Universidad Nacional Autónoma de México

Facultad de Ingeniería

Apéndice 1

Entrevista a los encargados de la seguridad y las redes de la Facultad de Ingeniería

14 de octubre del 2009 a las 13:00 hrs

Ing. Rafael Sandoval Vázquez
Jefe del departamento de seguridad en cómputo

¿Existe documentos previos a las Políticas de Seguridad en Cómputo (PSC)?

De manera oficial no, (No se conoce ninguna). En ese tiempo no existían lineamientos o un procedimiento, todo se resolvía como se podía y los casos críticos se transferían a DGSCA.

¿Por qué se decidió realizar un nuevo documento?

Existían necesidades importantes que cubrir en materia de seguridad informática, los problemas que existían hacían que la productividad menguara, había contaminación en las redes lo cual hacia que colapsaran y se colapsaran. Otro de los problemas que se tenían era la violación a la propiedad intelectual y el uso de programa peer-to-peer (p2p).

Además de estos problemas, el tráfico en las redes se acrecentaba por la infección en los equipos de cómputo contaminados por gusanos, por esto DGSCA se veía en la necesidad de bloquear y sacar de la red a un sin número de subredes.

¿Quiénes fueron los responsables de actualizar?

El Comité Asesor de Cómputo de la Facultad de Ingeniería, (CACFI)

¿Con la realización de este trabajo hubo alguna tesis u otro documento que dio como fruto las PSC y cual fue este?

Sí, se realizo un trabajo de tesis el cual lleva por título:

"Estrategias, procedimientos y políticas para implementar la seguridad informática en organizaciones con sistemas Linux red hat caso: unidad de servicios de cómputo académico de la Facultad de Ingeniería"[26]

¿Quién es el responsable directo de la autorización de las PSC?

[26] Roberto Carlos Zúñiga Ramírez y Yesenia Carrera Fournier, 2003

Es el comité ejecutivo de la Facultad de Ingeniería (el director de la FI)
¿Existe alguna organización con respecto a las PSC, es decir un autor, autorizador, custodio, ejecutor, supervisor y quienes serian?

Sí, el comité ejecutivo, el comité asesor de cómputo (CACFI) y el personal operativo son los encargados de realizar estas funciones.

¿Quiénes son los encargados de hacerlas respetar?

Los encargados de hacer respetar las PSC-FI, son los responsables de cada área los cuales a pueden contar con políticas internas en cada área.

¿Existe hoy en día algún tipo de documento, estándar, o norma que se considere como una guía para la revisión y actualización?

Sí, serían la ISO 27001 y la ISM3 en su apartado de procedimientos y políticas.

Respuesta a incidentes

¿Existe algún formato de reporte sobre incidentes de seguridad?

Sí existe un formato.

¿Existe algún procedimiento que existe en caso de un incidente?

El procedimiento de respuesta a incidentes varía dependiendo del área, algunos de ellas cuentan con personal para hacer frente a este, por lo cual solo se les notifica que existe un incidente y ellos lo resuelven, sin embargo en el caso de un incidente grave o de alto impacto este se transfiere al CACFI.

En el caso de que el área solicite ayuda, asesoría o que el incidente sea atendido el Departamento de Seguridad en Cómputo (DSC), cuenta con el personal para hacer frente al incidente ya que cuenta con personal calificado. De la misma forma en caso de que alguna área requiera asesoría, la realización de una auditoria el DSC ofrece estos servicios en caso de que el jefe o responsable los solicite.

¿Cómo es que se detectan los incidentes de seguridad y quién es el encargado o responsable?

Los incidentes pueden ser detectados de dos fuentes principales las cuales son los sistemas, firewalls y otras herramientas implementadas para el monitoreo de la misma Facultad de Ingeniería o por parte de DGSCA, estos reportes llegan al DSC y se notifica o reporta al jefe de la división o al responsable.

¿Existe un mail para enviar dichos reportes o contactar a los encargados de la seguridad?

Sí, seguridad@seguridad.fi-a.unam.mx y seguridad@unica.unam.mx

¿Existe algún procedimiento después del incidente?

Sí, existe un seguimiento después del incidente.

¿Existe de una página para la ayuda de usuarios de la FI, donde haya artículos y ayuda?

En este momento no hay, pero se ha estado trabajando para crear un portal donde habrá manuales, tutoriales y ligas a herramientas.

Escaneo

¿Es necesario un apartado para incluir el análisis de vulnerabilidades (escaneo)?

Las políticas actuales mencionan algo acerca de monitoreo que se considera en parte también como el análisis de vulnerabilidades, sin embargo tal cual no se encuentra pero sería bueno incluir esto en las políticas.

Es importante el no manejar el término escaneo o "sniffeo" ya que es un término ilícito y usar el término de análisis de vulnerabilidades ya que las palabras escaneo y "sniffeo" están asociadas a actividades ilícitas.

Redes inalámbricas

Las redes inalámbricas no están consideradas dentro de las políticas de la FI, que considera ¿qué es necesario realizar dentro de este marco?

Las redes inalámbricas han crecido sin orden, y se está trabajando para realizar un proceso de administración, control y ordenamiento de las mismas. Se realizo un trabajo de tesis acerca de este tema el cual contiene un análisis sobre este tema.[27]

Respecto a las políticas, claro que se requiere que estas contengan políticas que ayuden a la gestión, ordenamiento y que contengan buenas prácticas acerca de estas.

Auditorias

¿Qué procedimientos hay para la realización de una auditoria?

No existe un procedimiento establecido, y las que se llegan a realizar son cuando el administrador o responsable las requiere o existe un incidente grave.

Cuando se llega a presentar un incidente grave o se compromete un sistema se pueden realizar revisiones, auditorias y análisis forenses ya que en el DSCFI se tiene el personal capacitado para realizar estas tareas cuando son requeridas por administradores o responsables o cuando se tiene que responder ante un incidente.

Sanciones

¿Qué es una carta de extrañamiento?

Una carta de extrañamiento es un acta administrativa o reporte permanente en el expediente de la persona, dicha carta o sanción es hecha directamente por el jefe inmediato.

[27] Guerrero Martínez Edson Armando, Gestión de redes inalámbricas en la Facultad de Ingeniería.

¿Quién es el administrador general?

Es un término que se usaba en el tiempo que se realizaron las PSC, y se refería al administrador o responsable de cómputo por cada división.

¿Quién es el administrador general de la división?

Los responsables de cada división pertenecen al CACFI sus nombres salieron en la gaceta número 9. Es importante agregar que se tenga en cuenta que el responsable ante DGSCA es el Ing. Noé Cruz.

Políticas

¿Qué estándares se usan o deberían usarse para las PSI?

ISO 27001

¿Actualmente existe un plan de contingencias? Y ¿en dónde se pude consultar?

No se publican pero debe existe es confidencial.

¿Qué tipo de incidentes se presentan más en la FI?

1.- Malware (troyanos, bots, gusanos y virus)
2.- Spam
3.- Infracciones o violaciones a la propiedad intelectual
4.- otros

Y los porcentajes no se pueden publicar son confidenciales.

¿Se han tomado medidas al respecto de la seguridad?

Sí, se ha implementado un sistema de seguridad perimetral y otros sistemas que han resultado en la disminución de un 80% de incidentes.

Para una mejor difusión de las PSI ¿Cuáles serian sus sugerencias?

Hacer campañas constantes, promover un día de las PSI, conferencias o platicas informativas acerca de la protección de la información, promover las buenas prácticas, poner publicidad como posters en los laboratorios.

16 de octubre del 2009 a las 18:00hrs

Noé Cruz Marín
Jefe de departamento de Redes y operación de Servidores

¿Existe documentos previos a las Políticas de Seguridad en Cómputo (PSC)?

No existían.

¿En qué consistían esos documentos?

Antes de las políticas actuales solo existían recomendaciones y la experiencia de los administradores.

¿Cómo se implementaba la seguridad en ese tiempo?

Se implementaba de la mejor forma posible, era un proceso empírico.

¿Por qué se decidió realizar un este documento?

Existían casos severos de acoso de todos tipos, violencia, amenazas por medio de los diversos medios que se tenían en ese tiempo además de violaciones (accesos no autorizados en su mayoría) a los sistemas que se tenían.

Es por eso que se decidió realizar una normatividad que regulara muchas de las actividades y que ayudara a la minimización de los incidentes.

¿Quiénes fueron los responsables de actualizar o realizar este nuevo documento?

Fue un trabajo en conjunto de diversas áreas

¿Quién es el responsable directo de la autorización de las PSC?

La propuesta fue avalada por el asesor de cómputo, que fue un esfuerzo del director de la FI en ese tiempo.

¿Existe alguna organización con respecto a las PSC, es decir un autor, autorizador, custodio, ejecutor, supervisor y quienes serian?

De manera institucional es el Ing. Rafael Sandoval, el es el encargado y jefe del Departamento de Seguridad en Cómputo de la FI (DSCFI), dicho departamento tiene un papel importante ya que es un organismo independiente (no está ligado o asociado a ninguna división), que puede realizar funciones como auditorias, análisis forenses, revisiones y asesorías.

¿Durante la realización de las PSC se tomo alguna base, principio, se siguieron algunas reglas especificas para la redacción de este documento?

No, fue un consenso y esfuerzo conjunto de diversas áreas.

Sanciones

¿Qué es una carta de extrañamiento?

Es una manera formal de llamar la atención.

Universidad Nacional Autónoma de México

Facultad de Ingeniería

Apéndice 2

Encuesta

Nombre:
No. Cuenta:
Semestre:
Carrera:

1.- ¿Posee algún equipo portátil con acceso a Internet?

SÍ	NO

2.- ¿Tiene acceso a alguna de las redes internas de la Facultad de Ingeniería? (Sin contar la RIU)

SÍ	NO

3.- Para usted ¿Qué es la seguridad informática?

4.- ¿Cree usted que la seguridad informática es importante? ¿Por qué?

5.- De acuerdo con su definición de seguridad informática, ¿considera que la Facultad de Ingeniería cuenta con un buen nivel de seguridad informática?

SÍ	NO

6.- ¿Sabe usted qué son las buenas prácticas?

SÍ	NO

7.- Sabe usted ¿Qué son las políticas de seguridad informática?

SÍ	NO

8.- ¿Ha visto reglamentos pegados, reglas que deben seguirse, letreros que indiquen acciones que deben tomarse en cuenta o que deben realizarse de manera obligatoria, si alguien le ha comentado ciertas reglas antes de darle una cuenta, etcétera aquí en la Facultad?

SÍ	NO

9.- ¿Tiene conocimiento de las políticas de seguridad informática de la facultad de ingeniería? (si la respuesta es No pase a la pregunta 15)

SÍ	NO

10.- ¿Cómo se enteró de su existencia?

11.- ¿Las ha leído?

SÍ	NO

12.- ¿Tuvo problemas para entenderlas?

SÍ	NO

13.- Usted sigue las políticas antes mencionadas

SÍ	NO

14.- ¿Ha visto que las políticas de seguridad se sigan en la FI?

SÍ	NO

15.- ¿Usted cree que hace falta mayor difusión de las políticas de seguridad de la FI?

SÍ	NO

16.- ¿Si usted supiera dónde consultar las políticas de seguridad informática de la FI las leería?

SÍ	NO

17.- ¿Dónde le gustaría ver las políticas de seguridad informática de la FI? (páginas de Internet, entrada a laboratorios, etcétera) Mencione algunos lugares donde cree que tendrían mayor difusión.

NOTAS:

Universidad Nacional Autónoma de México

Facultad de Ingeniería

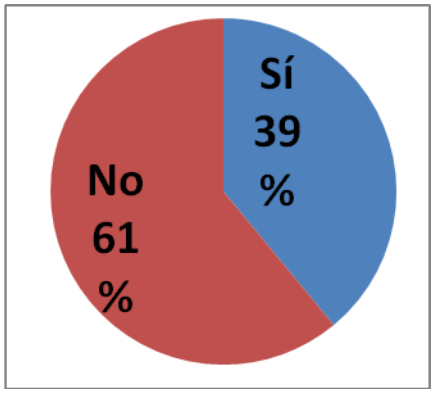
Apéndice 3

Resultados de la encuesta aplicada a alumnos de la Facultad de Ingeniería

Resultados de la encuesta aplicada

En el semestre 2010-1 tras la aplicación de una encuesta[28] con el objetivo de la obtención de datos sobre los conocimientos acerca de temas como las Políticas de Seguridad Informática (PSI), las buenas prácticas, seguridad informática, las políticas vigentes, y preguntas relacionadas para la realización de una propuesta adecuada y efectiva para la difusión de estas dentro de la Facultad de Ingeniería (FI).

Los datos recopilados revelaron que el 39% de los encuestados respondieron saber que son las políticas de seguridad informática (PSI), (ver grafica 1.1),es decir que menos de la mitad conoce o posee algún conocimiento acerca de estos temas, no obstante solo el 33% sabe que son las buenas prácticas. Estos indicadores son preocupantes ya que de manera general solo 3 de cada 10 tienen conocimiento acerca de estos temas lo cual deja a las otras 6 personas sin ningún conocimiento sobre el cómo manejar, administrar, cuidar y proteger su información y los recursos que se le confían.



Grafica 1.1 Conocimiento sobre las PSI

La encuesta también registro datos acerca de lo que los usuarios tienen definido como seguridad informática, y se encontró que el 80% piensa que la seguridad informática está principalmente relacionada con el evitar robos de información personal, con técnicas y herramientas para la protección de la información electrónica, así como la seguridad que se implementa en las redes de datos, mediante software, configuraciones y herramientas.
Esta parte de la población encuestada asocia la seguridad informática a la navegación segura por internet de manera que los datos personales que utilicen para las diferentes activida-

[28] Ver apéndice 2, formato de encuesta para la aplicación.

des sean debidamente protegidos, así mismo también se asocia con diversos tipos de virus (malware), que busca el robar y destruir la información de los usuarios.

Un punto recurrente de los usuarios es la preocupación acerca la información personal que se utiliza, esta preocupación está asociada al pensamiento de que atacantes (hackers), utilizan herramientas como los "sniffers" con el fin de interceptar información como el nombre de usuario y contraseña, esto con el fin de poder acezar cuentas de correo electrónico, cuentas de redes sociales, cuentas bancarias o de otros servidores para diversos propósitos con el fin de obtener un beneficio de forma ilícita.

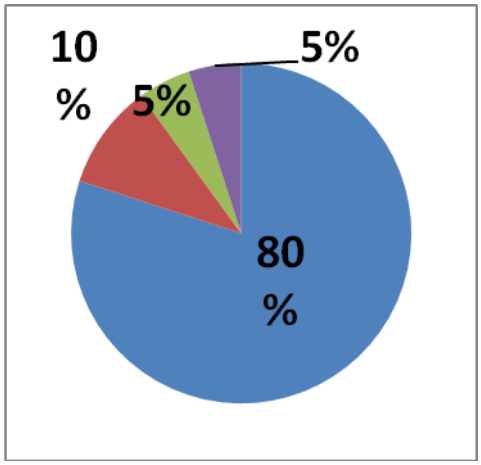
El robo de información, la suplantación de identidad, el daño a equipos, la extorción y los fraudes son temas que los usuarios comentaron son parte de las tareas u objetivos que tiene la seguridad informática, no obstante este tipo de problemas pueden ser evitados o prevenidos por parte de los usuarios de tener una capacitación adecuada acerca de estos temas que son explotados por los medios de información todo el tiempo al exagerar notas y al enfocarse de manera errónea, en otras palabras, los medios de comunicación exageran las noticias y crean un mito acerca de la existencia del "hacker" como un delincuente o terrorista cibernético y omitiendo que estos son errores que pueden ser evitados de manera muy sencilla.

La posibilidad de tener virus y que este tipo de hackers (Script Kiddies) puedan apoderarse o tener acceso a la información personal es un pensamiento recurrente en las respuestas, sin embargo esto es una señal clara de la falta de conocimiento que existe acerca de estos temas y de la desinformación que existe acerca de estos temas, es decir estas ideas son resultado de una mala capacitación o de la falta de ella.

Con respecto al otro 20% de la población encuestada acerca de la definición de seguridad informática solo el 10% contesto que la seguridad informática tenía que ver con la implementación de seguridad en las Tecnologías de la Información (TI), 5% contesto que no sabía o no tenía idea y solo un 5% la asoció con la protección de una organización y de los activos de una organización.

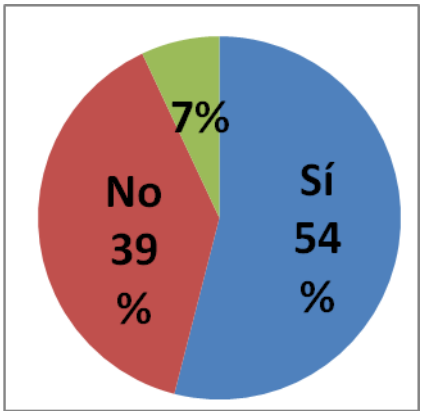
A continuación se presenta una breve síntesis de los porcentajes mencionados. (Ver gráfica 1.2).

80% - Protección de información personal de virus y atacantes.
10% - Implementación de seguridad en las Tecnologías de la Información (TI).
5% - No sabe o no tiene conocimiento.
5% - Está relacionada con la protección de todo tipo de activos de una organización



Grafica 1.2 Conocimiento sobre la Seguridad informática.

De acuerdo con la definición de los encuestados acerca de la seguridad informática se les preguntó si consideraban que en la Facultad de Ingeniería (FI), existía un buen nivel de seguridad informática lo que resulto en que solo el 54% de la población encuestada dijo que sí, el 39% dijo que no y el 7% fueron respuestas inválidas. (Gráfica 1.3)

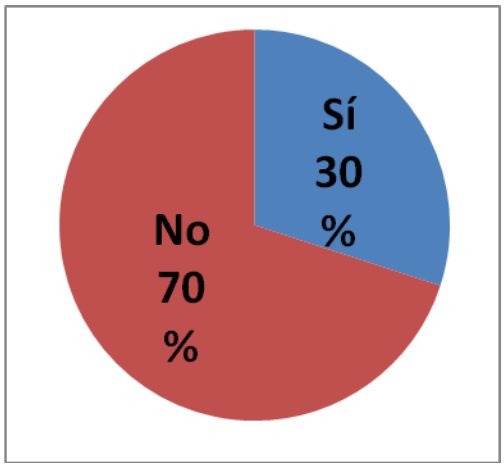


Gráfica 1.3 La existencia de un buen nivel de seguridad dentro de la Facultad de Ingeniería (FI).

Con respecto al acceso de los alumnos a las diferentes redes de la FI, y al uso de equipos dentro de se tienen los siguientes datos.

Cerca del 60% del grupo cuenta con algún tipo de equipo móvil y cerca del 30% tiene acceso a redes internas dentro de la Facultad, sin incluir la Red Inalámbrica Universitaria (RIU). Esto implica que la Facultad de Ingeniería (FI), presta el servicio de conexión a internet

para equipos móviles en los diferentes laboratorios, áreas y divisiones a una buena parte de la población. (Gráfica 1.4).

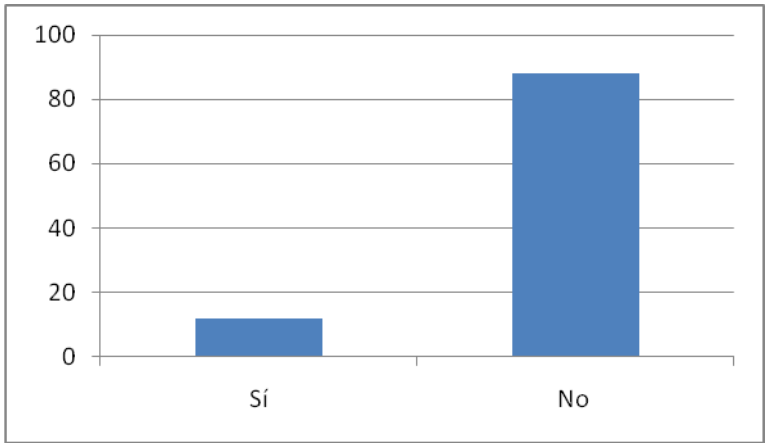


Gráfica 1.4 Acceso a redes internas de la Facultad de Ingeniería.

La población fue cuestionada acerca de su conocimiento sobre la existencia de reglamentos internos para los distintos laboratorios y solo el 41% contesto tener conocimiento sobre este tipo de normatividad, es decir menos de la mitad tiene conocimiento sobre reglamentos internos de laboratorio lo cual puede deberse a la falta o una falla en la difusión de estos, por esto se debe tener una mejor estrategia para dar a conocer estos reglamentos a los usuarios con el fin de que los laboratorios se beneficien en cuanto a que los recursos que estos poseen se aprovechen de una mejor forma por parte de los usuarios.

De esta forma se busca que los usuarios aprovechen y usen los recursos de una manera apropiada, efectiva y se disminuyan los problemas que se pudieran llegar a tener como son las fallas por malware, robos, perdida de información entre otras.

De la misma forma fueron cuestionados sobre la existencia de políticas de seguridad en la Facultad de Ingeniería (PSC-FI), y solo un 12% de la población afirmo tener algún conocimiento sobre estas. (Gráfica 1.5).

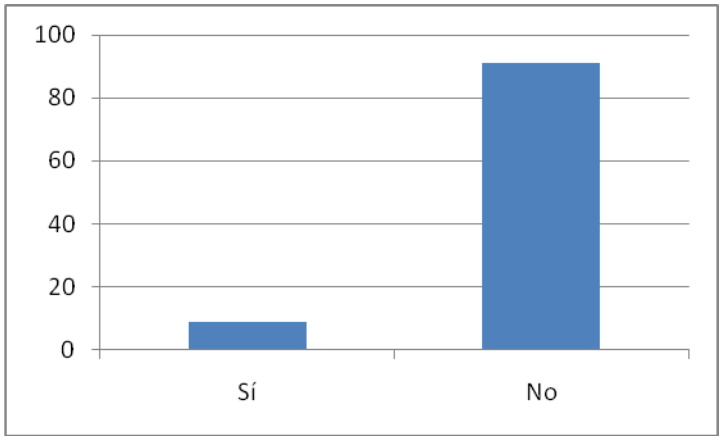


Gráfica 1.5 Conocimiento sobre la existencia de las PSI dentro de la Facultad de Ingeniería

Dicho de otra manera los encuestados han escuchado, leído, o sido capacitados acerca de este documento, en su mayoría los alumnos que contestaron de manera afirmativa son de semestres avanzados lo cual posibilita el que muchos de ellos estén realizando proyectos en conjunto con los diferentes laboratorios, se encuentren realizando su servicio social, laboren ahí, sean encargados o administradores.

De esa población que sabe sobre la existencia de las políticas solo el 72% contesto que ha leído el documento y de este total el 12% ha tenido problemas para entender el documento, esto es, 12 de cada 100 personas saben de la existencia del documento, y de estas 12 personas 1 ha tenido problemas para entender por completo el documento.

A estos datos se debe agregar que solo 9 personas siguen las políticas establecidas por el documento, por lo que en términos prácticos solo 9 de cada 100 siguen las políticas establecidas por lo que los otros 91 usuarios pueden estar incurriendo en faltas de todo tipo que pueden ocasionar perdidas de todo tipo. (Gráfica 1.6)



Gráfica 1.6 Usuarios que siguen las PSI dentro de la Facultad de Ingeniería.

De acuerdo con el 98% de los encuestados se debe tener una mejor difusión de las PSI y de temas relacionados con la seguridad informática lo cual refleja que hay un interés acerca de estos temas lo que facilitaría la realización de campañas, seminarios, talleres, conferencias y diversas maneras para capacitar a los usuarios en estos temas.

No obstante solo el 88% de la población consultaría las PSI de la FI de saber donde está dicho documento, por lo que se puede concluir que dicho lugar (sitio WEB), debe ser un sitio el cual pueda ofrecer esta información de una manera rápida y de manera apropiada, es decir que el visitante pueda ir o consultar la información en cuestión de manera fácil, por lo que sería bueno la implementación de un buen buscador, títulos efectivos, y que los documentos y la información contenida este bien estructurada.

Para la realización de un buen plan de difusión de las PSI es necesario el contar con propaganda en lugares en los cuales los usuarios acudan constantemente por información por lo que una de las preguntas era acerca de los lugares donde se tendría una mayor difusión.

A continuación se mencionan los lugares más citados por los encuestados en orden descendente.

En las página principal de la Facultad de Ingeniería y en las páginas de las diversas divisiones que la conforman.
En las bibliotecas, y a las entradas de los edificios.
Lugares para publicidad dentro de la Facultad de Ingeniería.
En los salones y los laboratorios existentes.
Boletines y gacetas.

La encuesta puso de manifiesto la falta de difusión, conocimiento y capacitación existente en la Facultad de Ingeniería por lo que es necesario la realización de un plan que busque el difundir más la cultura sobre estos temas los cuales sean abordados de manera práctica y con un nivel adecuado que pueda ser comprendido por los diferentes usuarios que conforman a la Facultad.

Por lo anterior se puede concluir que hace falta capacitación sobre este tema, ya que es evidente la falta de conciencia de los alumnos con respecto a que existe un alto porcentaje de ellos que desconocen lo que son las PSI y los beneficios que se pueden obtener de tener una buena capacitación sobre los temas de seguridad informática.

Por otra parte es necesario el aclarar que las seguridad informática tiene como finalidad el proteger la organización y que esta no solo abarca a las tecnologías de la información, sus objetivos y alcances van aun más allá al proteger entre esto se encuentran el prestigio de la organización, el nombre de esta, los bienes entre los que se encuentran como son los edificios, instalaciones, equipos, vehículos, sistemas, de esta misma manera también comprende todo tipo de información aunque esta no se encuentre en forma digital, o almacenada en medios electrónicos, busca el proteger al personal o recursos humanos que son indispensables en cualquier organización.

Puede concluirse que la mayor parte de los encuestados tiene la idea de la importancia que tienen los temas de seguridad así como los problemas asociados a estos que hoy en día están presentes, no obstante es necesario que se divulguen y difundan las políticas de seguridad que no solo tienen como objetivo la protección de la información y las tecnologías relacionadas con esta, lo cual es un error que es muy común.

Universidad Nacional Autónoma de México

Facultad de Ingeniería

Apéndice 4

Políticas de seguridad en cómputo para la Facultad de Ingeniería

Políticas de seguridad en cómputo para la Facultad de Ingeniería

Contenido

Posibles causas de violación de las políticas de seguridad
Procedimientos en caso de violación de las políticas de seguridad
¿Qué sucede si un usuario local viola las políticas de un sitio remoto?
Estrategias ante un incidente de seguridad

Plan de contingencias

Desarrollo de un plan de contingencias
Plan de contingencias
Definición de un plan de contingencias
Fases de un plan de contingencia
Características de un Plan de Contingencias
Características de un buen plan de contingencias
Estructura de general del plan de contingencias

Buenas Prácticas

Buenas prácticas para el uso de correo electrónico
Buenas prácticas para redes inalámbricas
Buenas prácticas para el uso de tecnologías emergentes
Buenas prácticas para la colaboración

Códigos de Ética

Códigos deontológicos en informática
Situación actual de la ética de la informática
Códigos de ética
Código de ética universitario
Código de ética para la facultad de ingeniería en el ámbito de la seguridad informática
Responsabilidad hacia la profesión
Evaluación a los alumnos

Normatividad y lineamientos para el desarrollo de sistemas para la Facultad de Ingeniería
Normatividad y lineamientos para el desarrollo de sistemas

Elaboró	**Aprobó**	**Autorizó**
_____	_____	_____
Firma **Responsable de la elaboración y edición del documento**	**Firma** **Responsable del departamento de seguridad en cómputo**	**Firma** **Responsable 4del CACFI**

Historial del documento

Fecha de elaboración	Fecha de autorización	Quién Autoriza	Naturaleza del cambio

Control de revisiones

Fecha de instauración	Ultima revisión	Tiempo entre revisión	Fecha de la próxima revisión

Copia para

Área / Dirección	Persona
Facultad de ingeniería, UNAM	**Toda la comunidad de la Facultad de Ingeniería**

Introducción

Este documento presenta las políticas de alcance institucional que permite crear y establecer 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 definen ciertos lineamientos que establecen un límite entre lo que está permitido a los usuarios dentro de la institución y fuera de ella así como lo que se encuentra prohibido, esto es con el propósito de proteger la información almacenada en los sistemas y el acceso a éstos.

Para ello, se considera que 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 se tienen con esta conectividad son casi ilimitadas, más no así, los recursos computacionales y de conectividad disponibles.

Este nuevo mundo virtual al que se tiene 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 claras, bien entendidas, que circulen ampliamente, sean difundidas 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 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 se cuente con un cierto nivel de seguridad, 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.
Estar redactadas de manera positiva.
Homogéneas al emplear los términos.
Considerar a todo el personal.

Las políticas son parte fundamental de cualquier esquema de seguridad eficiente. Como administradores, minimizan los riesgos, y permiten actuar de manera rápida y acertada en caso de haber una emergencia de cómputo. Como usuarios, 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.
Glosario de términos.

Al diseñar un esquema de políticas de seguridad, conviene que se divida el trabajo en diferentes políticas de tópico específico: cuentas, contraseñas, control de acceso, uso adecuado, respaldos, correo electrónico, contabilidad del sistema, seguridad física, etcétera.

Seguridad en cómputo

Es un conjunto de recursos destinados a lograr que los activos de cómputo de una organización sean confidenciales, íntegros, consistentes y disponibles para sus usuarios, autenticados 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 es protegida de cualquier tipo de alteración o modificación por parte de 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, día y cantidad de tiempo requeridos cuando se requiera o necesite.

Autenticado. Únicamente deben ingresar al sistema personas autorizadas siempre y cuando comprueben que son usuarios legítimos.

Control de acceso. El acceso es restringido, es decir, sólo personal autorizado puede estar en ciertos lugares, ciertos días, a ciertas horas dependiendo de su cargo y responsabilidades, ya que debe conocerse en todo momento quién entra al sistema y de dónde procede.

Auditoría. Es una función necesaria ya que mediante ésta se puede hacer un seguimiento de cómo es que los equipos se comportan de acuerdo con las políticas, son necesarias al ocurrir un incidente pues permiten conocer en cada momento las actividades de los usuarios dentro del sistema, analizarlas y diseñar e implementar planes de contingencia.
Las políticas del presente documento tienen como alcance a la Facultad de Ingeniería de la UNAM.

Factores críticos

Es fundamental para el éxito de un esquema de seguridad hacer énfasis en el apoyo por parte de la gente con el poder de decisión (cuerpo directivo), ya que sin él, algunos elementos de dicho esquema serían inválidos. Así mismo es vital mantener en constante capacitación al personal mediante cursos, seminarios, congresos, etcétera. 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 actividades ilícitas. 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 datos.

Filosofía de políticas de seguridad

La filosofía que se seguirá para redactar las políticas de seguridad será prohibitiva, es decir **“Todo está prohibido a excepción de lo que está específicamente permitido”**.

Comité asesor de cómputo de la Facultad de Ingeniería[29]

El Comité Asesor de Cómputo (CACFI), es el órgano conformado por representantes de todas las áreas que conforman la Facultad de Ingeniería cuyo objetivo es el de promover y asesorar el óptimo desarrollo informático, es decir, conjuntar los esfuerzos de las diferentes áreas que conforman la Facultad para lograr un desarrollo integral en temas de computación, procurar la normatividad, la estandarización y en general, buscar mecanismos de racionalización y optimización en materia de cómputo.

El CACFI tiene las siguientes funciones:

Verificar el cumplimiento de las políticas y normatividades dictadas por el Consejo Asesor de Cómputo de la UNAM, así como la difusión de nuevas disposiciones en temas sobre computación y tópicos relacionados con éste.

Constituir un foro de discusión sobre los distintos aspectos de la problemática de Cómputo en la Facultad de Ingeniería.

Participar en los planes de desarrollo que de manera integral involucren a la computación y sus disciplinas afines, tales como la informática, las telecomunicaciones y la electrónica.

Asesorar a la Dirección de la Facultad en el establecimiento de políticas de adquisición y mantenimiento de equipo de cómputo que permitan optimizar el aprovechamiento de los recursos disponibles.

[29] http://www.ingenieria.unam.mx/cacfi/documentos/art_comite.pdf, 2009

Promover la cultura informática en todo el ámbito de la Facultad.

Integrantes del CACFI

Mtro. José Gonzalo Guerrero Zepeda
Director de la Facultad de Ingeniería

Dr. Francisco Javier García Ugalde
Secretario del Comité Asesor de Cómputo

Ing. Rafael Sandoval Vázquez
Secretaría General

M.C. Eduardo Espinosa Ávila
Secretaría Administrativa

Ing. Jorge Ontiveros Junco
Secretaría de Servicios Académicos

M.I. Gerardo Avilés Rosas
Secretaría de Apoyo a la Docencia

Ing. Luis del Olmo Dacosta
Secretaría de Posgrado e Investigación

Ing. Dafne Abad Martínez
Coordinación de Planeación y Desarrollo

Lic. José Luis Camacho Calva
Coordinación de Vinculación Productiva y Social

Ing. Carlos Rodríguez Oliva
División de Educación Continua y a Distancia

M.C. Alejandro Velázquez Mena
División de Ingeniería Eléctrica

Ing. Tanya Itzel Arteaga Ricci
División de Ingenierías Civil y Geomática

Ing. Socorro Armenta Servín
División de Ingeniería Mecánica e Industrial

Ing. José Luis Hernández Ramírez
División de Ingeniería en Ciencias de la Tierra

M.I. Janete Mejía Jiménez
División de Ciencias Básicas

Ing. Guadalupe Dalia García Gálvez

División de Ciencias Sociales y Humani- dades

Departamento de Seguridad en Cómputo de la Facultad de Ingeniería

El Departamento de Seguridad en Cómputo de la Facultad de Ingeniería DSCFI es un organismo independiente encargado de brindar apoyo, asesoría, y diversos servicios como son auditorías, apoyo para la configuración de equipos y sistemas, análisis forenses, respuesta a incidentes, entre otros.

Este organismo es independiente e imparcial con el objetivo de poder realizar este trabajo con profesionalismo y ética de tal forma que pueda desarrollar actividades asociadas con la seguridad informática donde en ocasiones es necesario realizar investigaciones sobre incidentes, auditorías a equipos, recuperación de información, etcétera, donde en ocasiones es necesario el revisar información perteneciente a los usuarios la cual se maneja bajo estrictas normas de ética y discreción.

Algunas de las responsabilidades de este departamento es brindar y establecer un alto nivel de seguridad informática a las redes de la Facultad de Ingeniería, la respuesta a incidentes que puedan afectar el tráfico en las redes, minimizar los incidentes de seguridad informática dentro de la Facultad de Ingeniería.

Ing. Rafael Sandoval Vázquez

Jefe del Departamento de Seguridad En Cómputo[30]

[30] http://132.248.54.45/unica/organizacion/dsc.jsp

Sección de Políticas

Responsabilidades del usuario

La comunidad que conforma la Facultad de Ingeniería tiene como responsabilidad ~~el~~ hacer buen uso de los recursos informáticos, de las instalaciones y de todo tipo de información que se les confía. El que los usuarios se manejen de una forma responsable, digna, ética y respetuosa en todo momento es una prioridad y un objetivo que la Facultad promueve mediante la impartición de las materias de humanidades así como de otras actividades.

Es por esto que en todo momento los usuarios que pertenecen a esta comunidad, aun cuando las políticas de seguridad contenidas en este documento no contengan o hagan omisión de alguna normatividad o manera de conducirse, se sabe que éstos a través de diferentes acciones como son el navegar en internet, el envío de mensajes de cualquier clase, el usar todo tipo de equipos, el desarrollo académico, su manera y modo de conducirse o cualquier otro tipo de actividad que desarrollen están representando a la Facultad de Ingeniería y a la UNAM.

Por lo anterior es necesario tener en mente que la seguridad informática empieza por cada uno de los que pertenecen a esta comunidad, los cuales son dignos representantes de la Facultad de Ingeniería que es parte de la máxima casa de estudios de este país y que todo tipo de acciones o actividades que se desarrollen son a su vez reflejo de esta institución.

Los documentos presentados son las políticas de alcance institucional que permite crear y establecer una filosofía sobre la postura que en materia de seguridad en cómputo debe tener la institución respecto a los riesgos que la rodean.

Éstas definen ciertos lineamientos que establecen un límite entre lo que está permitido a los usuarios dentro de la institución y fuera de ella así como lo que se encuentra prohibido, esto es, con el propósito de proteger los equipos de cómputo, las actividades, así como la información almacenada en los sistemas y su acceso. Para ello, se considera que el principio básico de seguridad es:

"Lo que no se permite expresamente, está prohibido"

Por lo anterior es responsabilidad de toda la comunidad que conforma la Facultad de Ingeniería el revisar y cumplir con las políticas ya que mediante éstas se busca hacer un mejor y más eficiente uso de los recursos con los que se cuentan, no obstante en el caso de incumplimiento de las mismas puede resultar en una acción disciplinaria.

POLÍTICAS DE SEGURIDAD FÍSICA

El primer paso a considerar en un esquema de seguridad que muchas veces carece de la suficiente atención, es la seguridad física; es decir, 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, etcétera.

Políticas:

- Mantener el equipo de cómputo alejado de cualquier tipo de agente que pueda causar cualquier tipo de daño o interfiera con su rendimiento como son, el fuego, humo, polvo, temperaturas extremas, rayos solares, vibraciones, insectos, ruido eléctrico, balastras, equipo industrial, del agua, etcétera.

- Todos los servidores deben ubicarse en lugares de acceso físico restringido y deben contar, para acceder a ellos, con puertas con chapas.

- El lugar donde se instalen los servidores deben contar con una instalación eléctrica adecuada, entre sus características deben contar con tierra física y sistemas de alimentación ininterrumpida o de emergencia, UPS (Uninterruptible power supply).

- Las áreas donde se encuentra el equipo de cómputo deben estar libres de cualquier tipo de productos que pueda causar algún daño.

- El área donde se encuentren los servidores debe estar en condiciones de higiene, es decir, debe estar libre de objetos ajenos y de acuerdo con los estándares del cableado estructurado. Debe conservarse limpio, organizado, y despejado de objetos extraños o ajenos para el uso al cual está destinada esta área.

- Debe contarse con extintores en las salas de cómputo y el personal debe estar capacitado en el uso de éstos.

- Las salas de cómputo debe contar con una salida de emergencia.

POLÍTICAS DE REGLAMENTOS INTERNOS

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

Políticas:

- Los departamentos, áreas, laboratorios y áreas que requieran desarrollar normas, reglamentos internos o políticas de seguridad informática adicionales o complementarias a las políticas contenidas en este documento son respaldadas por el DSC y el CACFI.

- Los reglamentos, normatividades, y políticas deben buscar, perseguir y tener los mismos objetivos y metas que las Políticas de Seguridad en Cómputo (PSC-FI).

- En caso de presentarse alguna discrepancia el CACFI estudiará el caso y presentará una resolución a ésta a la brevedad posible.

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 autorizados. Se consideran usuarios autorizados a aquellos usuarios quienes hayan realizado su trámite de registro de cuenta y que:
- Sean miembros vigentes de la comunidad de la Facultad de Ingeniería.
- Participen en proyectos especiales y tenga la autorización del jefe inmediato o el jefe del proyecto.
- Una cuenta debe estar conformada por un nombre de usuario y su respectiva contraseña.
- La asignación de las cuentas la hace el administrador del área o departamento en cuestión y al usuario sólo le da derecho de acceder a los recursos destinados dependiendo de sus actividades, cargos, y tareas a realizar en dicho laboratorio o área de trabajo.
- El administrador debe deshabilitar las cuentas inactivas.
- Las cuentas y contraseñas son personales e intransferibles.

POLÍTICAS DE CONTRASEÑAS

Son una de las políticas de tópico específico 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 asigna la contraseña, qué longitud debe tener, a qué formato deberá apegarse, cómo es comunicada.

Políticas:

- El administrador del servidor es el responsable de la creación y administración de las cuentas, la activación y desactivación de ellas según sea el caso y propósito de ellas. La contraseña debe cambiarse la primera vez que se utilice por el usuario.

- El administrador debe contar con herramientas de detección de contraseña débiles.

- La longitud de una contraseña debe siempre ser verificada de manera automática al ser construida por el administrador/usuario. Todas las contraseñas deben contar con al menos seis caracteres.

- Todas las contraseñas deben ser robustas, es decir, son contraseñas que contienen letras mayúsculas, minúsculas, números, así como caracteres especiales, evitando el uso de palabras en cualquier idioma. Debe considerar que el uso de información personal es peligroso por lo cual se recomienda evitar el uso de datos personales. La contraseña debe tener una longitud mínima de 6 caracteres y que ésta sea cambiada periódicamente por lo menos cada 6 meses, evitando repetir contraseñas ya utilizadas en alguna cuenta.

- Todas las contraseñas elegidas por los usuarios deben evitar utilizar palabras que aparezcan en el diccionario de cualquier idioma, secuencias conocidas de caracteres, datos personales ni acrónimos.

- Los usuarios deben evitar la construcción de contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar.

- Las contraseñas que los usuarios construyan deben ser totalmente diferentes a las contraseñas anteriores o a las de otros usuarios.

- La comunicación de la contraseña se realiza de manera personal vía el administrador, y sin intermediarios entre el administrador y el interesado.

- Las contraseñas deben ser entregadas de manera personal, por lo que el interesado debe presentarse en el laboratorio o lugar de trabajo para la asignación de ésta autenticando su identidad ante el responsable antes de entregarle su contraseña.

- Las contraseñas deben cambiarse periódicamente cada seis meses. El administrador debe contar con algún sistema el cual pueda evaluar la situación de la contraseña con la finalidad de que el usuario conserve su derecho a la privacidad y de esta manera hacer que el usuario cambie y respete las políticas; el sistema también tiene que cifrar el historial de contraseñas del usuario, el cual guardará las últimas 6 contraseñas con la finalidad de conservar la integridad de los datos contenidos, en este caso las contraseñas.

Véase también el apartado de gestión de contraseñas.

POLÍTICAS DE CONTROL DE ACCESO

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

Políticas:

- Todos los equipos que den un servicio de acceso remoto deben contar con aplicaciones que permitan una comunicación segura y cifrada.
- Todos los usuarios deben autenticarse y hacer uso sólo de su cuenta.
- Será sancionada la persona que acceda al sistema con una cuenta diferente de la propia, aún con la autorización del dueño de dicha cuenta.
- Al momento de ingresar a cualquier sistema operativo (UNIX, Windows, Mac o algún otro), cada usuario debe ser notificado de la fecha, hora y dirección IP desde la que se conectó al sistema por última vez, lo cual permitirá detectar si alguien más está haciendo uso del sistema.
- El usuario tiene derecho a cambiar su contraseña. Ésta debe ser robusta, es decir, que cumpla con las siguientes características.
- Tener una extensión mínima de 6 caracteres
- Evitar el uso de datos personales o información privada, como fecha de nacimiento, nombres, apellidos, RFC, CURP, direcciones, números asociados al usuario como números telefónicos, número de trabajador, número de cuenta etcétera.
- Evitar el uso de palabras contenidas en diccionarios de cualquier tipo, incluyendo otros idiomas.
- La contraseña debe usar combinaciones de letras, números y caracteres especiales.
- Evitar el uso de una sola contraseña para diferentes cuentas, es decir, usar una contraseña por cuenta.

- Cambiar la contraseña al menos cada 6 meses.
- El usuario puede utilizar los servicios de sesiones remotas si se brinda.

POLÍTICAS DE USO ADECUADO

Las políticas de uso aceptable están basadas en las políticas de seguridad en cómputo de la Facultad de Ingeniería, éstas 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.

Políticas:

Usuarios en general:

- La ejecución y utilización de software o hardware, todo tipo de programas o herramientas que se ocupen para la obtención de cualquier tipo de información como contraseñas, usuarios, información personal, vulnerabilidades de los sistemas, configuración de los equipos, una clara violación a estas políticas, por lo que la persona que lo haga debe ser sancionada. (Ver POLÍTICAS DE CONTABILIDAD DEL SISTEMA).

- La cuenta de un usuario es personal e intransferible, es decir, el único autorizado para el uso de la cuenta y los recursos es el dueño de dicha cuenta la cual es intransferible.

- Es responsabilidad del usuario tener una gestión apropiada de las cuentas que le son asignadas. (Ver apartado de gestión de contraseñas).

- La instalación de programas y software, en caso de requerirse debe ser solicitado al administrador del sistema.

- El uso del equipo es estrictamente con fines académicos y/o investigación por lo que cualquier usuario que le dé algún otro uso como el lucro, ocio, descarga de música, imágenes, videos, chat, debe ser sancionado.

Alumnos:

- Pueden realizar sus tareas con fines académicos y asociadas con los programas académicos de la Facultad de Ingeniería.

- Pueden utilizar los servicios de Internet donde se brinden siempre y cuando sólo se haga con fines académicos.

- Pueden utilizar software de aplicación ya instalado.

- Pueden utilizar los servicios de impresión donde se brinden.

Académicos, Investigadores y Administrativos:

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

- El Departamento de Seguridad en Cómputo de la Facultad de Ingeniería (DSCFI), y las áreas de Investigación de Seguridad en Cómputo de la Facultad de Ingeniería (AISCFI), son las autorizadas por el CACFI, para la realización de pruebas e investigación en seguridad informática, en ambientes controlados. El DSCFI y las AISCFI deben solicitar permiso e informar de dichas pruebas al CACFI, para programar el tipo, lugar, fecha y hora de éstas. Como requisito deben llevarse a cabo en lugares aislados (redes internas), con la finalidad de evitar comprometer la operación de otras áreas.

- 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.

POLÍTICAS DE RESPALDOS

Especifican la responsabilidad que tienen los usuarios sobre el manejo de la información de la que son responsables según sean su caso.

Políticas:

Usuarios en general:

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

Administradores:

- El administrador del sistema es el responsable de realizar respaldos de la información crítica. Cada treinta días debe efectuarse un respaldo completo del sistema y verificar que se haya realizado correctamente.
- El administrador del sistema es el responsable de restaurar la información.
- La información respaldada debe cifrarse y almacenarse en un lugar seguro.
- Debe 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 debe borrarse del medio total y permanentemente.
- Si algún medio que contiene información es dado de baja o cambiado hacia otra área, el administrador debe cerciorarse de que sea borrada total y permanentemente.
- En caso de ser necesario transportar información sensible o de carácter confidencial en una unidad portátil de almacenamiento (memoria USB Flash, disco duro, laptop, etcétera) ésta debe ir cifrada.

POLÍTICAS DE CORREO ELECTRÓNICO

Establece el uso adecuado del uso y servicio de correo electrónico, así como los derechos y las 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 o responsable puede auditar dicha cuenta. (ver políticas referentes a la auditoría)

- El uso de las cuentas de correo electrónico proporcionadas por la organización es para uso personal con fines académicos.

Véase también Buenas prácticas para el uso de correo electrónico.

POLÍTICAS DE DESARROLLO DE SOFTWARE

Las políticas aquí presentadas especifican los lineamientos para el desarrollo de todo tipo de código ya que son una parte importante de la seguridad informática.

Políticas:

- 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 así como los distintos proyectos en colaboración con alguna otra organización interna o externa a la UNAM, debe seguir los lineamientos establecidos para ello. (Véase Normatividad y lineamientos para el desarrollo de sistemas para la Facultad de Ingeniería)[31].

- Con respecto al desarrollo de herramientas de seguridad informática se deben seguir las mismas políticas y lineamientos especificados que para el desarrollo de sistemas para la Facultad, de Ingeniería además de que dicho desarrollo debe ser notificado al DSC para su supervisión.

[31] http://www.ingenieria.unam.mx/cacfi/documentos/normativiadweb.pdf, 2011

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 debe contar con herramientas de auditoría en el sistema.

- El DSC está facultado para realizar y autorizar el uso de herramientas de seguridad para el análisis de vulnerabilidades en las redes y equipos de la Facultad de Ingeniería para la detección de posibles incidentes de seguridad.

- El único autorizado para realizar monitoreo de la red es el administrador o el personal que se haya asignado para esa responsabilidad.

- El administrador o responsable, así como el departamento de cómputo, tienen la autoridad de realizar auditorías internas cuando éstas se requieran contando previamente con la autorización del responsable, jefe directo del departamento o área a la que está asociado el administrador.

- El administrador o responsable puede realizar un monitoreo de la red en caso de que se presente un incidente de seguridad y cuando necesite estadísticas para rediseñar la red.

POLÍTICAS DE USO DE DIRECCIONES IP

El área responsable en representar a la Facultad de Ingeniería ante DGSCA es el Departamento de Operación de Servidores.

Políticas:

- El administrador de la red debe contar con un registro de las direcciones IP utilizadas.
- El formato que debe utilizar para registrar su información está contenido en el Apéndice A.
- El uso de las direcciones IP está regulado, por lo que sólo se pueden emplear direcciones IP las cuales hayan sido asignadas previamente.
- Ningún usuario final puede hacer alguna modificación en la configuración de la dirección IP asignada al equipo bajo su responsabilidad.
- En el campus de C.U. debe evitarse el uso de servidores de DHCP con Direcciones IP homologadas.
- Las subredes deben emplear rangos relacionados con la zona en la que se encuentren.
- Cada equipo que se incorpore a la red Internet debe tener la autorización del administrador de la red del área en cuestión.
- Si se realiza un cambio de la tarjeta de red se debe informar al administrador de la red, del reemplazo y de la dirección física asociada a la IP.
- Se permiten rangos de direcciones privadas de la forma 192.168.X.X pero su asignación debe controlarse únicamente a los equipos asignados al área.
- Las direcciones IP que pueden otorgarse son homologadas o privadas. Las homologadas sólo son otorgadas si se justifican su uso y disponibilidad. Para asignar una

dirección IP debe justificarse su utilización y solicitarla al administrador o responsable de cómputo para su autorización.

- El administrador de red de la división puede realizar reasignaciones de los rangos de las direcciones IP homologadas y privadas para un mejor desempeño de la red.

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

POLÍTICAS DE SITIOS WEB

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

Políticas:

- Las sitos WEB además deben seguir con las normas, lineamientos y recomendaciones establecidas por la Facultad de Ingeniería (véase Normatividad WEB)[32].

- Es responsabilidad de los administradores y responsables la actualización de los certificados digitales en el caso de requerir o contar con alguno.

- Los servicios que se prestan por medio de los servidores deben sólo tener instaladas las herramientas y aplicaciones necesarias para los servicios que proporcionan.

- La configuración de los servidores es responsabilidad del administrador o encargado de éste el cual debe configurarlos con el principio de mínimo privilegio.

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

- La creación de sitios web o repositorios en servidores y equipos de la Facultad de Ingeniería 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.

[32] http://www.ingenieria.unam.mx/cacfi/documentos/normativiadweb.pdf

POLÍTICAS PARA REDES INALÁMBRICAS

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

Políticas:

- Registro de la Red inalámbrica ante el DSC de la FI.
- Cambiar las claves por defecto cuando se instale el software del Punto de Acceso (Access Point) o PA
- 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 PA.
- El administrador es el encargado de cambiar el SSID que trae el equipo como predeterminado por el SSID registrado ante el DSC.
- El responsable o el administrador es responsable de la protección física de los dispositivos del medio ambiente y sus efectos, así como de posibles atacantes.

POLÍTICAS DE TECNOLOGÍAS EMERGENTES

Son las políticas referentes al uso de tecnologías como la robótica, la inteligencia artificial, las tecnologías de la información y las comunicaciones, las cuales están en constante desarrollo y cambios.

Políticas:

- Es necesario contactar al DSC en caso de requerir hacer uso de tecnologías nuevas o emergentes dentro de la Facultad con el fin de tener un control y conocimiento de qué tecnologías se están implementando y en dónde.

- Es responsabilidad del administrador o encargado proteger de manera adecuada el equipo con el fin de evitar daños y robos.

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:

- Quedan excluidos de ser contratados como administradores de sistemas o áreas de seguridad informática aquellos 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 de los sistemas.

- Los responsables de sistemas deben cambiar todas las contraseñas cuando un administrador de su área deje de prestar sus servicios.

POLÍTICAS DE COLABORACIÓN CONJUNTA

Descripción de lineamientos para la colaboración conjunta con otras áreas, departamentos, facultades u organizaciones externas.

Políticas:

- Es responsabilidad de los interesados la realización, supervisión, implementación de políticas en el caso de colaboración conjunta.

Véase también Buenas prácticas de Colaboración conjunta

ACTUALIZACIÓN DE LAS POLÍTICAS

Establece los procedimientos y acciones para la revisión de las políticas de seguridad con lo que se busca el mejor aprovechamiento de los recursos.

Políticas:

- Las políticas de seguridad deben ser actualizadas y revisadas en un periodo el cual será estipulado por el CACFI.

- El CACFI está facultado para realizar cambios en las políticas en caso de que se consideren necesarias las cuales serán publicados a la brevedad.

- Las recomendaciones, cambios y observaciones que se presenten a estas políticas pueden ser presentadas al departamento de seguridad en cómputo por el administrador a cargo del área, éstas serán analizadas y estudiadas antes de ser presentadas al CACFI.

POLÍTICAS REFERENTES A LA AUDITORÍA

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

Políticas:

- El departamento de seguridad, de cómputo y el administrador en cuestión tienen la autoridad de realizar auditorías internas cuando éstas se requieran contando previamente con la autorización del responsable directo, el jefe del área o división a la que está asociado el administrador.

- Un jefe de área, departamento, división, administrador o responsable directo debe justificar la realización de toda auditoría la cual puede pedir la realice el personal del departamento de seguridad en cómputo.

- La evaluación de los planes de contingencia es conforme a los puntos que se manejan en este documento y pueden ser auditados en caso de ser necesario. (Ver Políticas de plan de contingencia).

- Los responsables de realizar la auditoría deben tener en cuenta que la información que encuentren es confidencial y de propiedad de un usuario por lo que deben ser éticos, y profesionales al realizar su trabajo enfocándose específicamente en lo que van a auditar, y manteniendo respeto absoluto y discreción.

- Al concluir una auditoría se debe generar un reporte el cual debe contener la razón por la cual se realizó y los resultados de ésta.

POLÍTICAS SOBRE INCIDENTES GRAVES

Se considera un incidente de seguridad grave un evento que pone en riesgo la seguridad de un sistema de cómputo y la información contenida en ellos.

Políticas:

- Obtener privilegios o el control de cuentas del sistema, sin que se le haya otorgado explícitamente.
- Atentar contra la confidencialidad, integridad y confiabilidad de los sistemas.
- Difundir, copiar, o utilizar información confidencial para otro propósito ajeno al destinado cual está destinada.
- Cualquier tipo de ataque o intento de explotar alguna vulnerabilidad a equipos de cómputo.
- Ejecución de cualquier tipo de programa para obtener o escalar privilegios, información, cuentas de algún sistema incluyendo cuentas de correo, ingreso al sistema de manera ilícita ya sea de manera local o remota.
- En un incidente donde esté involucrado directamente un administrador de sistema o trabajador de la UNAM.
- Infectar intencionalmente un servidor con cualquier tipo de malware.
- Modificar configuraciones de cualquier tipo de equipo de cómputo sin ser autorizado para realizar dicho cambio.
- Causar cualquier tipo de daño intencional a los medios de comunicación de la red. (como son fibra óptica, UTP, Switches, hubs, ruteadores, transceivers, cableado, etcétera).

Véase Incidentes de seguridad

IMPORTANTE

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

POLÍTICAS DEL PLAN DE CONTINGENCIAS

Especifican el que todas las áreas deben desarrollar estrategias para la protección de sus equipos y las metodologías que el plan debe tener al desarrollarse.

Políticas:

- Todas las áreas, departamentos, o divisiones deben contar con un plan de contingencias para sus equipos o servicios críticos de cómputo el cual es responsabilidad de ellos el desarrollarlo y tenerlo implementado correctamente.

Véase parte de Desarrollo de un plan de contingencias

Sanciones

Se deben aplicar las siguientes sanciones que pueden consistir en la suspensión de los servicios de cómputo por el tiempo estipulado según la falta cometida, o alguna otra más según sea la gravedad de la falta cometida.

Actividad ilícita	**Sanción**	
	Por primera vez	**En caso de Reincidencia**
Consumo de alimentos, bebidas, utilización de los servicios por ocio.	Suspensión de los servicios de cómputo por un día.	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.	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 el permiso del propietario	Suspensión por un mes de los servicios de cómputo a los involucrados en todas las áreas de la Facultad de Ingeniería.	Suspensión a los involucrados de los servicios por un semestre.
Ejecución de programas que intenten obtener información, privilegios, cuentas de algún sistema incluyendo cuentas de correo, o ingreso al sistema de manera ilícita de manera local o remota.	Suspensión de los servicios por un año en todas las áreas de la Facultad de Ingeniería.	Cese definitivo de los servicios de cómputo, durante toda su carrera.
Ejecución de herramientas para rastrear vulnerabilidades en sistemas de cómputo dentro de la Facultad	Suspensión de los servicios por un año en todas las áreas de la Facultad de Ingeniería.	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 de Ingeniería.	Cese definitivo de los servicios de cómputo, durante toda su carrera.
Instalación de software sin autorización previa.	Suspensión del servicio de cómputo por una semana.	Suspensión del servicio por un mes.
Cambio en la configuración de los Equipos.	Suspensión del servicio de cómputo por un mes.	Suspensión de los servicios de cómputo durante un semestre.
Envíos de cualquier tipo de mensajes o propaganda que atenten contra la integridad física o moral de las personas.	Suspensión de los servicios de cómputo por un año en todas las áreas de la Facultad de Ingeniería.	Cese definitivo de los servicios de cómputo, durante toda su carrera.
Utilización de los recursos con fines de ocio y esparcimiento.	Suspensión del servicio de cómputo por un día.	Cancelación de los servicios por un mes en todas las áreas de la Facultad de Ingeniería.

Actividad ilícita	**Sanción**
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 menor.	Carta de “extrañamiento” dirigida al Jefe de División o Secretaría.
Utilización de los recursos con fines diferentes a las funciones de su plaza en caso de ser empleado	Carta de “extrañamiento” dirigida al Jefe de División o Secretaría.

NOTA

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 jefe o responsable del área afectada.

Incidentes de Seguridad

Posibles causas de violación de las políticas de seguridad

Al crear las políticas es necesario contemplar diferentes escenarios. Tarde o temprano, todas las políticas serán violadas.

¿Qué puede llevar a que una política sea violada?

Negligencia.

Falta ocasionada por un acto u omisión por parte del usuario en el desempeño de sus actividades.

Error accidental.

Falta ocasionada por error del usuario.

Desconocimiento de la misma.

Falta por desconocimiento del usuario

Falta de entendimiento de la misma.

Falta ocasionada por mala interpretación o por confusión de la normatividad

Procedimientos en caso de violación de las políticas de seguridad

¿Qué se debe 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).

NOTA: En caso de ser un incidente grave de seguridad, se debe notificar al DSCFI.

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

Debe darse parte al DSC para la realización de una investigación.

Llenar o realizar un reporte acerca del incidente.

Estrategias ante un incidente de seguridad

Proteger y perseguir

Su principal objetivo es proteger y preservar los servicios del sitio pudiendo realizar acciones drásticas, tales como dar de baja los servicios, desconectar el sistema de red, apagarlo, etc. Para posteriormente restablecerlos lo más rápido posible.

Se utiliza esta estrategia cuando:

- Los activos están bien protegidos
- Se corre un gran riesgo debido a la intrusión.
- Existe la imposibilidad o disposición para enjuiciar.
- Se desconoce la base o el origen del intruso.
- Existe un agujero de seguridad y la información está en peligro.
- Los recursos de los usuarios 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.

Se utiliza esta estrategia cuando:

- Los recursos están bien protegidos.
- Se dispone de respaldos confiables.
- El riesgo para los activos es mayor que el daño de ésta 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.

Desarrollo de un plan de contingencias

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", en vez de contar con éste "por si falla el sistema".

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."[33]

"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."[34]

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 este caso es la de interés.

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

[33] http://sistemas.dgsca.unam.mx, 2003

[34] BORGHELLO, Cristian F. "Seguridad Informática". 2001. Capítulo 9, página 13.

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

"Conjunto de procedimientos y acciones que se llevan a cabo antes, durante y después de un desastre, problema o incidente, que permiten recuperar y restablecer el funcionamiento, de los sistemas, servicios y actividades de una organización en el menor tiempo posible."

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 es poco eficiente. En la forma de desarrollar esta fase se diferencian las dos familias metodológicas. Éstas son llamadas Análisis de Riesgo (Risk Analysis) y el Impacto Económico (Business Impact).

El Análisis de Riesgo se basa 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.

La metodología de impacto económico, se basa 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 (Tabla pc1)

Análisis de Riesgo	**Impacto Económico**
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.	1. Identificación de servicios finales. 2. Análisis del impacto. En estas metodologías se evalúan los daños económicos y de imagen y otros aspectos ajenos a los económicos. 3. Selección de servicios críticos. 4. Determinación de recursos de soporte. 5. Identificación de alternativas para entornos. 6. Selección de alternativas. 7. Diseño de estrategias globales de respaldo. 8. Selección de la estrategia global de respaldo.

Tabla pc1, tabla comparativa para el análisis y diseño de un plan de contingencias.

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

Para que un plan de contingencias sea efectivo, se busca que este llene los siguientes requerimientos.

Un plan de contingencia debe 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.

A continuación se explican y desglosan las características mencionadas anteriormente.

Aprobación.

El plan debe 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 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 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.

Es insuficiente sólo 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 auditoría 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 previamente impresos 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 está 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 si es viable, así como los resultados de las pruebas que se hayan realizado, 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 en ocasiones también son los propietarios de las mismas.

Si las revisiones aportan garantías insuficientes 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, carece de 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 éstos 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.

Estructura general del plan de contingencias

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 se deben evitar 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, debe ser detenido 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 ~~el~~ evitar implementar los Planes de Contingencia, sin embargo, por si esto sucede, se debe estar preparado y tener instructivos claros para todas las tareas que deberían realizarse.

Reinstalación: La contingencia como su nombre lo indica, es una situación temporal. 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 sufran lo menos posible al terminar el periodo de contingencia.

Gestión de contraseñas

Gestión de contraseñas

Este apartado tiene como propósito que los usuarios en general sepan la importancia sobre la gestión de contraseñas.

Las contraseñas son de gran importancia ya que son las encargadas de resguardar y proteger la información de los usuarios, sin la existencia de éstas o con una contraseña muy débil es imposible tener los servicios de seguridad, los cuales proporcionan seguridad a la información. Entre ellos se encuentran:

Confidencialidad → Permite que la información sea privada.

Integridad →Que nadie más pueda hacer cambios.

Disponibilidad →Que se pueda tener la información cuando sea necesaria.

Autenticación →Verifica que realmente sean los dueños de la información.

Sin estos servicios cualquier persona puede alterar la información, robarla, destruirla, verla, impedir su utilización cuando sea necesaria. Por esto es importante la gestión de contraseñas.

A continuación se mencionan algunas recomendaciones sobre cómo hacer que las contraseñas sean más seguras.

- Evitar el uso de palabras contenidas en diccionarios de cualquier clase o idioma
- Uso de contraseñas de longitud mínima de 6 caracteres.
- Memorizar las contraseñas y mantenerlas en secreto.
- Es recomendable tener una contraseña por cada cuenta que se tenga ya sea de correo o de usuario en algún equipo.
- Cambiar la contraseña periódicamente, al menos cada 6 meses.
- Uso de mayúsculas, minúsculas y caracteres especiales.

- Evitar el uso de información asociada con la cuenta, usuario o con el propósito de la cuenta.

- El uso de contraseñas previamente utilizadas se considera una falla grave, por lo tanto se debe evitar.

Nota: La simple sustitución de letras por números o símbolos es considerada una contraseña débil que puede ser vulnerada.

Ejemplo:

Contraseña	**Acerca de la contraseña**
facultad	Palabra del idioma Castellano
f4cult4d	Cambio de "a" por el número "4"
F4cult4D	Uso de Mayúsculas
F4cu1t4D	Cambio de "l" por número"1"
F4cu1t4D05	Añadir un par de números "05"
F4cu1t4D-05	Añadir caracteres especiales "-"

El uso de estas recomendaciones hace más segura la contraseña además de ser relativamente fácil el poder memorizarla.

Para el desarrollo de una contraseña fuerte también pueden usarse técnicas nemotécnicas que están asociadas a las antes vistas las cuales consisten en la asociación de frases a palabras nuevas inexistentes en cualquier idioma.

Ejemplo:

Se toma cualquier oración o frase para la construcción de la contraseña:

La mejor escuela de ingeniería es la facultad de ingeniería

Se toman las primeras letras de cada palabra para crear la contraseña.

lmedielfi → Esta palabra es inexistente

Sin embargo, esta contraseña es aún débil, por lo que se sugiere seguir las recomendaciones ya vista, es decir, incluir el uso de mayúsculas, números y caracteres especiales.

Contraseña: **Lm3di3l_FI**

Por último, es importante cambiar la contraseña en caso de sospechar que la cuenta ha sido accedida por alguien más, así como evitar volver a usar esa contraseña en alguna cuenta nuevamente.

Visite la página: **http://132.248.52.4/proyectos/politicas/veri.html** donde se encuentra un software para evaluar el nivel de las contraseñas, el cual puede ayudar a la formulación de una contraseña fuerte.

Buenas Prácticas

BUENAS PRÁCTICAS PARA EL USO DE CORREO ELECTRÓNICO

Las recomendaciones aquí contenidas tienen el fin de hacer un uso adecuado del correo electrónico así como el evitar cualquier tipo de incidentes.

- ✓ Evitar el envío de correos SPAM, es decir cadenas, publicidad, anuncios publicitarios o con intereses personales, chistes, forwards, información intranscendente ajena a actividades académicas, así como el envío de correos ofensivos, los cuales contengan malas palabras, injurias, contenido inadecuado como imágenes de desnudos, entre otros.

- ✓ Es importante evitar abrir correos que carezcan de remitente o asunto, así como direcciones de correo desconocidas.

- ✓ Si se requiere reenviar información se debe evitar que el correo reenviado contenga las direcciones de correo de otros usuarios, por lo que se recomienda el uso de la opción CCO: (con copia oculta), la cual oculta las demás direcciones de correo a las que fue enviado dicho correo.

BUENAS PRÁCTICAS PARA REDES INALÁMBRICAS

Las recomendaciones aquí sugeridas deben tomarse en cuenta para la implementación de seguridad en las redes inalámbricas, ya que por su fácil y sencilla implementación se comete una serie de errores que pueden causar incidentes de seguridad. Por esto se recomiendan las siguientes acciones.

- ✓ Elección de un canal diferente a los utilizados por las redes inalámbricas cercanas para obtener una mejor señal.
- ✓ Apagar el equipo al término de las actividades o cuando el equipo pase a inactividad por periodos largos
- ✓ Tener una buena ubicación para los PA.
- ✓ Desactivar el Broadcasting SSID.
- ✓ Manejar una buena gestión de contraseñas
- ✓ La revisión de las bitácoras de los PA periódicamente para búsqueda de anomalías.
- ✓ Establecer un número máximo de equipos por PA.
- ✓ Control y filtrado de direcciones MAC.
- ✓ Evitar en lo posible la utilización de cifrado con WEP.
- ✓ Ajustar la potencia del PA con la finalidad de sólo tener la potencia suficiente para lo que requerimos, con esto evitar que el alcance de la red salga de la zona donde se trabaje y pueda así ser atacada.

BUENAS PRÁCTICAS PARA EL USO DE TECNOLOGÍAS EMERGENTES

La implementación de tecnologías nuevas y las aplicaciones de éstas para la realización de nuevos productos son algo que se vuelve más común. Un ejemplo de esto es el increíble y rápido avance de las redes inalámbricas, las cuales se han hecho muy populares, algunas de estas tecnologías emergentes son zigbee, bluetooth, rfid, gps, el uso de ambiente virtuales.

Por esto se recomiendan las siguientes acciones.

- ✓ Informarse bien acerca de la tecnología en cuestión antes de operar o adquirir algún dispositivo o producto con esa tecnología.
- ✓ Apagar el dispositivo o producto al finalizar las actividades.
- ✓ En caso de descubrir anomalías o interferencias se debe avisar al responsable con el fin de evitar algún incidente.
- ✓ Evitar el uso para el procesamiento o transmisión de información sensible.
- ✓ Usar algún tipo de cifrado de ser posible.
- ✓ Si existe la necesidad de realizar pruebas, éstas deberán ser en un área y de manera controlada. (Véase también POLÍTICAS DE USO ADECUADO).

BUENAS PRÁCTICAS PARA LA COLABORACIÓN

El establecer recomendaciones para la colaboración conjunta entre dos o más laboratorios, áreas, departamentos, divisiones, facultades u otras organizaciones.

- ✓ De requerir el acceso por parte de personal ajeno a los recursos informáticos, el administrador o responsable debe proveer dicho servicio para garantizar, revocar, y renovar.

- ✓ Capacitar y crear conciencia en los usuarios acerca de la importancia de la seguridad así como acerca de las políticas de seguridad.

- ✓ Aplicar el concepto del mínimo privilegio para la implementación del acceso a los recursos informáticos que se requieren.

- ✓ El personal con el que se colabora debe ser notificado acerca de las políticas, reglamentos, buenas prácticas y procedimientos involucrados los cuales debe seguir durante su estancia.

- ✓ Al término de la relación de colaboración el administrador debe revocar, borrar y deshabilitar todo tipo de cuentas involucradas en dicha relación.

Códigos de Ética

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."[35]

Es conveniente diferenciar la ética de la moral, la ética es una disciplina filosófica, la cual tiene como objeto de estudio la moral, esto es opuesto a decir que la ética crea la moral, 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."[36]

"Otro concepto importante es el de valor, éste no lo poseen los objetos por sí mismo, sino que éstos lo adquieren gracias a su relación con el hombre como ser social."[37]

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

[35] Garza de Flores, Ética, 1993 Ed. Alhambra Mexicana.

[36] Lozano V, Rodríguez, Ética, Ed. Alhambra Mexicana, 1986

[37] Dr. Emma Godoy, ¿Qué son y para qué sirven los valores?

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 ética informática son mucho más amplias. No se reducen a un nuevo campo de ética aplicada sino que, por ejemplo, en el libro de James Moor[38], la ética informática 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 ética informática 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 claridad o nitidez principios de actuación.

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 ética informática es aportar guías de actuación cuando la reglamentación es inexistente 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.

[38] MOOR, James H., "What is Computer Ethics? Metaphilosophy, Vol. 16, No. 4, October 1985, pp. 265-275.

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, es responsable de los aspectos técnicos del producto, como 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 son poco percibidos. Éstos tienen que evitar 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 evaden o son carentes de principios de actuación o respuestas a las preguntas "debe" (qué debería hacer yo como persona, qué debería hacer yo y los míos como organización, qué normas sociales se deberían promover, qué leyes se deberían tener...).

El objetivo de la ética informática busca más que proponer un análisis sobre "sociología de la informática" o sobre la evaluación social de las tecnologías (technology assessment), busca ir 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.

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 se propone 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 apegado 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 INGENIERÍA 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 con 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 eviten vulnerar 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:

a) Interesarse en el bienestar común y aplicar sus conocimientos profesionales para beneficio de la institución así como de sus integrantes.

b) Desarrollar sus deberes con honestidad e imparcialidad y servir con dedicación a sus superiores, sus empleados y a la comunidad universitaria general.

c) 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.

d) Esforzarse por aumentar la competencia y prestigio de los trabajadores y empleados universitarios en todas sus actividades.

Postulados

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.

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.

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 evitar 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 ingeniería en el ámbito de la seguridad informática

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, las cuales desempeñan diferentes actividades como son administradores, monitores, auditores, analistas, desarrolladores, y demás expertos con conocimientos en la rama independientemente del puesto que ocupen.

2. Actitud profesional

La excelencia técnica y ética del personal 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.

El personal encargado de la seguridad informática tienen la obligación de regir su conducta de acuerdo con 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 todo el personal encargado de la seguridad informática, en sus relaciones con el público en general, con quien presta sus servicios (usuarios) y con sus compañeros de trabajo.

El personal encargado de la seguridad informática debe 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

El personal encargado de la seguridad informática así como 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. De la misma forma deben cumplir los compromisos adquiridos por convicción propia.

Los encargados de la seguridad informática deben ~~de~~ respetar y hacer respetar su tiempo y el de los demás, predicar con el ejemplo, poseer espíritu de servicio, habilidad para comunicarse con los demás, actuar con cuida~~n~~do y de manera responsable para conservar la integridad física, emocional y económica de las personas.

4. Calidad profesional en el trabajo

El personal encargado de la seguridad informática, 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 personal responsable que defina estrategias para su generación, administración y difusión; por toda persona ajena o carente de conocimiento respecto a la informática, computación o sistemas computacionales, que sea falto de experiencia y capacidad necesaria para realizar éstas actividades de manera satisfactoria y profesional, por ningún motivo podrá llevar a cabo dicha actividad.

El personal encargado de la seguridad informática, es responsable de su propia actualización y capacitación profesional con la finalidad de que ésta sea de crecimiento permanente.

6. Práctica de la profesión

El personal encargado de la seguridad informática debe ~~-~~analizar cuidadosamente las verdaderas necesidades que puedan tenerse de sus servicios para proponer aquellas que más convengan dependiendo de las circunstancias.

Responsabilidad hacia la profesión

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

Todo el personal cuidará las relaciones que sostiene con sus compañeros de trabajo y colegas, buscando mejorar el ambiente de trabajo y fomentar el trabajo en equipo.

También 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, respetar, fomentar y adoptar los códigos de ética, contenidos en este documento.

2. Difusión y enseñanza de conocimientos

Los administradores, encargados, responsables y demás personal 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, encargados, y responsables 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

Es responsabilidad de los administradores, responsables y demás personal mantener actualizados todos los conocimientos inherentes a las áreas de su profesión así como participar en la difusión de estos conocimientos a otros miembros de la profesión.

Es responsabilidad del personal informarse permanentemente sobre los avances de la informática, la computación y los sistemas computacionales.

5. Evaluación de capacidades

Los administradores, responsables y las personas que laboran en sistemas dentro de la Institución deben autoevaluarse periódicamente con la finalidad de determinar si cuentan con los conocimientos suficientes para ofrecer un trabajo de calidad, de la misma forma en caso de tener 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, 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.

Evaluación a los alumnos

Los administradores, 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, de esta misma forma 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.

Al impartir un curso es importante llevar una supervisión del desempeño del alumno de tal forma que se pueda establecer si los bajos resultados son resultado del desempeño del alumno o del profesor o instructor.

Normatividad y lineamientos para el desarrollo de sistemas para la Facultad de Ingeniería

Normatividad y lineamientos para el desarrollo de sistemas

1. Importancia del usuario

El principal objetivo de los administradores, responsables 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 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 de todos los usuarios. Los administradores deben asegurarse del buen uso de los recursos informáticos evitando el mal uso de éstos, es decir, el uso para el que fueron planeados y autorizados.

3. Responsabilidad profesional

Los administradores 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 este 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, responsables 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, responsables, auditores 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, responsables y las personas que trabajan en el área de sistemas deben impedir el acceso a la información a personal sin autorización, ni utilizar la información confidencial de los usuarios o de la Institución para beneficio propio.

6.- Honestidad profesional.

Los administradores y las personas que trabajan en el área de sistemas tienen prohibido 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 y las personas que trabajan en el área de sistemas deben evitar participar en actos que se califiquen de deshonestos.

7. Evitar el uso de equipo de cómputo y programas de la Institución para beneficio personal

Los administradores y las personas que trabajan en el área de sistemas tiene prohibido =usar el equipo de cómputo para fines de esparcimiento que afecten su desempeño profesional, aun cuando tenga la autorización para utilizar el equipo, así mismo deben impedir que personas ajenas a la Institución puedan ingresar a las instalaciones y utilicen el equipo y los programas del software.

8. Trato adecuado a los usuarios y compañeros de trabajo

Los administradores 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 jefes, directivos, y responsables de las diferentes divisiones, áreas o departamentos deben dar a sus colaboradores el trato que les corresponde como profesionales y vigilarán su adecuado desempeño.

9. Finalización del trabajo

Al finalizar cualquier proyecto se debe cumplir cabalmente 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 y las personas que trabajan en el área de sistemas deben cuidar que el equipo de cómputo y los programas propiedad de la Institución se conserven en buen estado para su uso y aprovechamiento.

Al concluir el trabajo para el cual fue contratado, los administradores, responsables y las personas encargadas del desarrollo de sistemas en la Institución deben implementar los mecanismos necesarios para que se tenga la posibilidad de continuar haciendo uso de los programas de aplicación, así como de la modificación y mantenimiento de los mismos, aun cuando se ausenten por cualquier causa.

10. Desarrollo de sistemas

Las personas encargadas del desarrollo de sistemas en Institución tienen las siguientes responsabilidades y funciones:

- Determinar perfectamente el alcance del sistema y los requerimientos necesarios para su desarrollo.

- 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.

- Llevar a cabo las evaluaciones en las fechas determinadas y entregar los resultados en un tiempo adecuado que permita tomar decisiones.

- Dejar siempre documentado el sistema desarrollado, con todos los detalles necesarios, de tal manera que con su consulta se conozca el funcionamiento del sistema.

- Deben tener la capacidad para reconocer sus fallas en las revisiones, hacer correcciones y aclarar las dudas de quien solicitó el sistema, así como proponer posibles alternativas de solución.

- Comunicar los problemas que se les vayan presentando.

Universidad Nacional Autónoma de México

Facultad de Ingeniería

Apéndice 5

Guía para la elaboración de políticas de seguridad informática

Importancia de las políticas de seguridad en una organización

Las políticas de seguridad han venido a jugar un papel vital o de gran importancia, se han integrado rápidamente como una estrategia que forma parte de todo programa de seguridad que se implementa en cualquier organización alrededor del mundo.

El éxito de todo programa de seguridad se basa en que el documento donde se encuentran dichas políticas tiene como base alcanzar los objetivos y metas de la organización, es decir, ya que ellas están totalmente orientadas a la búsqueda de los diferentes objetivos, la misión y la visión que la organización tiene, de esta forma se pretende que este documento sea un apoyo para el alcance de las metas a corto, mediano y largo plazo.

Cada organización tiene una estructura interna, organigramas, procedimientos, necesidades, normas, reglas, información, instalaciones, necesidades, rubros, objetivos, etcétera, por lo que ninguna es exactamente igual a otra, es por esto que no es posible que varias organizaciones tengan exactamente las mismas políticas de seguridad.

El que una organización tenga metas, necesidades, objetivos similares no significa que deban tener políticas de seguridad iguales, este documento varía dependiendo de las necesidades, rubro, forma de trabajo, la forma en que se organiza la compañía, procedimientos internos, metas a corto, mediano y largo plazo, el tipo de instalaciones, el equipo que se maneja, la información que posee la organización entre otras muchas variables existentes que hacen que este documento sea único e intransferible.

Esta característica que hace a las políticas existentes en una organización ser únicas e intransferibles es porque el manejo de los bienes, procedimientos, personal, información, relaciones comerciales, clientes, rubro, etcétera, hacen que este documento no funcione de manera apropiada para alguna otra organización.

Las políticas de seguridad son una necesidad básica en toda organización que por lo general ocupa el último lugar en la gran larga lista de actividades dentro de ésta, es también en lo último que se piensa al diseñar instalaciones o implementar los sistemas necesarios para que la organización continúe sus actividades.

En ocasiones se considera contar con estas políticas, pero el trabajo que se requiere para desarrollar, implementar, mantener y vigilar su cumplimiento necesita que se desvíen valiosos recursos, por lo que se decide mejor contratar alguna empresa especializada para que ésta realice el trabajo.

Sin embargo, es importante que el personal de la organización que contrata los servicios de expertos para el desarrollo y capacitación acerca de las políticas de seguridad participe activamente en el desarrollo de este documento con el fin de que cumpla con las necesidades y requerimientos necesarios para el desarrollo de todas las diversas actividades que se realizan dentro de dicha organización.

Es importante aclarar que el documento debe considerar el trabajo colaborativo con otras organizaciones, es decir, deben existir políticas para el intercambio de información y accesos a recursos por parte de una organización con la cual colabore o se requiera que ésta preste algún servicio.

La subcontratación de una organización para realizar cualquier tipo de actividad, apoyo, colaboración o trabajo debe estar reglamentado y previsto dentro de las políticas de seguridad, las cuales regulan, delimitan y sancionan, de ser necesario, a las diferentes actividades, al acceso y al intercambio de bienes que se realicen cuando se requiera este tipo de trabajo colaborativo.

El que una organización cuente con políticas de seguridad implementadas es importante, ya que ayuda a la protección de la organización en general, pues los usuarios o el personal capacitados se concientizan sobre qué tan importante es la información, tanto la que se encuentra bajo su responsabilidad como la personal, el mejor aprovechamiento y manejo de las diferentes tecnologías de la información, entre otras.

El mantenimiento de los sistemas, la continuidad del trabajo, la disminución del factor error humano, involucrar a todo el personal de la organización y evitar errores que podrían causar daños de cualquier tipo, son acciones que las políticas de seguridad promueven para ofrecer un nivel apropiado de seguridad y así brindar protección a la organización y a los que laboran en ella.

La búsqueda de capacitación y mantenimiento de un programa en el cual las políticas de seguridad se implementen de manera apropiada, contarán con el principio para la obtención de un buen nivel de seguridad, sin embargo, es de suma importancia la persistencia y la continuidad, es decir, que exista un esfuerzo real por parte de la organización para dar continuidad a las políticas, lo cual también incluye el seguir trabajando en ellas, el monitoreo, auditorías internas, un programa de difusión y capacitación del personal de manera constante, revisiones y actualizaciones que promoverán y harán que la seguridad dentro de la organización tenga un nivel de apropiado.

Correcta redacción de las políticas de seguridad

Una buena redacción de las políticas de seguridad pude ser la manera de hacer que el usuario entienda de manera más fácil la importancia de la seguridad dentro de la organización y no como una capacitación más que debe tomar.

A continuación se mencionan algunas recomendaciones o principios para la redacción de las políticas de seguridad con el fin de que éstas puedan ser más efectivas.

1. Escoger una filosofía prohibitiva o permisiva

Existen dos filosofías que se pueden utilizar al redactar las políticas de seguridad, estos tipos de filosofías se usan con el fin de evitar los vacíos legales que puedan llegar a existir o presentarse por muy pequeños que sean, es decir, son una forma de acotar y restringir de manera efectiva las políticas, éstas son:

Prohibitiva

Este tipo de filosofía maneja que todo aquello que no está permitido explícitamente está prohibido.

Permisiva

En el caso de esta filosofía se maneja que todo aquello que no está prohibido de manera explícita está permitido.

De esta manera se evita la existencia de vacíos legales, los cuales pueden ser utilizados por los usuarios o personal que pueden aprovecharlos para obtener algún beneficio a costa de la organización o el excusar su comportamiento.

Existe un caso donde una mujer en los Estados Unidos demandó a una organización por un vacío legal existente en las políticas de seguridad donde se prohibía el acceso a páginas pornográficas a las que dicha mujer tuvo acceso. Éste fue un error en la redacción que fue

aprovechado por ella, quien ganó la demanda obteniendo una fuerte cantidad de dinero argumentando que era culpa de la organización el que ella hubiera accedido a esos sitios.[39]

Es importante mencionar que escoger una filosofía no sólo es el hecho de optar por alguna de las dos filosofías ya explicadas, es hacer énfasis en que el usuario también es responsable de sus acciones, es decir, que parte de la responsabilidad descansa en el usuario, de esta manera se acotan y limitan las acciones que la organización le permite o prohíbe al usuario.

2. **Establecer lo que se debe o necesita hacer y por qué, pero no el cómo**

Dejar libre la forma de implementar la seguridad, teniendo en cuenta que se deben cumplir con ciertas características y configuraciones dictaminadas por las políticas de seguridad, las cuales deben ser respetadas, hace que el personal y los usuarios puedan disponer o escoger de entre una gran variedad de herramientas, dispositivos, marcas, y distintas opciones, las cuales se adapten mejor a sus recursos y necesidades para implementar la seguridad.

Que las políticas ofrezcan a los usuarios la opción de escoger ¿con qué? y ¿cómo? implementar la seguridad siempre y cuando cumplan con lo estipulado por ellas, permite que se pueda trabajar, colaborar, utilizar y evaluar una gama de equipos, así como aprovechar algunos que ya se tienen sin necesidad de comprar nuevos con ciertas características que probablemente no son lo mejor para el trabajo o las actividades que se realizan, en otras palabras, es el aprovechar al máximo los recursos que se tienen sin necesidad de alterar el tipo de equipos que utilizan, que prefieren o con los que trabajan.

3. **Tener en mente a quién van dirigidas y usar un lenguaje adecuado**

Tener claro quién es el responsable de lo que es importante, ya que la asignación de responsabilidad debe estar sin ambigüedades con el fin de que no exista duda acerca de esto, los usuarios deben poder entender y comprender de manera plena, adecuada y bien definida sus responsabilidades y hasta dónde llegan éstas. Deben poder responder a las siguientes preguntas de manera sencilla:

[39] David Jarmon, A preparation guide to information security policies http://www.sans.org/reading_room/whitepapers/policyissues/preparation-guide-information-security-policies_503

¿Quién es el que implementa la política?

¿Quién es el encargado del mantenimiento, monitoreo, verificación y auditorías?

¿Quién es el administrador y de qué es responsable?

¿Cuáles son las responsabilidades de los usuarios?

Cuando un usuario sabe quién es el responsable y de qué, si éste requiere ayuda o asesoría puede saber con quién se tiene que ir y qué procedimientos debe realizar ante este tipo de situaciones, esto favorece que exista una mejor y más pronta reacción a los incidentes.

4. Ser positivo y evitar emplear la palabra "NO"

"People respond better to positive statements than to negative ones."[40] Esta frase en inglés puede explicarse en español en el siguiente párrafo:

La gente responde de mejor manera a las declaraciones formuladas de manera positiva, evitando la palabra "NO" en el documento. Las personas tienen mejor aceptación hacia las declaraciones de manera afirmativa.

5. Uso de oraciones sencillas y concretas

El uso de declaraciones concisas hace que el lector encuentre la información que necesita, crea desagrado o disconformidad por parte de éste leer declaraciones muy largas, ya que esto hace que el usuario pierda interés, además de que si el lenguaje utilizado es demasiado técnico o con terminología abstracta, la lectura se hace muy pesada para el usuario.

[40] S, Garfinkel, G. Spafford, Practical Unix & Internet Security, 3rd edition, pág.48

Lo que los lectores no entienden lo ignoran, es decir, al no comprender lo que están leyendo, los usuarios hacen caso omiso, pierden interés y se desaniman, pensando que el tema es demasiado complejo y complicado, que requiere invertir demasiado tiempo para entender, es por esto que se recomienda el uso de oraciones sencillas y concretas para atrapar la atención del usuario.

Es importante mencionar que no todo el personal que labora en una organización tiene el mismo grado de estudios y que es necesario que todo el personal conozca las políticas, es por esto que deben ser sencillas, es decir, que las oraciones se estructuren empleando sujeto, verbo y complemento, para que la declaración sea clara y transparente y no haya lugar a ninguna duda ya que el propósito es realizar un documento que pueda ser accesible, fácil de leer y muy claro.

6. Utilización de lenguaje adecuado

Las políticas deben ser escritas en un lenguaje adecuado, como se ha mencionado, debe ser sencillo y concreto, evitar usar lenguaje técnico. Sin embargo, se debe guardar un balance con respecto al lenguaje, debe ser accesible pero a su vez formal, ya que si el lenguaje utilizado es demasiado informal, el usuario no lo verá como un documento serio y lo ignorará, sin embargo, debe ser a la vez no demasiado formal usando lenguaje que sólo los expertos en la materia puedan entender ya que tendría el mismo efecto y lo ignorarían.

Es por eso que el lenguaje debe ser amigable para el usuario sin dejar de ser formal y perder importancia ante el usuario, siendo ésta la mejor combinación.

7. Formato unificado

Al igual que el uso de lenguaje apropiado, el documento que contiene las políticas de seguridad debe tener un solo formato, es decir, tipos de letra, viñetas, subtítulos, títulos, espacios, etcétera, para darle más formalidad e importancia.

Contar con un solo formato facilita la búsqueda de información en el documento lo que hace que al usuario se le facilite el trabajo, además de poder identificar conceptos, apartados, títulos, subtítulos, etcétera.

8. Uso de títulos efectivos

El uso de títulos efectivos es importante para poder transmitir la idea general, el contenido del apartado o parte de un documento, mediante un título es posible encontrar la información de manera más rápida lo que motiva al usuario a emplear el documento ya que no tiene que leer o hacer otra lectura nuevamente cuando requiere alguna información específica, sólo tiene que encontrar los títulos o subtítulos para saber acerca del documento e ir directamente a la parte que le interesa.

Poder transmitir información contenida en un apartado puede ser de gran utilidad al momento de alguna emergencia o cuando se requiere una pronta acción, lo que se facilita con el uso de los títulos efectivos.

9. Fomentar la capacitación constante

Que los usuarios tengan una capacitación constante forma parte de los deberes que el personal de toda organización debe tener, ya sea sólo realizar pláticas para recordar la importancia de las políticas, mostrar el avance y los diferentes cambios en ellas y en la organización. De la misma manera se debe tener en cuenta que con el avance del tiempo se desarrollan nuevas herramientas, nuevas amenazas, riesgos, técnicas y nueva información.

Una formación constante refleja lo importante que es el personal para la organización, la confianza que la organización tiene en la capacidad del personal, es por esto que se busca capacitar y enseñar a todo el personal que será el que realice las diferentes actividades que se requieren para que la organización continúe con el trabajo que viene realizando de manera ininterrumpida.

El hecho de que el personal esté capacitado es una ventaja para la organización ya que tendrá y manejará de una manera más eficiente las diferentes crisis, incidentes así como la resolución de los problemas que se presenten.

10. Asignación de un dueño a todo recurso informático

Todo recurso informático, es decir, los recursos y bienes dentro de la organización, debe ser asignado o puesto bajo la responsabilidad de alguien, debe existir un responsable que cuide, proteja y esté al pendiente de él.

La existencia de un responsable es una manera de delegar responsabilidad para que no todo esté concentrado en una sola persona, sino que existan muchas personas realizando trabajo en conjunto, lo que ayuda a la protección de los diferentes bienes, recursos, su manejo apropiado y mejor aprovechamiento.

11. El factor error humano

Las políticas de seguridad no son reglas que buscan castigar al usuario en caso de cometer algún error, el hecho de que el usuario cometerá errores está contemplado, es decir, las políticas buscan que el usuario no cometa errores por medio de la capacitación y la experiencia, sin embargo, que los usuarios cometan errores es algo normal.

Cuando un usuario cometa por error algún incidente o se vea envuelto en algún incidente de seguridad de manera intencional, éste debe ser tratado con respeto. El que un usuario cometa errores es normal, sin embargo, existe una diferencia en cometer un error y el realizar un ataque.

En caso de que un usuario pueda ser involucrado en un incidente debe ser tratado de manera discreta, respetuosa y ética respetando la información o bienes que se estén auditando, teniendo en cuenta que se puede encontrar mucha información personal que no se debe incluir en el reporte ya que sería una invasión a la privacidad del usuario y auditando sólo lo que es requerido para este efecto.

Cometer un error no debe ser causa de severidad con el usuario, sin embargo, que se haya realizado un ataque contra los bienes de la organización debe ser investigado de manera cuidadosa y de manera discreta, ya que el que un usuario esté involucrado no significa que éste haya realizado el ataque, por lo que es necesario hacer una investigación y no asumir hechos hasta que se haya llegado a una conclusión sustentada por pruebas generadas por una auditoría, un análisis forense o una investigación.

Se debe tomar en cuenta que el usuario es un ser humano propenso a cometer errores y como tal los cometerá y que debe ser capacitado para que evite cometerlos nuevamente, sin embargo, cuando los cometa de manera continua, de manera consciente, con alevosía o viole la normatividad de manera constante debe ser sancionado conforme a las políticas de seguridad.

12. Especificar a quién van dirigidas

Especificar a quién van dirigidas, de quién es la responsabilidad o quién es el encargado de qué, es importante, ya que hacer que las políticas sean lo más claras para el personal ayuda a que entienda en su totalidad sus responsabilidades y límites, es decir, qué es lo que tiene y debe hacer, de la misma manera hasta dónde llega su responsabilidad con el fin de que cumpla con su deber.

De esta manera no tiene mayor ni menor carga en cuanto a su responsabilidad sino sólo la que le corresponde, es decir, todo usuario sabe de manera clara y precisa qué es lo que tiene que hacer y cómo se debe desempeñar.

Tener reglas, guías o recomendaciones para la realización de una mejor redacción es sumamente útil ya que las políticas de seguridad así como los documentos que las conforman serán asimiladas y entendidas de una mejor manera por los usuarios que las leen, de esta forma con este tipo de recomendaciones se busca que sean más efectivas, que los usuarios consideren este documento con la seriedad que debe tenerse por sí mismo, que sea consultado cuando se requiera y que los usuarios lo vean como un documento de fácil acceso para aclarar sus dudas, como un apoyo para el desarrollo de sus actividades.

Es indispensable tomar en cuenta otras consideraciones al momento de redactar o revisar las políticas de seguridad de una organización, estos puntos son una parte importante de las políticas como son la experiencia sobre incidentes de seguridad, el seguimiento de los incidentes, la ética del personal, así como la importancia de la buena capacitación.

Puntos importantes a considerar en las políticas de seguridad

Existen puntos a considerar al hablar de políticas de seguridad, los cuales darán mayor cohesión y mejorarán los resultados, teniendo en mente estos puntos ayudarán a entender de

una mejor manera el funcionamiento y será de gran apoyo para las revisiones, cambios, sugerencias así como a la implementación de las mismas.

a) Ventajas asociadas a un buen documento

Un documento bien estructurado y redactado ayuda a la adquisición de equipo y software que requiere la organización para un mejor desempeño, así como la pronta acción de las autoridades en caso de alguna situación. Permite también tener procedimientos para eventualidades, conflictos, ampliaciones en la organización, tratamiento de la información y el acceso a ella.

Facilita la auditoría, el control de la información y el uso de los recursos con los que cuenta la organización, permite que los encargados o administradores de los distintos laboratorios puedan administrar y asignar equipos a los usuarios según sus necesidades, facilita que los encargados puedan mejorar los servicios que se prestan dentro de la organización con el fin de mejorar el desempeño al momento de trabajar, lo cual representa una clara ventaja para todos los usuarios.

En cuanto al software, es preciso que la organización cuente con los programas necesarios para que los usuarios puedan desarrollar sus actividades. Sin embargo, las políticas de seguridad deben regular la instalación, uso y acceso, ya que no todos los usuarios tienen los mismos privilegios, mismos que son asignados de acuerdo con sus actividades y responsabilidades.

Las políticas en este caso juegan un papel de suma importancia al regular el uso de los programas, el acceso a la información, el uso de los recursos, la instalación de programas, el mantenimiento, el acceso a bitácoras de los sistemas, el monitoreo de la red, la configuración de los equipos, la actualización de los sistemas con los que se cuenten, el acceso a las distintas áreas dentro de la organización, el prestigio de la organización, así como proteger a los usuarios y su información personal.

En ocasiones parece ser que las políticas de seguridad no son tan importantes, que las personas no poseen información que pueda ser sensible o de gran valor, que los equipos están protegidos y que no es necesario ser tan formal; sin embargo, hoy en día la información que se comparte por medio de los diversos medios de transmisión, del llenado de formatos, o simplemente al platicar con una persona (ingeniería social), representa un agujero de seguridad, ya que no se sabe cuáles sean las verdaderas intenciones. La información que se proporciona todos los días puede comprometer a la organización.

Por todo lo anterior, es de suma importancia que se capacite a los usuarios con la finalidad de que éstos puedan evitar dar información que aparentemente es inservible o sin relevancia, pero que puede ser utilizada para otro tipo de propósitos, los cuales puedan dañar a los usuarios y a la organización.

Frecuentemente, cuando un usuario es capacitado puede que ocurran 3 casos principalmente:

Caso 1

El usuario es capacitado adecuadamente concientizándolo acerca de la importancia de la seguridad, de su información, por esto el usuario crea una conciencia no sólo dentro de la organización sino en su vida personal.

Caso 2

El usuario está mal capacitado, por lo que no le da la importancia requerida a su información lo que a futuro puede terminar en un incidente de seguridad.

Caso 3

El usuario es capacitado erróneamente por lo que actúa de manera paranoica, pensando que todas las personas están intentando obtener información con el objetivo de hacer algún daño.

No sólo es importante avisar y advertir al usuario sobre los peligros que existen, sino que es primordial que él sepa proteger su información, así como compartirla sin que esto le genere un sentimiento de paranoia.
Se sabe de antemano que no existe ningún sistema seguro, es decir, no se puede afirmar que se está 100% seguro, no importando qué tan buenos sean los mecanismos de seguridad. Se sabe también que con el tiempo se tienen incidentes de seguridad provocados por diversas razones como son, la evolución de los sistemas, la mala implementación, trabajos internos (incidentes de seguridad provocados por personal de la propia organización), el cambio de tecnologías, la actualización de los equipos y en ocasiones por errores de los propios usuarios.
Por esto último, es de suma importancia que las políticas de seguridad estén actualizadas, bien redactadas, que sea un documento que esté a la mano, que pueda ser consultado y que

los usuarios las conozcan con la finalidad de que cuando surja algún incidente de seguridad se pueda reaccionar de manera adecuada para minimizar o reparar el daño causado.

b) Viabilidad de la implementación de las políticas

Algunas veces en las organizaciones, el departamento encargado de la seguridad junto con el comité de seguridad redactan políticas que son necesarias para ella, sin embargo, que éstas puedan ser implementadas o llevadas a la práctica es sumamente difícil ya que puede ser que el personal no tenga la experiencia necesaria para hacerlo.

Tomar en cuenta las limitantes para poner una política en práctica es un punto importante, ya que hay que considerar realizar cambios, capacitar al personal o contratar personal calificado, es decir, hay diversas variantes que son importantes y que influyen al tomar decisiones como la experiencia, el tiempo, contar con los recursos necesarios y con el conocimiento necesario.

Como se ha manejado a lo largo de este capítulo, las políticas de seguridad las políticas de seguridad buscan el aprovechamiento de todos los bienes y recursos de la organización, sin embargo, cuando se necesite el uso de alguna tecnología nueva que después de analizarla cuidadosamente sea indispensable que se implemente, es importante considerar cómo se llevará a cabo y si es viable que se haga tal implementación.

c) Factores involucrados en la implementación

La existencia del personal para que las políticas de seguridad puedan ser implementadas es importante ya que no sólo consiste en el uso de las tecnologías dentro de la organización sino contar con suficiente personal que esté disponible para que las haga respetar, que las lleve a cabo, que ayude al mantenimiento, apoyo, vigilancia, monitoreo y seguimiento de los incidentes.

El seguimiento de las políticas de seguridad consiste en brindar apoyo a los departamentos que hayan solicitado ayuda, la investigación de incidentes, análisis forense, auditoría, la realización de reportes, la difusión de las políticas, apoyo para la capacitación del personal en general, actualización de las políticas, realización de sugerencias, actualización de portales para informar a los usuarios y el seguimiento de los cambios dentro de la organización, actividades que deben ser desempeñadas por personal ético y capacitado para este tipo de actividades.

Es indispensable tener conciencia de que con el tiempo existen cambios dentro de la organización y que es importante darles un seguimiento apropiado, algunos cambios se presentan en el personal que se integra o ya no labora más en la organización, las nuevas relaciones o colaboraciones de trabajo con otras organizaciones, la necesidad de otorgar nuevos privilegios o el cambio de algunos de ellos, entre muchos otros.

Por lo anterior es necesario concluir de manera formal cualquier tipo de colaboración, siguiendo las políticas de seguridad al solicitar pases de acceso, credenciales, notificar al personal de vigilancia, la entrega de todo tipo de bienes confiados al personal, llaves, de la misma manera cancelar o dar de baja todo tipo de cuentas en equipos y servidores, correo electrónico, o cualquier otro tipo de recurso confiado durante la colaboración con el fin de evitar algún tipo de incidente.

La difusión que debe existir dentro de cualquier organización no sólo es importante para la gente de seguridad o para los directivos y sus equipos. La difusión acerca de este tipo de programas es importante para todas las áreas por lo que es necesario que ésta sea adecuada y llegue a todo el personal que labora y colabora en la organización.

Tener información disponible sobre la organización, sus cambios, aclaraciones, la existencia de asesorías, informes y reportes sobre incidentes, vulnerabilidades que se hayan detectado, fallas en la seguridad, ayudan a la prevención de incidentes que puedan gestarse.

Universidad Nacional Autónoma de México

Facultad de Ingeniería

Apéndice 6

Carta del ISSSTE proporcionada por el médico capacitado

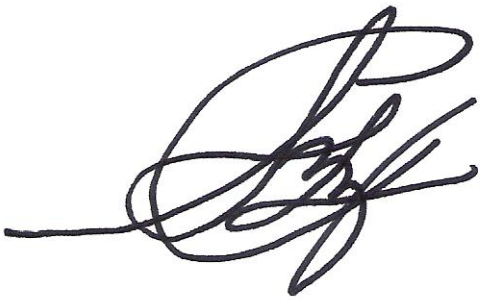
Hospital Regional "Lic. Adolfo López Mateos"
Av. Universidad # 1321
Col. Florida, Delegación Álvaro Obregón
C.P. 01030, México, D.F.
www.hospitallopezmateos.org

Por medio de esta carta se hace constar que la capacitación realizada a uno de los médicos de esta unidad acerca de la importancia que tienen las políticas de seguridad informática y como es que éstas y una capacitación adecuada son una herramienta sumamente útil para la prevención y corrección ante los incidentes informáticos.

La capacitación con respecto a la propagación, comportamiento y consecuencias del malware que se almacena y se propaga por medio de las memorias y dispositivos de almacenamiento USB (memorias flash USB), las cuales son los causantes de diversos problemas entre los cuales se encuentran las fallas en los equipos de cómputo, como son la destrucción y pérdida de información, diversas fallas en los sistemas operativos, entre las que se encuentran la disminución considerable del desempeño del equipo y las fallas en el reconocimiento de los dispositivos de almacenamiento.

Como resultado de la capacitación hubo una clara disminución de este tipo de incidentes en más de un 60%, lo cual permite que los recursos que se tienen sean aprovechados y destinados al trabajo y a las actividades pertinentes.

Unidad de patología
Médico capacitado: Dr. Carlos Sánchez Lara



Universidad Nacional Autónoma de México

Facultad de Ingeniería

Apéndice 7

Reporte de incidente de seguridad informática

Reporte de incidente de seguridad informática[41]

Un incidente de seguridad se define como el acontecimiento de un suceso inesperado que pretende obtener, dañar, destruir, o realizar cualquier tipo de modificación a un bien o activo de una organización, siendo éste exitoso o no para la obtención de un beneficio de manera ilícita; así como cualquier violación a las políticas de seguridad establecidas.

El objetivo de la realización de un reporte es permitir una respuesta apropiada para la solución y corrección de cualquier tipo de incidente que se presente con la finalidad de evitar que se vuelva a presentar, con esto se busca minimizar la ocurrencia de incidentes que interrumpan servicios, trabajos y actividades que se desempeñan en la Facultad de Ingeniería. De esta misma forma se quiere dar un seguimiento y un manejo apropiado a los diversos incidentes que se presenten.

Por lo anterior se requiere el llenado del formato anexo con la mayor seriedad y de la mejor manera posible, el cual deberá presentar a la brevedad posible con el administrador o responsable inmediato. En caso de no conocer algunos términos o requerir asistencia para el llenado de este formato el administrador de red le ayudará a llenar dicho formato, o escriba un correo electrónico al Departamento de Seguridad en Cómputo (DSC).

Responsable:
Teléfonos:
Correo electrónico:

[41] Este reporte fue basado en un formato de la Universidad Nacional de Lujan, Argentina.

Reporte de incidente de seguridad informática

Fecha y hora del llenado del reporte:

Datos personales

Llene esta parte con los datos personales de la persona que está llenando el reporte.

Nombre Completo:	
División:	Departamento:
Correo electrónico:	
Teléfono interno:	Teléfono particular:

Información sobre el incidente

La información que usted proporcione acerca del incidente ayudará a dar solución de una mejor y más rápida forma.

Fecha y hora en que se suscitó el incidente:

Marque con una cruz las opciones aplicables al incidente

	Uso indebido de información.		Cambio en la configuración del equipo.
	Uso inadecuado de recursos informáticos.		Ataque o infección de malware, o código malicioso (virus, gusanos, troyanos, etc.)
	Divulgación no autorizada de información personal.		Acceso o intento de acceso a un sistema informático.
	Acceso o intrusión física.		Pérdida o destrucción no autorizada de información.
	Ingeniería social.		Interrupción en los servicios de red.
	Uso indebido de correo electrónico institucional.		Anomalía o vulnerabilidad técnica del software.
	Modificación de información de un sitio o página.		Robo o pérdida de equipo.

	Robo o pérdida de información.		Amenaza o acoso por medio electrónico
	Modificación, instalación o eliminación de software.		Otro no contenido:

Descripción del incidente

Brevemente describa y proporcione información acerca del incidente				
Detección del incidente				
Describa brevemente cómo se detectó el incidente				
El incidente aún está en progreso	Sí		No	
Tiempo aproximado de duración del incidente:				

Información sobre el activo o bien afectado

Si conoce la información, llene los campos acerca de la información concerniente al bien afectado.

Número de inventario:

Descripción del activo o bien:				
Localización física:				
Descripción breve de la información en cuestión:				
¿Existe una copia o respaldo de la información?	Sí		No	
¿El recurso afectado tiene conexión con la organización?	Sí		No	
¿El recurso afectado tiene conexión a internet?	Sí		No	
Sistema Operativo:				

En caso de intrusión llene esta parte.

Nombre(s) de la(s) máquina(s) comprometida(s).
Sistema operativo indicando versiones:

Indique las acciones que se tomaron antes o después de la intrusión:		
Usuarios comprometidos:		
Existen otras máquinas afectadas por la intrusión. Especifique.		
¿Se ha contactado a otras organizaciones? Especifique.		
Si se autoriza o no al DSC para suministrar información a otras organizaciones que colaboren para la solución e investigación del incidente.	Sí	No
Nombre completo y firma del responsable que autoriza.		

Otros contactos

Nombres e información de contacto de otras personas que pueden tener información para asistir en la investigación del incidente:

Nombre:	
Correo electrónico:	Teléfono:
Nombre:	
Correo electrónico:	Teléfono:

Glosario

Antivirus

Programa cuyo objetivo es detectar, prevenir y proteger la integridad de los programas y datos contenidos en un equipo de cómputo de todo tipo de malware como son los virus informáticos, los gusanos, troyanos, software espía, entre otros.

Back-door

Código oculto que proporciona una forma para tener acceso no autorizado a un programa, servicio, datos, módulo o sistema completo que sólo es conocido por la persona que lo realizó.

Bloqueo de e-mails

Es una estrategia que tiene como objetivo filtrar los correos electrónicos no deseados o no solicitados.

Bluetooth

Estándar de transmisión de datos inalámbrico vía radiofrecuencia de corto alcance (10 metros) que permite la comunicación entre diferentes dispositivos.

CACFI

Comité Asesor de Cómputo de la Facultad de Ingeniería, el cual es el órgano encargado de promover y asesorar el óptimo desarrollo informático de la Facultad de Ingeniería así como procurar la normatividad, la estandarización y en general, buscar mecanismos de racionalización y optimización en materia de cómputo.

CERT

Computer Emergency Response Team o Equipo de Respuesta a Emergencias Informáticas, es la organización que se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo, así como publicar información respecto a vulnerabilidades de seguridad, alertas y realizar investigaciones en el área de cómputo y así ayudar a mejorar la seguridad de los sistemas informáticos.

Código Malicioso

Término utilizado para nombrar cualquier código o parte de un programa que tiene la finalidad de dañar un sistema o realizar acciones no autorizadas por el usuario.

Compresión de datos

Proceso por el cual se busca la reducción en el volumen de la información (menor cantidad de espacio de almacenamiento) con el fin de poder transportar, transmitir, almacenar, grabar o procesar dicha información de una manera más sencilla y eficiente.

Crackers

Criminales cibernéticos, personas con intenciones destructivas o delictivas cuyas actividades principales son la de introducirse o quebrantar las políticas de seguridad de un sistema con la intención de robar, dañar u obtener algún beneficio propio.

DSCFI

Departamento de Seguridad en Cómputo de la Facultad de Ingeniería el cual está encargado de brindar la máxima seguridad informática a las redes de cómputo de la Facultad de Ingeniería.

Efectividad

Es la capacidad de alcanzar, adquirir o lograr un objetivo claro y bien definido.

Eficiencia

Es el uso apropiado de los recursos, procurando el uso mínimo de éstos para conseguir y lograr un objetivo.

FI

Facultad de Ingeniería organización encargada de la formación de ingenieros.

Firewall

Programa o parte de un sistema diseñado para controlar, limitar y filtrar el acceso, la transmisión y comunicación en una red de datos.

Gusanos

Es un tipo de malware que se replica y se propaga automáticamente a través de redes, dispositivos de almacenamiento y diversos equipos de cómputo. Algunos de ellos sólo buscan alojarse en un equipo sin crear o hacer daño aparente, otros buscan dañar o destruir archivos.

Hackers

Término asociado a personas que poseen conocimientos avanzados sobre diversas áreas de las tecnologías de la información, la ingeniería, seguridad informática y el cómputo. Estos expertos tienen la capacidad y las habilidades de entrar en sistemas, modificar hardware, programar, diseñar aplicaciones y herramientas.

IEC

International Electrotechnical Commission o Comisión Electrotécnica Internacional, es la organización que prepara y publica normas internacionales para todas las tecnologías eléctricas, electrónicas y afines

Incidente

Evento que atente contra la confidencialidad, integridad y disponibilidad de la información así como de los recursos informáticos.

Ingeniería social

Acción o conducta social destinada a conseguir información de las personas cercanas a un sistema por medio de habilidades sociales que explotan vulnerabilidades como inocencia, desconocimiento, confianza o credulidad.

ISM^3 (también conocida como ISM3)

Information Security Management Maturity Model, es una iniciativa internacional sin fines de lucro dedicada a definir estándares técnicos y éticos aplicables en sistemas de gestión de la seguridad de la información.

ISO

International Organization for Standardization (organización internacional para la estandarización), es un organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

Lammers

Persona que cree o dice tener un vasto conocimiento, sin embargo, no posee dicho conocimiento.

Malware

Término que se le ha otorgado a todo aquel software que daña, destruye, afecta el rendimiento o realiza actividades no autorizadas o sin el conocimiento del propietario del equipo. Algunos ejemplos de malware son: virus, gusanos, rootkits, backdoors, códigos maliciosos, troyanos entre otros.

Peer-to-peer (P2P)

También llamada red entre iguales, la cual es una red de computadoras en la que todas las integrantes de dicha red tienen las mismas capacidades y cualquiera de las partes puede iniciar comunicación, en dicho modelo no existe como tal un cliente y un servidor.

Phishing

Grupo de técnicas destinadas al engaño de usuarios de servicios mediante las cuales se duplica algún sitio, se monta una página parecida o igual a la original en el Internet con el fin obtener información.

Phreaking

Término asociado con el estudio, comprensión, funcionamiento y uso de las tecnologías vinculadas con los dispositivos telefónicos y las comunicaciones.

Políticas de seguridad en cómputo (PSC)

Conjunto de norma, reglamentos y recomendaciones que están enfocados en proteger los activos relacionados con el cómputo en una organización.

Políticas de seguridad informática (PSI)

Conjunto de normas, reglamentos y recomendaciones que buscan proteger todos los activos de una organización.

Riesgos informáticos

Es la probabilidad de que una falla, ataque, amenaza o vulnerabilidad se presente y que esta afecte de alguna manera a de los sistemas informáticos, dispositivos, o el contenido en ellos.

Rootkits

Herramientas usadas para esconder procesos, aplicaciones y archivos que permiten al intruso mantener el acceso o el control del sistema para realizar diversas actividades sin ser detectados por el usuario.

SANS

SysAdmin, Audit, Network, Security (Administración de Sistemas, Auditoría, Redes y Seguridad), es una organización dedicada a la capacitación sobre temas de la seguridad informática.

Scam

Correo electrónico o e-mail fraudulento con la única finalidad de estafar económicamente a la víctima mediante un engaño, generalmente utilizando ingeniería social

Spam

Es el uso y envío de todo tipo de mensajes electrónicos (correo electrónico, sitios web, telefonía, fax, televisión e Internet) no solicitados de manera indiscriminada.

Script Kiddies

Término usado para describir personas que utilizan aplicaciones, programas y scripts desarrollados por otros para atacar sistemas de computadoras y redes.

Scripts

Es un programa generalmente simple para la realización de diferentes tareas.

Sistemas de Gestión de la Seguridad Informática (SGSI)

Conjunto de políticas de administración de la información asociado principalmente a la ISO/IEC 27001.

Spyware

Programa de computadora que recolecta información de un equipo de cómputo sin el consentimiento del usuario, esta información es enviada al atacante quien podría usarla para realizar fraudes financieros, robo de identidad o algún otro tipo de ataque.

SSID

Service Set IDentifier, (servicio de identificación) el cual es un identificador o nombre asignado para identificar una red inalámbrica.

Técnicas criptográficas

Procedimientos, normas o conjunto de reglas cuyo objetivo es el de robustecer el cifrado de datos o información.

Troyanos

Programa cuya función es el ocultar o disfrazar a otro programa que busca realizar alguna actividad sin conocimiento o autorización por parte del usuario o propietario.

USB

Abreviación de Universal Serial Bus (bus universal en serie), es un puerto que sirve para conectar periféricos a un ordenador.

USB flash drive

Dispositivo de almacenamiento el cual consta de una memoria flash (o memoria no volátil), integrada a un puerto USB.

Virus informáticos

Es un tipo de malware cuyo objetivo principal es el dañar o destruir archivos o datos.

Vulnerabilidad

Es una falla o debilidad en un sistema (hardware o software), a la hora de la implementación, configuración o en el diseño.

WIFI

Es un término asociado con redes inalámbricas y los estándares 802.11

ZigBee

Es el nombre asociado al protocolo IEEE 802.15.4 de redes inalámbricas.