuevo?
- ¿Contiene el Plan listados del Inventario del proceso de datos y hardware de comunicaciones, software, formularios preimpresos y stock de papel y accesorios?
- ¿Están actualizados los listados telefónicos del personal de recuperación así como empleados del proceso de datos, alta dirección, usuarios finales, vendedores y proveedores?
- ¿Cómo esta contenido el plan?
- ¿Quién es el responsable de actualizar el Plan?
- ¿Cuándo fue actualizado el plan?
- ¿Hay copias del Plan distribuidas en otro lugar?

En la auditoría es necesario revisar si existe tal plan, si es completo y actualizado, si cubre los diferentes procesos, áreas y plataformas, o bien si existen planes diferentes según entornos, evaluar en todo caso su idoneidad, así como los resultados de las pruebas que se hayan realizado, y si permite garantizar razonablemente que en caso necesario, y a través de los medios alternativos, propios o contratados, podría permitir la reanudación de las operaciones en un tiempo inferior al fijado por los responsables del uso de las aplicaciones, que a veces son también los propietarios de las mismas pero podrían no serlo.

Si las revisiones no aportan garantías suficientes se deben sugerir pruebas complementarias o hacer constar en el informe, incluso indicarlo en el apartado de limitaciones.

Es necesario verificar que la solución adoptada es adecuada: instalaciones propias, ajenas, compartidas, etc. Y que existe el contrato oportuno si hay participación de otras entidades aunque sean del mismo grupo o sector.

Dentro de lo crítico de las aplicaciones se puede distinguir entre las más críticas, con impacto muy alto en el negocio y sin alternativa, otras con alternativas, e incluso diferenciado si con costos altos o inferiores, y aquellas cuya interrupción, al menos en un número de días fijado, no tiene casi incidencia y habrá que distinguir qué tipos de consecuencias e impacto, en función del sector y entidad, y día del mes en que ocurriera el incidente, y tal vez la hora en algunos casos. Frente a lo que venía siendo la previsión de contingencias en estos años pasados, centrándose sólo en el host como un gran servidor, hoy en día, con la clara tendencia a entornos distribuidos, es necesario considerar también estos en la previsión de las contingencias.

Debe existir un manual completo y exhaustivo relacionado con la continuidad en el que se contemplen diferentes tipos de incidencias y a qué nivel se puede decidir que se trata de una contingencia y de qué tipo.

En términos generales, el Plan de Contingencias deberá contener:

- Objetivo del Plan de Contingencias: Se deben indicar aquellos componentes de la función crítica que se pretenden cubrir frente a la contingencia considerada. Estos componentes pueden variar, así como su grado de cobertura para las distintas contingencias analizadas.

- Criterio para la ejecución del Plan de Contingencias: Condiciones bajo las cuales se considera que debe comenzar a aplicarse el Plan de Contingencias.
- Tiempo esperado de duración del Plan de Contingencias: Es el tiempo máximo que se puede continuar operando bajo estas condiciones de contingencia.
- Roles, responsabilidad y autoridad: Esto es clave para la buena marcha del Plan de Contingencias. Se debe determinar muy claramente, cuál es el papel de cada uno de los sectores de la organización ante la contingencia y cómo se alteran los procedimientos habituales para dar lugar a los procedimientos de contingencia.
- Requerimientos de recursos: Qué recursos se necesitan para operar en el modo contingencia y cuáles de los recursos habitualmente utilizados no se deben utilizar. Esto debe estar debidamente documentado y verificado lo más exhaustivamente posible.
- Capacitación: Otro aspecto importante es la capacitación al personal que debe intervenir en la contingencia, cuando ésta se presente. Es necesario que el personal involucrado sepa cómo se saca de servicio cualquier componente que, según el Plan de Contingencias, no debe seguir operando ante alguna falla; que pueda darse cuenta de qué debe hacer y que esté en capacidad de hacerlo cuando sea preciso. También debe tenerse en cuenta que en algún momento habrá que volver a la operación habitual; por lo tanto deberán incluirse en el plan de mecanismos para volver a la operatoria anterior a la contingencia y el tiempo máximo que la función puede permanecer en estado de contingencia.
- Implementación y Operación de los Planes de Contingencia: Se desea que no haya que implementar los Planes de Contingencia, sin embargo, por si esto sucede, hay que estar preparado y tener instructivos claros para todas las tareas que deberían realizarse.
- Reinstalación: La contingencia como su nombre lo indica, no es una situación permanente. Por lo tanto, se deben prever mecanismos como para recuperar los datos de operación durante la contingencia, si es que son necesarios, y para aplicar las instrucciones necesarias para que las operaciones no sufran una interrupción traumática al terminar el periodo de contingencia.

XVI. ÉTICA INFORMÁTICA

La ética se define como: “principios directivos que orientan a las personas en cuanto a la concepción de la vida, el hombre, los juicios, los hechos, y la moral.”

Es conveniente diferenciar la ética de la moral, la ética es una disciplina filosófica, la cual tiene como objeto de estudio la moral, esto no quiere decir que la ética crea la moral, sino solamente reflexiona sobre ella.

“La moral se refiere a la conducta del hombre que obedece a unos criterios valorativos acerca del bien y el mal, mientras que la ética reflexiona acerca de tales criterios, así como de todo lo referente a la moralidad.”

Otro concepto importante es el de valor, este no lo poseen los objetos por si mismo, sino que estos lo adquieren gracias a su relación con el hombre como ser social.

Definiciones de la Ética Informática

La Ética de la Informática (EI) es una nueva disciplina que pretende abrirse campo dentro de las éticas aplicadas. El origen remoto de la EI está en la introducción masiva de las computadoras en muchos ámbitos de nuestra vida social. Muchas profesiones reivindican para sí una ética particular con la cual pueden regirse ante los problemas morales específicos de esa profesión o actividad ocupacional. La existencia de la EI tiene como punto de partida el hecho de que las computadoras suponen unos problemas éticos particulares y por tanto distintos a otras tecnologías. En la profesión informática se quiere pasar de la simple aplicación de criterios éticos generales a la elaboración de una ética propia de la profesión. Los códigos éticos de asociaciones profesionales y de empresas de informática van en esta dirección.

La definición más restrictiva de la EI es considerarla como la disciplina que analiza problemas éticos que son creados por la tecnología de las computadoras o también los que son transformados o agravados por la misma, es decir, por las personas que utilizan los avances de las tecnologías de la información. Algunos de los autores se plantean si la cambiante sofisticación tecnológica plantea nuevos dilemas éticos o si las cuestiones éticas permanecen constantes.

Otras definiciones de la EI son mucho más amplias. No se reducen a un nuevo campo de ética aplicada sino que, por ejemplo, en el libro de James Moor, la EI es el análisis de la naturaleza y el impacto social de la tecnología informática y la correspondiente formulación y justificación de políticas para un uso ético de dicha tecnología. La EI estaría relacionada con los problemas conceptuales y los vacíos en las regulaciones que ha ocasionado la tecnología de la información. El problema es que hay una falta de reglamentación en cómo utilizar estas nuevas tecnologías que posibilitan nuevas actividades para las cuales no hay o no se perciben con nitidez principios de actuación claros. Las personas con responsabilidades en el área de diseño o gestión de sistemas de información cada vez han de tomar más decisiones sobre problemas que no se resuelven con lo legal y lo cuasi-legal (reglamentos, manuales de procedimiento de las empresas, etc.) sino que rozan lo ético mismo. La tarea de la EI es aportar guías de actuación cuando no hay reglamentación o cuando la existente es obsoleta. Al vacío de políticas se añade generalmente un problema de vacío conceptual. Por ello la EI también ha de analizar y proponer una marco conceptual que sea adecuado para entender los dilemas éticos que ocasiona la informática.

Otra definición más general viene de Terrel Bynum, que basándose en Moor, define la EI como la disciplina que identifica y analiza los impactos de las tecnologías de la información en los valores humanos y sociales. Estos valores afectados son la salud, la riqueza, el trabajo, la libertad, la democracia, el conocimiento, la privacidad, la seguridad o la autorrealización personal. En este concepto de EI se quieren incluir términos, teorías y métodos de disciplinas como la ética aplicada, la sociología de las computadoras, la evaluación social de las tecnologías o el derecho informático.

Códigos Deontológicos en Informática

La Deontología (Del Griego Deón (deber) y Logos (razonamiento o ciencia): Ciencia del Deber), es la disciplina que trata lo concerniente a los deberes que corresponden a ciertas situaciones personales y sociales.

Originada en las profesiones intelectuales de antiguo origen histórico (Derecho, Medicina) la Deontología, en particular, denota el conjunto de reglas y principios que rigen determinadas conductas de los profesionales, ejercidas o vinculadas, de cualquier manera, al ejercicio de la profesión y a la pertenencia al respectivo grupo profesional.

Las asociaciones de profesionales de informática y algunas empresas relacionadas con la informática han desarrollado códigos de conducta profesional. Estos códigos tienen distintas funciones:

- Existan normas éticas para una profesión, esto quiere decir que un profesional, en este caso un técnico, no es sólo responsable de los aspectos técnicos del producto, sino también de las consecuencias económicas, sociológicas y culturales del mismo.
- Sirven como un instrumento flexible, como suplemento a las medidas legales y políticas, ya que éstas en general van muy lentas comparadas con la velocidad del desarrollo de las tecnologías de la información. Los códigos hacen de la ley su suplemento y sirven de ayuda a los cuerpos legislativos, administrativos y judiciales.
- Sirven como concientización pública, ya que crear unas normas así, hace al público consciente de los problemas y estimula un debate para designar responsabilidades.
- Estas normas tienen una función sociológica, ya que dan una identidad a los informáticos como grupo que piensa de una determinada manera; es símbolo de sus estatus profesional y parte de su definición como profesionales.
- Estas normas sirven también como fuente de evaluación pública de una profesión y son una llamada a la responsabilidad que permiten que la sociedad sepa qué pasa en esa profesión; aumenta la reputación del profesional y la confianza del público.
- En las organizaciones internacionales, estas normas permiten armonizar legislaciones o criterios divergentes existentes (o ausentes, en su caso) en los países individuales.

Los códigos son un paso en la concientización de las sociedades y organizaciones que quieren mejorar situaciones en las que los impactos sociales del desarrollo tecnológico no se tienen en cuenta. No tienen que duplicar lo que ya existe en la ley. La ley trata de la legalidad de las prácticas sociales, es normativa por definición y se impone con sanciones. Los códigos, en cambio, tratan del comportamiento según principios éticos, su normatividad es mostrar una declaración de intenciones sobre la "misión" de una institución y la coerción real con que se imponen es pequeña, aunque en algunos casos se incluyen expulsiones de la asociación en cuestión. La ley es el acercamiento de más poder normativo y asigna con claridad los derechos, responsabilidades y deberes de cada uno.

Un Código de ética se suma a un cambio de actitud por parte de la sociedad, respetando el accionar de la misma.

Situación actual de la Ética de la Informática

- La literatura existente es más sociológica que ética; es menos prescriptiva o normativa que descriptiva. En general no se ofrecen principios de actuación o respuestas a las preguntas "debe" (qué debería hacer yo como persona, que debería hacer yo y los míos como organización, qué normas sociales deberíamos promover, que leyes debemos tener...). El objetivo de la EI no es solamente proponer análisis sobre "sociología de la informática" o sobre la evaluación social de las tecnologías (technology assessment), sino ir algo más allá en el sentido de proporcionar medios racionales para tomar decisiones en temas en los que hay en juego valores humanos y dilemas éticos.

XVII. CÓDIGOS DE ÉTICA

En México, existen algunos códigos de ética sobre todo en el ámbito periodístico, en el derecho y la medicina. Sin embargo, hay instituciones educativas y empresas que se preocupan por tener un código de ética; en cuanto a seguridad informática son muy pocos, es por eso que propondremos una código de ética para la Facultad de Ingeniería.

Algunos de los códigos de ética que hacen referencia a la seguridad informática o a la informática, son los siguientes:

- Código de Ética del Ingeniero Mexicano (UMAI)
- Código de Ética de la IEEE
- American Society for Industrial Security (ASIS)
- Código de Ética de la Asociación Mexicana de la Industria Publicitaria y Comercial en Internet, A. C. (AMIPCI)

Se anexa el código de ética universitario, como una muestra de que la UNAM se preocupa porque la gente que labora en ella esté comprometida a realizar su trabajo apegada a los principios establecidos en este código de ética.
Para el personal involucrado en los áreas de sistemas informáticos seguirán el
CÓDIGO DE ÉTICA UNIVERSITARIO y el CÓDIGO DE ÉTICA PARA LA FACULTAD DE INGENIERIA EN EL ÁMBITO INFORMÁTICO.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

CÓDIGO DE ÉTICA UNIVERSITARIO

*** A LA COMUNIDAD UNIVERSITARIA**

Considerando que la Universidad Nacional Autónoma de México, como organismo descentralizado del estado, está comprometida con una responsabilidad moral y ética en el sentido de actuar de acuerdo a normas y principios que rijan la conducta del buen vivir de su comunidad.

Que esa responsabilidad ética obliga a una continua evaluación del comportamiento social y público de sus funcionarios y empleados, a fin de garantizar en todo momento el respeto al derecho y la observancia de su Normatividad evitando con ello faltas a las normas éticas que pongan en riesgo la estabilidad de la institución.

Que para fortalecer la confianza de la comunidad universitaria, así como la del pueblo de México, es preciso adoptar medidas tendientes a reforzar la grandeza de la institución, haciéndolos sentir parte importante de la misma, además de propiciar que sus labores no vulneren los principios de una ética institucional.

Se emite el presente Código de Ética para los funcionarios y empleados universitarios cuya implementación, es de trascendental importancia para esta Universidad.

*** ALCANCE Y OBJETIVO DEL CÓDIGO**

Reglamentar la conducta de los funcionarios y empleados universitarios y, en general, a toda persona que desempeñe un empleo, cargo o comisión de cualquier naturaleza en la administración universitaria.

*** PRINCIPIOS FUNDAMENTALES**

I. Todo funcionario y empleado universitario considerará un deber, desempeñar su trabajo en apego a este Código de Ética.

II. Todo funcionario y empleado universitario, para apoyar y promover el honor y la dignidad de la institución con las normas más elevadas de la ética deberá:

- Interesarse en el bienestar común y aplicar sus conocimientos profesionales para beneficio de la institución así como de sus integrantes.
- Desarrollar sus deberes con honestidad e imparcialidad y servir con dedicación a sus superiores, sus empleados y a la comunidad universitaria general.
- Reconocer que la trayectoria universitaria es el origen de una disponibilidad económica que debe permitir vivir con decoro, procurando asegurar para los suyos los recursos materiales y los elementos morales que le sean indispensables para su progreso y bienestar.
- Esforzarse por aumentar la competencia y prestigio de los trabajadores y empleados universitarios en todas sus actividades.

POSTULADOS

I. Responsabilidad hacia la sociedad en general

Bien común: Asumo un compromiso irrenunciable con el bien común, entendiendo que la Universidad es patrimonio de la Nación, que sólo se justifica y legitima cuando se procura ese bien común, por encima de los intereses particulares.

Imparcialidad: Actuaré siempre en forma imparcial, sin conceder preferencias o privilegios indebidos a persona alguna.

Vocación de Servicio: Entiendo y acepto que trabajar para esta Universidad constituye al mismo tiempo el privilegio y el compromiso de servir a la sociedad, porque es ella quien contribuye a pagar mi salario.

Liderazgo: Promoveré y apoyaré estos compromisos con mi ejemplo personal, abonando a los principios morales que son base y sustento de una sociedad exitosa en institución ordenada y generosa.

Dignidad con la sociedad: Respetaré en el debate y en la toma de decisiones, la dignidad de las personas, siendo justo, veraz y preciso en mis apreciaciones, reconociendo la legítima diversidad de opiniones.

II. Responsabilidad hacia la comunidad universitaria

Honradez: Nunca usaré mi cargo para ganancia personal, ni aceptaré prestación o compensación alguna a mis remuneraciones a las que tengo derecho, de ninguna persona u organización que me pueda llevar a actuar con falta de ética mis responsabilidades y obligaciones.

Justicia: Ceñiré mis actos a la estricta observancia de la Normatividad Universitaria, impulsando una cultura de procuración efectiva de justicia y de respeto a la Institución.

Transparencia: Acepto demostrar en todo tiempo y con claridad suficiente, que mis acciones como funcionario y empleado universitario se realizan con estricto y permanente apego a las normas y principios de la Institución, fomentando su manejo responsable y eliminando su indebida discrecionalidad.

Rendición de cuentas: Proveeré la eficacia y la calidad en la gestión de la administración universitaria, contribuyendo a su mejora continua y a su modernización, teniendo como principios fundamentales la optimización de sus recursos y la rendición de cuentas.

Respeto: Respetaré sin excepción alguna la dignidad de la persona humana y los derechos y libertades que le son inherentes, siempre con trato amable y tolerancia para toda la comunidad universitaria.

Lealtad: Afirmo que todos mis actos se guían e inspiran por exaltar a la institución y a sus símbolos; así como el respeto a su Ley Orgánica y demás Normatividad que de ella emana y por la más firme creencia en la dignidad de la persona humana.

Responsabilidad: Acepto estar preparado para responder de todos mis actos de manera que la comunidad universitaria y la gente con que trato en particular, aumenten permanentemente su confianza en mí y en nuestra capacidad de servirles.

Competencia: Reconozco mi deber de ser competente, es decir, tener y demostrar los conocimientos y actitudes requeridos para el ejercicio eficiente de las funciones que desempeño, y actualizarlos permanentemente para aplicarlos al máximo de mi inteligencia y de mis esfuerzo.

Efectividad y Eficiencia: Comprometo la aplicación de mis conocimientos y experiencias de la mejor manera posible, para lograr que los fines y propósitos de la Universidad se cumplan con óptima calidad y en forma oportuna.

Manejo de recursos: todos los recursos propiedad de la Universidad sin importar su origen, los aplicaré únicamente para la consecución de los objetivos institucionales.

Calidad del personal: Contrataré para los cargos de mi dependencia, sólo a quienes reúnan el perfil para desempeñarse con rectitud, aptitud y la actitud necesarios.

III. Responsabilidad hacia los compañeros de trabajo

Valor civil: Reconozco mi compromiso de ser solidario con mis compañeros y conciudadanos; pero admito mi deber de denunciar y no hacerme cómplice de todo aquel que contravenga los principios éticos y morales contenidos en este instrumento.

Igualdad: Haré regla invariable de mis actos y decisiones el procurar igualdad de oportunidades para todos los universitarios, sin distingo de sexo, edad, raza, credo, religión o preferencia política.

Probidad: Declaro que todos los recursos y fondos, documentos, bienes y cualquier otro material confiado a mi manejo o custodia debo tratarlos con absoluta probidad para conseguir el beneficio colectivo.

Diálogo: Privilegiaré el diálogo y la concertación en la resolución de conflictos.

CÓDIGO DE ÉTICA PARA LA FACULTAD DE INGENIERIA EN EL ÁMBITO INFORMATICO.

1. Aplicación del código

El presente código de ética establece algunos puntos que regularán la conducta y el desempeño profesional de las personas encargadas de la seguridad informática de la Facultad de Ingeniería, a las cuales definiremos como Administradores de red (y de sistemas), independientemente del sistema operativo que utilicen; incluyendo a las personas que laboran en cualquier área de sistemas, sin importar el puesto que ocupen.

2. Actitud profesional

La excelencia técnica y ética de los administradores de red se vuelve indispensable para todos los profesionales de esta área, por lo que es necesario que ellos promuevan la difusión y práctica de los principios expresados en este código.

Los Administradores de red tienen la obligación de regir su conducta de acuerdo a las reglas contenidas en este código, las cuales deben considerarse mínimas pues se reconoce la existencia de otras normas de carácter legal y moral que amplían el de las presentes.

Este código rige la conducta de los Administradores de Red, así como el de las personas que pertenecen a cualquier área de sistemas, en sus relaciones con el público en general, con quien presta sus servicios (usuarios) y con sus compañeros de trabajo.

Los Administradores de red y las personas que trabajan en el área de sistemas, deben abstenerse de hacer comentarios sobre sus compañeros de trabajo o usuarios, que perjudiquen su reputación o el prestigio de su profesión, a menos que se soliciten por quién tenga un interés legítimo de ellos.

3. Actitud personal

Los Administradores de red y las personas que trabajan en el área de sistemas deben respeto a toda persona y su comportamiento tanto en lo personal como en lo social, debe atender a la práctica de buenas costumbres y seguir un objetivo útil.

Los Administradores de red y las personas que trabajan en el área de sistemas deben tener la costumbre de cumplir los compromisos adquiridos, no por el hecho de estar escritos, sino por convicción propia.

Los Administradores de red y las personas que trabajan en el área de sistemas deben de respetar y hacer respetar su tiempo y el de los demás, predicar con el ejemplo, poseer espíritu de servicio y habilidad para comunicarse con los demás.

Los Administradores de red y las personas que trabajan en el área de sistemas siempre actuarán cuidando el no afectar la integridad física, emocional ni económica de las personas.

4. Calidad profesional en el trabajo

Los Administradores de red y las personas que trabajan en el área de sistemas, deben realizar un trabajo de calidad en cualquier servicio que ofrezcan.

5. Preparación y calidad profesional

Por ser la información un recurso difícil de manejar, se requiere de Administradores de definan estrategias para su generación, administración y difusión; por lo que ninguna persona que no esté relacionada con la informática, computación o sistemas computacionales, que no cuente con experiencia y con la capacidad necesaria para realizar éstas actividades de manera satisfactoria y profesional, por ningún motivo podrá llevar a cabo esta actividad.

Los Administradores de red y las personas que trabajan en el área de sistemas, se preocuparán de que su propia actualización y capacitación profesional sea de crecimiento permanente.

6. Práctica de la profesión

Los Administradores de red y las personas que trabajan en el área de sistemas, deben analizar cuidadosamente las verdaderas necesidades que puedan tenerse de sus servicios, para proponer aquellas que más convengan dependiendo de las circunstancias.

Responsabilidades hacia el usuario

1. Importancia del usuario

El principal objetivo de los Administradores de la red y las personas que trabajan en el área de sistemas es la atención adecuada al usuario, al cual se le debe brindar todo el respeto .

2. Proteger el interés del usuario

Los Administradores de red y las personas que trabajan en el área de sistemas, deben aprovechar las herramientas (software, equipo de cómputo) adquiridas por la Facultad para el beneficio no sólo de ella sino también de los usuarios.

Los Administradores de Red deben asegurarse del buen uso de los recursos informáticos, evitando el mal uso para el que no fueron planeados y autorizados.

3. Responsabilidad profesional

Los Administradores de red y las personas que trabajan en el área de sistemas expresarán su opinión en los asuntos que se les hayan encomendado, teniendo en cuenta los principios expresados en éste código.

Deberán ser objetivos, imparciales en la emisión de sus opiniones o juicios, buscando siempre el beneficio de la institución de sus compañeros y usuarios.

4. Acceso a la información

Los Administradores de red y las personas que trabajan en el área de sistemas respetarán la información de carácter privado relativa a las personas, contenida en las bases de datos, excepto cuando se requiera una investigación por un incidente de seguridad o una investigación de carácter legal.

5.- Discreción profesional

Los Administradores de red y las personas que trabajan en el área de sistemas tienen la obligación de guardar discreción en el manejo de la información que se les ha proporcionado para poder prestar sus servicios. Considerar como confidencial toda la información que le ha sido confiada.

Los Administradores de red y las personas que trabajan en el área de sistemas no deben permitir el acceso a la información a personal no autorizado, ni utilizar para beneficio propio la información confidencial de los usuarios.

6.- Honestidad profesional.

Los Administradores de red y las personas que trabajan en el área de sistemas, no podrán modificar o alterar la información que se les ha confiado, para beneficio propio o de terceros, ni con fines de encubrir anomalías que afecten directamente los intereses de la Institución.

Los Administradores de red y las personas que trabajan en el área de sistemas no deben participar en actos que se califiquen de deshonestos.

7. No usar equipo de cómputo ni programas de la Institución para beneficio personal

Los Administradores de red y las personas que trabajan en el área de sistemas no deben usar el equipo de cómputo para fines de esparcimiento que afecten su desempeño profesional, aún cuando tenga la autorización para utilizar el equipo. Ni fomentar que personas ajenas a la Institución ingresen a las instalaciones y utilicen el equipo y los programas del software.

8. Trato adecuado a los usuarios y compañeros de trabajo

Los Administradores de red y las personas que trabajan en el área de sistemas deben tratar con respeto a todas las personas sin tener en cuenta raza, religión, sexo, orientación sexual, edad o nacionalidad.

Los directivos de las áreas de sistemas debe dar a sus colaboradores el trato que les corresponde como profesionales y vigilarán su adecuada superación profesional.

9. Finalización del trabajo

Al finalizar un proyecto independientemente del área de la que lo solicite, debe cumplir con todos los requisitos de funcionalidad, calidad y documentación pactados inicialmente, a fin de que se pueda obtener el mayor beneficio en la utilización de los mismos.

Los Administradores de red y las personas que trabajan en el área de sistemas deben cuidar que el equipo de cómputo y los programas propiedad de la Unidad se conserven en buen estado para su uso y aprovechamiento.

Al concluir el trabajo para el cual fue contratado, Los Administradores de red y las personas encargadas del desarrollo de sistemas en la Institución deben implementar los mecanismos necesarios, para que tenga la posibilidad de continuar haciendo uso de los programas de aplicación, así como de modificarlos, a pesar de su ausencia.

10. Desarrollo de sistemas

Las personas encargadas del desarrollo de sistemas en Institución deben determinar perfectamente el alcance del sistema y los requerimientos necesarios para su desarrollo.

Las personas encargadas del desarrollo de sistemas en la Institución deben determinar de manera clara la entrega de las diferentes etapas de desarrollo y establecer las fechas y compromisos formales de entrega, de cada una de las personas que participen en el desarrollo del sistema.

Las personas encargadas del desarrollo de sistemas en la Institución deben llevar a cabo las evaluaciones en las fechas determinadas y entregar los resultados en un tiempo adecuado que permita tomar decisiones.

Las personas encargadas del desarrollo de sistemas en la Institución deben dejar siempre documentado el sistema desarrollado, con todos los detalles necesarios, de tal manera que con su consulta se conozca el funcionamiento del sistema.

Las personas encargadas del desarrollo de sistemas en la Institución deben tener la capacidad para reconocer sus fallas en las revisiones, hacer correcciones y aclarar las dudas de quien solicito el sistema, así como proponer posibles alternativas de solución.

Las personas encargadas del desarrollo de sistemas en la Institución deben comunicar los problemas que se les vayan presentando.

RESPONSABILIDAD HACIA LA PROFESIÓN

1. Respeto a sus compañeros de trabajo y a su profesión

Los Administradores de red y las personas que trabajan en el área de sistemas cuidarán las relaciones que sostienen con sus compañeros de trabajo y colegas, buscando mejorar el ambiente de trabajo y fomentar el trabajo en equipo.

Los Administradores de red y las personas que trabajan en el área de sistemas deberán basar su reputación en la honestidad, honradez, lealtad, respeto, laboriosidad y capacidad profesional, observando las reglas de ética más elevadas en sus actos y evitando toda publicidad con fines de lucro o auto elogio.

Buscarán la manera de hacer cumplir y respetar este código de ética; además de fomentar la adopción de un código de ética.

2. Difusión y enseñanza de conocimientos

Los Administradores de red y las personas que trabajan en el área de sistemas deben mantener altas normas profesionales y de conducta, especialmente al transmitir sus conocimientos, logrando contribuir al desarrollo y difusión de los conocimientos de su profesión.

3. Especialización profesional de los Administradores del Sistema

Los Administradores de red y las personas que trabajan en el área de sistemas deben tener una orientación hacia cierta rama de la informática, computación o sistemas computacionales, debiéndose mantener a la vanguardia en el área de conocimiento de su interés.

4. Competencia profesional

Los Administradores de red y las personas que trabajan en el área de sistemas mantener actualizados todos los conocimientos inherentes a las áreas de su profesión así como participar en la difusión de éstos conocimientos a otros miembros de la profesión.

Los Administradores de red y las personas que trabajan en el área de sistemas deben informarse permanentemente sobre los avances de la informática, la computación y los sistemas computacionales.

5. Evaluación de capacidades

Los Administradores de red y las personas que laboran en sistemas en la Institución deben autoevaluarse periódicamente con la finalidad de determinar si cuentan con los conocimientos suficientes para ofrecer un trabajo de calidad.

En caso de que los Administradores de red y las personas que laboran sistemas en la Institución tengan personas a su cargo deberán asegurarse de que sean evaluados sus conocimientos periódicamente.

6. Personal a sus servicios

Los Administradores de los Sistemas y las personas encargadas del desarrollo de sistemas en la Institución deben realizar una supervisión del desempeño de las personas que colaboran con ellos en el desarrollo de sistemas.

7. Práctica docente

Los Administradores de red o instructores y las personas que pertenecen a Institución que den clases en la Facultad de Ingeniería o que den cursos deben cumplir con su responsabilidad en asistencia y puntualidad en el salón de clases.

Evaluaciones a los alumnos

Los Administradores de red o instructores y las personas que pertenecen a Institución que den clases en la Facultad de Ingeniería o que den cursos deben comunicar los procedimientos de evaluación durante el tiempo que dure la enseñanza.
Los Administradores de red o instructores y las personas que pertenecen a Institución que den clases en la Facultad de Ingeniería o que den cursos deben llevar a cabo las evaluaciones en las fechas determinadas y entregar los resultados en un tiempo adecuado, así como también hacer una revisión total del examen y aclarar todas las dudas que resulten derivadas de su aplicación.
Los Administradores de red o instructores y las personas que pertenecen a Institución que den clases en la Facultad de Ingeniería o que den cursos llevar una supervisión del desempeño del alumno en forma personal preocupándose por establecer si los bajos resultados son resultado del desempeño del alumno o del profesor o instructor.

XVIII. GLOSARIO

Sitio

Cualquier organización (militar, gubernamental, comercial, académica, etc.) que posea recursos relativos a redes y computadoras.

Usuario

Cualquier persona que hace uso de alguno de los recursos de cómputo con los que cuenta una organización.

Administrador

El responsable de mantener en operación continua los recursos de cómputo con los que cuenta un sitio

Seguridad en cómputo

Un conjunto de recursos destinados a lograr que los activos de una organización sean confidenciales, íntegros, consistentes y disponibles a sus usuarios, autentificados por mecanismos de control de acceso y sujetos a auditoría.

- Confidencial: La información debe ser leída por su propietario o por alguien explícitamente autorizado para hacerlo.
- Íntegro: La información no debe ser borrada ni modificada por alguien que carezca de autorización para hacerlo.
- Consistente: el sistema, al igual que los datos, debe comportarse como uno espera que lo haga.
- Disponible: La información debe estar siempre disponible en el lugar y cantidad de tiempo requeridos.
- Autentificado: Únicamente deben ingresar al sistema personas autorizadas, siempre y cuando comprueben que son usuarios legítimos.
- Control de acceso: Debe conocerse en todo momento quién entra al sistema y de dónde procede.
- Auditoría: Deben conocerse en cada momento las actividades de los usuarios dentro del sistema.

Incidente

Un evento que pone en riesgo la seguridad de un sistema de cómputo.

Ataque

Un incidente cuyo objetivo es causar daño a un sistema, robar información del mismo, o utilizar sus recursos de forma no autorizada.

Firewall

Un dispositivo de hardware y software que actúa como una barrera protectora entre una red privada y el mundo exterior; se usa para proteger el acceso a los recursos internos desde el exterior, así como para controlar los recursos externos que son accedidos desde la red privada.

Herramientas de seguridad

Programas que nos permiten incrementar la fiabilidad de un sistema de cómputo. Existe una gran variedad de ellas, casi todas de libre distribución. Algunos ejemplos de herramientas de seguridad a considerar para implementar un esquema de seguridad son:

- Para el manejo de contraseñas: anipasswd, passwd+, crack, John The Ripper, S/Key
- Para el manejo de autenticación: Kerberos, SecureRPC
- Para el monitoreo de redes: Satan, ISS
- Para auditoría interna: COPS, Tiger, Tripwire
- Para control de acceso: TCP-Wrapper, PortSentry

SPAM

Mensaje de correo electrónico no solicitado por el receptor, usualmente distribuido a una lista de direcciones y cuyo contenido generalmente es publicidad de productos o servicios.

DHCP

DHCP (Dinamic Host Configuration Protocol) es una extensión del protocolo BOOTP (BOOTP habilita a clientes disskless a inicializar y automáticamente configurar TCP/IP). DHCP centraliza y administra la información de la configuración de TCP/IP, automáticamente asigna direcciones IP a las computadoras configuradas para utilizar DHCP.

SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

IDS es la abreviatura de Sistema de Detección de Intrusos(por sus siglas en inglés), que es el arte de detectar actividad inapropiada, incorrecta o anónima. Los sistemas de Detección de Intrusos que operan en un host para detectar actividad maliciosa se les conoce como Sistemas de Detección de Intrusos para host y los sistemas DI que operan en el flujo de datos de una red se les conoce como sistemas de Detección de Intrusos.