



# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

---

---

**FACULTAD DE INGENIERÍA**

**División de Ingeniería Eléctrica**

**Actualización y Difusión de las Políticas  
de Seguridad de Cómputo de la Facultad  
de Ingeniería.**

**TESIS PROFESIONAL**  
para obtener el título de  
**INGENIERO EN COMPUTACIÓN**

**PRESENTA**  
**MOISÉS ALVARADO HERMIDA**  
**GIBRÁN TORÍZ DÍAZ CONTRERAS**

**DIRECTORA DE TESIS**  
**M.C. CINTIA QUEZADA REYES**

**MÉXICO, D.F. 2011**





Universidad Nacional  
Autónoma de México

Dirección General de Bibliotecas de la UNAM

**Biblioteca Central**



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

## Agradecimientos

A mis padres de quien siempre voy a estar agradecido por todo el amor que me han dado, el gran apoyo que siempre he tenido y los sacrificios que han hecho por mí y mis hermanos.

A mis hermanos Emmanuel y Vania así como también a Lorena con quienes siempre he podido contar y sé que siempre tendré a quién acudir en ustedes.

A mi tío que me brindó su amistad y ha sido un ejemplo para mí.

A mi asesora M.C. Cintia Quezada Reyes así como a toda la plantilla de profesores de los cuales he tenido la oportunidad de aprender de su conocimiento y experiencia.

Además quiero expresar mi agradecimiento, pero sobre todo mi orgullo por ser parte de la UNAM, he tenido la fortuna de estar en áreas de gran competitividad y siempre he tratado de representar a la UNAM con dignidad y personalidad.

Gibrán Toríz Díaz Contreras

A mi alma Mater que me ha dado la oportunidad de estudiar y pertenecer a ella.

A mis padres Venancio Alvarado Escobar y Esther Hermida Mayoral, a mi tío Saturnino Hermida Mayoral así como a mis hermanos Abraham y Esther.

A los académicos y profesores que con su apoyo y trabajo contribuyeron a mi formación pero en especial a:

A mi asesora de tesis M.C. Cintia Quezada Reyes

A mi tutora Ing. Maricela Castañeda Perdomo

Al Dr. Rogelio Alcántara Silva

Moisés Alvarado Hermida

# Índice

Introducción .....	7
--------------------	---

## Capítulo 1

Fundamentos Teóricos .....	11
1.1 Conceptos básicos de seguridad informática.....	14
1.2 Servicios Informáticos.....	21
1.3 Mecanismos de Seguridad.....	23
1.4 Gestión de contraseñas .....	26

## Capítulo 2

Políticas de Seguridad.....	29
2.1 Definición de política de seguridad.....	33
2.2 Definición de política de seguridad informática.....	36
2.3 Objetivos de una política de seguridad.....	38
2.4 Definición y objetivos de las buenas prácticas .....	42

## Capítulo 3

Importancia de las políticas de seguridad .....	45
3.1 Importancia de las políticas de seguridad en una organización.....	49
3.2 Importancia de revisar periódicamente las políticas de seguridad .....	51
3.3 Correcta redacción de las políticas de seguridad.....	56
3.4 Puntos importantes a considerar en las políticas de seguridad .....	62
3.5 Las buenas prácticas y las políticas de seguridad.....	66

3.6 Plan de contingencia .....	68
<b>Capítulo 4</b>	
Estándares a considerar para la redacción de las políticas de seguridad .....	75
4.1 Definición de estándar .....	77
4.2 Estándares que existen respecto a las políticas de seguridad .....	79
4.3 Estándares a considerar en las políticas de la Facultad de Ingeniería .....	86
4.4 Revisión de las políticas de seguridad informática de la Facultad de Ingeniería .....	90
4.5 Estandarización de las políticas de seguridad informática de la de la Facultad de Ingeniería.....	93
4.6 Redacción de las políticas de seguridad informática de la FI.....	95
<b>Capítulo 5</b>	
Revisión de las políticas de seguridad informática de la Facultad de Ingeniería .....	96
5.1 Por qué es importante una revisión de las políticas de seguridad informática de la Facultad de Ingeniería .....	102
5.2 Actualización de las políticas de seguridad informática de la FI .....	106
5.3 Propuesta para la modificación de las políticas de seguridad informática de la FI.....	107
5.4 Reestructuración y redacción de las políticas de seguridad informática .....	110
<b>Capítulo 6</b>	
Difusión de las políticas de seguridad informática de la Facultad de Ingeniería.....	112
6.1 Propuestas para una mejor difusión.....	116
6.2 Actualización periódica de las políticas de seguridad informática de la Facultad de Ingeniería.....	125
<b>Conclusiones</b> .....	130

## **Apéndices**

Entrevista a los encargados de la seguridad y las redes de la Facultad de Ingeniería.....	134
Encuesta .....	142
Resultados de la encuesta aplicada a alumnos de la Facultad de Ingeniería.....	145
Políticas de seguridad en cómputo para la Facultad de Ingeniería .....	153
Guía para la elaboración de políticas de seguridad informática.....	238
Carta del ISSSTE proporcionada por el médico capacitado .....	252
Reporte de incidente de seguridad informática .....	254
<b>Glosario</b> .....	260
<b>Bibliografía</b> .....	269

# Introducción



**Propuesta de Revisión, Actualización y Difusión de Las Políticas de Seguridad en Cómputo para la Facultad de Ingeniería.**

## **Introducción**

Las Políticas de Seguridad Informática (PSI), son un documento que busca el proteger y conservar los activos de todo tipo de recursos e información de una organización, no obstante aun cuando este documento es de suma importancia, no tiene el peso que debería tener en la organización por el hecho de tener una idea equívoca acerca de que estas requieren una inversión enorme y constante de recursos que se perderán al no ser esta una inversión que generará algún tipo de ganancia.

Sin embargo esta inversión es un esfuerzo que vale la pena realizar por el hecho de minimizar, reducir y evitar incidentes que pudieran causar pérdidas a la organización que mediante de un buen desarrollo de PSI pudiese haber evitado ya que estas contribuyen no solo para la protección de los activos, recursos e información de una organización sino que también buscan que los recursos sean aprovechados de una forma apropiada y que estén ahí para ser utilizados cuando sean requeridos.

Las PSI son un documento que reúne las reglas, protocolos, lineamientos y normas de una organización con el fin de que los recursos que esta tiene para la realización de las diferentes actividades sean usados de una manera apropiada, también buscan el que el usuario tenga un conocimiento adecuado para la protección y aprovechamiento de estos. Estas reglas contrariamente a lo que podría pensarse como reglas o protocolos tediosos que entorpecen las actividades buscan contrariamente a esto, el que el trabajo no sea afectado por estas medidas y que exista un mejor control de manera que la administración de recursos sean mejor aprovechados.

Los objetivos y metas que las PSI buscan no han sido bien comprendidos de manera que se piensa que la inversión para la realización de esta estrategia resulta muy complicada dado que requiere el desviar recursos de la organización para el análisis, elaboración, desarrollo, capacitación y mantenimiento de un programa de seguridad adecuado. Por esto muchas organizaciones solo recurren a paquetes que ofrezcan la implementación de seguridad de manera que esta sea lo más rápida y menos costosa, es decir buscan el minimizar los costos y el tiempo.

El implementar PSI de esta manera es contraproducente ya que cada organización es única, puesto que varía con respecto a las demás en cuestiones como son sus objetivos, metas, recursos, activos, forma de manejo, estructura, rubro, etcétera. Esto hace que los paquetes o la copia de reglamentos, normas, lineamientos y protocolos que en ocasiones las organi-

**Propuesta de Revisión, Actualización y Difusión de Las Políticas de Seguridad en Cómputo para la Facultad de Ingeniería.**

zaciones adquieren de otras sean obsoletas y poco prácticas ya que lo que para una organización funciona para otra puede no funcionar correctamente o no funcionar del todo.

Las PSI son una estrategia integral que desarrolla normas, técnicas y establece lineamientos para el buen funcionamiento y administración dentro de la organización de manera que en caso de presentarse algún imprevisto que pudiera afectar a la organización, su producción o su renombre esta pueda contrarrestar o minimizar este acto de manera que la organización, su trabajo o actividades así como su producción sea afectada lo menos posible.

Con la idea de ofrecer un documento que reúna conocimiento, estrategias, información, observaciones y lineamientos acerca del desarrollo, mantenimiento, revisión y actualización de políticas de manera que este pueda ser utilizado por una organización; en el caso particular por todas las divisiones, áreas y laboratorios que conforman la Facultad de Ingeniería (FI) con el objetivo de mejorar, actualizar y tener un documento que pueda ayudar al desarrollo de las políticas y además poder ser una ayuda práctica para el desarrollo de reglamentos internos, normatividades, lineamientos para las diversas sub-organizaciones.

De la misma forma este trabajo presenta una propuesta de actualización de las políticas vigentes en la Facultad de Ingeniería (FI), lineamientos para el desarrollo de PSI, estrategias para la actualización o revisión de estas, observaciones acerca de la importancia de la capacitación y sus consecuencias, además de propuestas para una mejor difusión la cual incluye la creación de un sitio WEB que pueda ser útil para la consulta de las estas.

Con este trabajo se busca también el que los usuarios entiendan que la Seguridad Informática empieza primeramente por respetar y acatar las disposiciones contenidas en las mismas, las cuales buscan el proteger todo tipo de información y los diversos recursos que la organización confía a los usuarios, esto es el que los usuarios sean conscientes de lo importante que son estos recursos y lo valiosa que es la información de manera que posean una conciencia acerca de la Seguridad Informática.

Esta conciencia de la que se habla será fruto de la capacitación que la organización provea a través de una difusión apropiada de manera que el usuario tenga un conocimiento adecuado de temas relacionados con la seguridad de manera que este pueda tomar decisiones, realizar tareas o actividades, responder de una manera adecuado ante algún suceso, prevenir posibles problemas mediante acciones bien definidas y acceso a las PSI en el caso de tener dudas.

**Propuesta de Revisión, Actualización y Difusión de Las Políticas de Seguridad en Cómputo para la Facultad de Ingeniería.**

La investigación aquí presentada busca ser un manual para conocer más acerca de este tema, es decir busca establecer recomendaciones, lineamientos, técnicas, estrategias, observaciones para la elaboración del documento en el cual se basa toda la implementación, desarrollo, configuración y diseño de medidas, sistemas y procedimientos necesarios para la realización de un programa de seguridad.

# Fundamentos Teóricos

## 1. Fundamentos teóricos

En la actualidad el avance de las comunicaciones y las tecnologías de la información han hecho que la manera de compartir, acceder y comunicar la información sea más rápida y fácil. El hecho de poder consultar todo tipo de información desde cualquier parte del mundo en todo momento desde algún dispositivo como lo son las computadoras, es una de las maravillas que hoy se puede tener gracias a medios como el Internet.

Al poder tener toda esta información se tiene la necesidad de protegerla ya que no toda la información puede ser consultada, editada, borrada o eliminada por personas sin autorización. Si cualquier persona pudiera editar, borrar, destruir, consultar y leer la información de manera arbitraria, sin un orden, crearía un caos, pérdidas económicas, robos de identidad, información errónea, entre otras muchas más.

Es por esto que el tema de la seguridad de la información es un tema muy explotado en películas, las cuales presentan personas que se dedican al robo y otras acciones ilícitas por medio del uso de computadoras, celulares y otros dispositivos digitales.

Estas personas son generalmente aquellas que no tienen límites en sus habilidades al poder acceder a cualquier tipo de información desde diversos lugares, obteniendo ésta en cuestión de minutos.

Esto ha creado la ilusión de que es imposible el poder detener a este tipo de personas con habilidades extraordinarias que se conocen como “hackers”, sin embargo, en realidad este tipo de publicidad es totalmente falsa. Muchos de los términos que se utilizan normalmente, son erróneos, o no utilizados de manera correcta.

Dado que la información que comúnmente no es del todo fidedigna y se emplean de manera incorrecta muchos de los términos, se cometen errores y se es presa de desinformación, lo cual en ocasiones conduce a las personas a tomar decisiones incorrectas que ponen en peligro su información.

Los medios de comunicación presentan nuevos dispositivos de cómputo con capacidad de almacenar, enviar y consultar información de todo tipo, como son fotos, video, audio, texto, entre otros, los cuales contienen información que puede ser o no importante para el usuario. Esta información en ocasiones es utilizada para beneficio de manera ilícita al exponer o publicar esta información en internet, difundirla vía radio o televisión y otros medios.

Este tipo de acciones crea incertidumbre y miedo en el usuario de que la información pueda ser vista por otras personas, es por eso que las compañías promueven dispositivos novedosos, herramientas para la seguridad principalmente antivirus y sistemas operativos que prometen mantenerla de manera más segura.

Este tipo de publicidad “fraudulenta” promete proteger la información de diversas amenazas, como son los hackers, virus informáticos, troyanos, rootkits, scripts, bloqueo de e-mails scam, phishing, y realizar análisis de sitios en internet para una navegación segura, configurar firewalls, entre otras acciones. Este tipo de publicidad crea la ilusión de que los” hackers” crean y controlan estos virus que son la razón de la pérdida y robo de la información.

Este tipo de publicidad tiene por objetivo el vender, prometiendo que sus productos son confiables y de fácil manejo, es decir, que no contienen fallas de ningún tipo y que cualquiera puede manejarlos de una manera muy sencilla con resultados asombrosos. Esto crea una falsa seguridad en la que las personas piensan que su información está protegida y segura.

La realidad es que los medios de comunicación y las organizaciones que fabrican estos productos han exagerado en el hecho de promover éstos al punto de garantizar la seguridad de la información.

Es importante el comprender la relevancia que tiene la seguridad de la información ya que todo el mundo tiene “enemigos”. Este tipo de personas puede utilizar la información de manera ilegal para obtener algún tipo de beneficio propio.

Para ilustrar esto, se puede mencionar que cualquier país tiene enemigos, todas las organizaciones tienen competidores, y de manera más pequeña pero no menos importante, las envidias y celos dentro de un grupo de trabajo.

Por otra parte, el considerar que una organización o persona intente, pretenda, robe, destruya u obtenga cualquier tipo de información de manera ilícita o sin el consentimiento del dueño de ésta, es considerado como un ataque, no importando si es de manera intencional o por error. Cabe mencionar que en ocasiones el que el dueño de la información puede ser el propio enemigo ya que por error, desconocimiento o de manera intencional puede realizar algún tipo de ataque con la finalidad o no de obtener algún beneficio.

## 1.1 Conceptos básicos de seguridad informática

La necesidad de contar con definiciones adecuadas acerca de la seguridad de la información, cobra mucha importancia, ya que contando con un mejor conocimiento acerca de estos temas será más sencillo, fácil y eficiente proteger la información.

En términos generales, se puede afirmar que la mayoría de las personas cometen errores por el hecho de confundir y saber definiciones incorrectas sobre estos temas, el desconocimiento de los temas relacionados, y la desinformación de los medios al difundir la información de manera errónea, entre otros.

Antes de poder definir lo que es la seguridad informática se deben definir algunos conceptos que ayudan a esclarecer mejor el concepto.

### ➤ Organización

Una organización es un conjunto de recursos materiales y humanos con el propósito de alcanzar objetivos y metas. Una organización puede ser un país, una empresa, una universidad, una familia, etcétera.

### ➤ Recursos Humanos

Recibe el nombre de recursos humanos el conjunto de los empleados o trabajadores de una organización.

### ➤ Bienes o Activos

Reciben el nombre de bienes o activos cualquier propiedad de una organización o de una persona. Entre éstos se pueden encontrar, equipo, edificios, autos, mobiliario, derechos de autor, marcas registradas, nombre de la empresa, información, etcétera.

### ➤ Información

La información es el conjunto de datos que obtienen algún significado para quien los manipula.

Ahora bien, antes de pasar a la definición es necesario aclarar que la información en ocasiones no solo se encuentra en forma digital, no dejando por esto de ser información. Por otra parte, el lugar donde se almacena y se maneja dicha información es de suma importancia, ya que sin éste, la información no estaría protegida; por último pero no menos importante, el aclarar que el personal o las personas que trabajan con ella, son las encargadas y responsables de su manejo.

Por esto, es posible definir a la seguridad informática como:

➤ Seguridad de la información o la seguridad informática

Es el manejo adecuado y protección de todo tipo de información (impresa, digital, oral o conocimiento acerca de la organización), de los recursos como son, los bienes o activos (equipos, renombre, recursos informáticos, entre muchos otros) así como de los recursos humanos.

Ya que se cuenta con una definición de lo que es la seguridad informática, y sabiendo que es la encargada de proteger los bienes y recursos de la organización, es importante el saber de qué o de quién se protegen los bienes y recursos de una organización. Para esto es necesario definir dos conceptos.

➤ Amenaza

“Una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño cuando existe una violación de la seguridad.”<sup>1</sup>

Podemos definir como amenaza a todo aquello que intente, puede o pretende destruir o dañar.

---

<sup>1</sup> María Jaquelina López, Cintia Quezada, Fundamentos de seguridad informática, p.91



Las amenazas pueden provenir de varias fuentes:

- 1) Humanas
- 2) Errores de hardware
- 3) Errores de la red
- 4) Problemas de tipo lógico o errores de software
- 5) Desastres

#### 1) Humanas

Este tipo de amenazas son generadas por los seres humanos al manejar la información. Este tipo de amenazas se pueden dar por la ignorancia, la falta de capacitación, descuido, negligencia, errores, intencionales.

En este tipo de amenazas es posible mencionar las siguientes: ingeniería social, robo, el mal uso de los recursos, fraude, sabotaje, terrorismo, espionaje, entre otros.

#### 2) Errores de hardware

Este tipo de amenazas se da por fallas en los dispositivos como son, deterioro, funcionamiento incorrecto, fallas en la energía eléctrica, sobrecalentamiento, problemas en el diseño, mala implementación.

#### 3) Errores de la red

Ocurren cuando la red no está bien diseñada ya que el flujo de información es mucho más grande de lo que se tenía previsto, o cuando existe alguna mala configuración en los sistemas que conforman la red. Entre éstos se pueden encontrar, cableado defectuoso, interferencia, la lentitud en el tráfico.

#### 4) Problemas de tipo lógico o errores de software

Se presentan cuando se implementa algún tipo de seguridad de manera errónea o malas configuraciones, así como cualquier tipo de malware. Algunos ejemplos son los virus, gusanos, código malicioso, caballos de Troya.

#### 5) Desastres

Las amenazas de este tipo son fenómenos naturales que ocasionan algún tipo de siniestro, entre éstos se encuentran los incendios, las inundaciones, los tornados, huracanes, terremotos, entre otros. También se conocen como actos de Dios.

#### ➤ Vulnerabilidad

“Una vulnerabilidad es un punto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo, es decir, representan las debilidades o aspectos atacables en un sistema informático. Se trata de una debilidad que puede ser explotada para violar la seguridad.”

<sup>2</sup>

Se define como vulnerabilidad a todas las debilidades existentes en un sistema.

Las vulnerabilidades se pueden clasificar de la siguiente manera:

- 1) Físicas
- 2) Naturales
- 3) De hardware
- 4) De software

---

<sup>2</sup> Ídem, p. 100

5) De red

6) Humanas

1) Físicas

Este tipo de vulnerabilidad se refiere al acceso físico a las instalaciones de una organización. En otras palabras se refiere al acceso a edificios, estacionamientos, laboratorios, oficinas, y demás áreas que puedan existir en una organización.

2) Natural

Las vulnerabilidades de tipo natural se refieren a cómo es que las condiciones geográficas y las condiciones ambientales pueden afectar al sistema cuando no se cuenta con las medidas necesarias para prevenirlos o disminuir el impacto, es decir, la posibilidad de que el entorno pueda afectar el sistema al tener nuestras instalaciones en regiones donde los incendios, huracanes, inundaciones, terremotos y otros fenómenos naturales sean muy comunes, de esta misma forma que las condiciones ambientales hagan difícil el manejo u operación del equipo como son las condiciones de extremo calor o frío.

También se incluyen los malos diseños de las instalaciones, o la poca previsión de algún tipo de instalación que no se tenía contemplada en el momento de construir, así como el crecimiento de la misma. La falta de copias de seguridad y de la dependencia de una sola área que contenga toda la información en algún punto geográfico, la falta de dispositivos auxiliares, la cercanía a instalaciones de alto riesgo en las que se contengan materiales peligrosos.

3) De hardware

En este tipo de vulnerabilidades se presentan cuando hay malas instalaciones, falta de mantenimiento, y falta de protección de los dispositivos.

4) De Software

Las vulnerabilidades en el software surgen por la falta de previsión al realizar la programación, errores en la misma, también se dan por la mala configuración de los programas y problemas, conflictos y errores en los sistemas operativos que puedan alterar información, permitir modificaciones en los programas, así como la modificación y consulta de la información del sistema.

#### 5) De red

Se presentan cuando no se tiene un control sobre los equipos que se conectan a una red o al sistema, las fallas en la implementación al realizar el cableado estructurado, la falla en la configuración de cualquier tipo de acceso a la red, (incluyendo también las tecnologías inalámbricas, bluetooth, infrarrojos, radio frecuencia, ZigBee, entre otras).

#### 6) Humana

Las vulnerabilidades de tipo humana, se presentan al no contar con personal adecuado, por la falta de capacitación, la falta de ética, la mala disposición del personal, etcétera.

Es importante saber distinguir entre una amenaza y una vulnerabilidad, ya que no son términos que hagan referencia a lo mismo.

Una amenaza se aprovecha de las vulnerabilidades para dañar o destruir, es decir, las amenazas explotan las vulnerabilidades.

Para clarificar esto, se puede decir que al ir a una gasolinera y cargar combustible hay una vulnerabilidad, la cual es que esa área puede incendiarse con facilidad. La amenaza sería que alguien encendiera un cigarro.

La persona que enciende su cigarro podría causar un incendio en la gasolinera. La persona que enciende su cigarro sería la amenaza que se aprovecharía de que la gasolinera es un lugar que es propenso a los incendios y que no cuenta con las medidas de precaución convenientes para evitarlo.

El entender las amenazas y las vulnerabilidades proporciona información que puede ayudar a prevenir incidentes que debilitan, dañan o destruyen a la organización. El hecho de que se presente algún incidente es una clara muestra de un ataque.

Es necesario entonces también definir qué es un ataque:

➤ Ataque

“Es intentar de alguna manera quebrar el sistema destino, los mecanismos de redes y de seguridad.”<sup>3</sup>

Como se ha visto, la seguridad informática protege cualquier tipo de bien o activo de una organización, así como del personal que labora en ella. Tomando esto en cuenta se observa que:

Un ataque es entonces el intento por el cual se pretende obtener, dañar, destruir, o realizar cualquier tipo de modificación a un bien o activo de una organización, siendo éste exitoso o no. Un ataque es la culminación de una amenaza cuando ésta explota una vulnerabilidad.

Con base en lo anterior, un atacante es el individuo, grupo de individuos u organización que realiza algún ataque.

Es importante mencionar que se puede clasificar a los ataques en dos tipos:

I. Pasivos

II. Activos

I. Pasivos

Este tipo de ataques son aquellos en los cuales sólo se reúne información, es decir, se obtiene la información con el fin de poder elaborar y llevar a cabo un plan mediante el cual se pueda obtener un beneficio.

---

<sup>3</sup> <http://www.seguridadinformatica.dcyd.ipn.mx/glosario.html>

De esta forma el atacante no modifica, daña o destruye nada, su propósito es el reunir toda la información posible mediante la observación, la escucha o la lectura para que de esta manera pueda elaborar y realizar su plan para obtener un beneficio.

Al ser atacado de manera pasiva es sumamente difícil y complicado el percatarse de esto, es decir, no se sabe que se está siendo atacado ya que el atacante sólo reúne información, por esto no hay indicios de ningún tipo de daño, pérdida o destrucción evidente en el momento en el que está ocurriendo.

## II. Activos

Un ataque activo es aquél en el cual el atacante daña, destruye, y realiza modificaciones a los bienes de una organización de manera evidente. Este tipo de ataques es perceptible, es decir, a diferencia de los ataques pasivos en los cuales en el momento del ataque no se sabe que se está siendo atacado, en un ataque activo es muy fácil percatarse de él.

El éxito de este tipo de ataque depende en gran manera del pasivo, ya que dependiendo de qué tanta información haya obtenido el atacante, mayor será el daño que cause a los bienes de la organización. En la mayoría de los casos es difícil el contrarrestar este tipo de ataques si el atacante cuenta con la información necesaria para lograr su objetivo.

Cuando una organización es atacada de manera activa puede generar gran confusión, pánico, miedo, daños considerables a los bienes de la organización. Un ejemplo claro de este tipo de ataques son los ataques terroristas los cuales tiene una planeación cuidadosa al reunir información acerca del objetivo (ataque pasivo), en el momento en que se lleva a cabo el plan se convierte en un ataque activo.

## 1.2 Servicios Informáticos

La seguridad informática tiene como objetivo el proteger los bienes de una organización, principalmente la información, de cualquier tipo de ataque ya sea pasivo o activo. De esta manera la seguridad informática cuenta con los servicios informáticos los cuales están enfocados al manejo, control y a la confiabilidad principalmente.

Los servicios informáticos, también llamados servicios de seguridad, deben estar presentes todo el tiempo dentro de cualquier organización; la seguridad informática debe garantizar que estos servicios estén presentes al implementar cualquier medida de seguridad. Éstos se pueden clasificar en:

- 1) Confidencialidad
- 2) Autenticación
- 3) Integridad
- 4) No repudio
- 5) Control de Acceso
- 6) Disponibilidad

- 1) Confidencialidad

Este servicio consiste en asegurar que la información sólo puede ser accedida por ciertas personas, es decir, sólo personas que estén autorizadas por el dueño de la información serán las que podrán tener acceso a ésta.

La privacidad o confidencialidad es un servicio que cumple con la función de mantener en secreto la información.

- 2) Autenticación

La autenticación es la verificación de la identidad. Este servicio se encarga de verificar o tener la seguridad de que la identidad sea confirmada.

- 3) Integridad

El servicio de integridad es la verificación de que la información no ha sido alterada o modificada y que permanecerá de esta manera mientras el dueño de la misma así lo requiera o necesite.

#### 4) No repudio

Este servicio consiste en evitar y garantizar que los emisores, receptores, o las partes involucradas puedan negar la recepción, transmisión, lectura u otras actividades con respecto a la información.

#### 5) Control de Acceso

El control de acceso es el servicio encargado de impedir o permitir el acceso a un sistema, área, o recurso, así como el limitar el acceso al mismo.

#### 6) Disponibilidad

Es el servicio que se encarga de garantizar que el recurso, sistema, información o área pueda ser accedida cuando se requiera o necesite.

Los servicios de seguridad utilizan estos principios en conjunto para garantizar que los recursos, la información, los sistemas, y demás bienes sean utilizados, accedidos, consultados, modificados, borrados sólo por las personas designadas por el dueño de éstos. Con esto se pretende evitar las pérdidas y los accesos a estos bienes de manera que sean utilizados para los propósitos para los que fueron designados originalmente.

### **1.3 Mecanismos de Seguridad**

Así como los servicios de seguridad tienen el propósito de que los recursos, información, sistemas y demás bienes sean utilizados para lo que fueron destinados. Los mecanismos de seguridad se basan en:



- ❖ Conjuntos de algoritmos, los cuales permiten implementar técnicas criptográficas.
- ❖ Conjuntos de procedimientos, que establecen cómo se emplearán los algoritmos.
- ❖ Información secreta, que puede ser algo que se tiene, que se posee o que se sabe (claves, contraseñas, credenciales, etcétera).

Esto es con el fin de implementar los diferentes servicios de seguridad dentro de una organización. Estos mecanismos se emplean dependiendo del nivel de seguridad deseado y del tipo de servicio que se desee implementar.

Algunos de estos mecanismos de seguridad son:

- 1) Intercambio de autenticación
- 2) Cifrado
- 3) Integridad de datos
- 4) Firma digital
- 5) Control de encaminamiento
- 6) Unicidad

- 1) Intercambio de autenticación

Los mecanismos de intercambio de autenticación son los encargados de verificar y corroborar la identidad por medio de técnicas criptográficas, para verificar con certeza el origen y destino de la información. Un ejemplo de este tipo de mecanismo son los certificados digitales en páginas para las transferencias bancarias.

- 2) Cifrado

Es un mecanismo por el cual mediante técnicas criptográficas se garantiza que la información sea ilegible para los usuarios no autorizados. Con esto se garantiza la confidencialidad de la información.

### 3) Integridad de datos

La integridad de datos es un mecanismo en el cual se utiliza el cifrado y compresión de una cadena de datos con el fin de que el receptor pueda realizar una verificación de la integridad de la información enviada.

### 4) Firma digital

Es el mecanismo en el que se utilizan técnicas criptográficas con lo que se garantiza la integridad de la información así como la autenticación del emisor. Consiste en un conjunto de caracteres que vinculan al autor con el documento y se anexan a él, con el fin de acreditar quién es el autor y comprobar que la información no haya sido manipulada.

El receptor procesa la información para validar al autor y la integridad de la información. Cabe señalar que la firma digital no cifra el mensaje, únicamente garantiza el origen.

### 5) Control de encaminamiento

Este mecanismo de seguridad permite enviar información de manera controlada por zonas determinadas. Con este tipo de mecanismo se evitan zonas donde se detecten violaciones a la integridad de la información enviada.

### 6) Unicidad

La unicidad consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, incluyéndose en la firma digital o integridad de datos. De esta forma se logra que la información tenga una secuencia única.

## 1.4 Gestión de contraseñas

Las contraseñas son un mecanismo mediante el cual se accede a información, recursos, sitios, etcétera. También mediante las contraseñas es posible autenticar la personalidad al querer acceder a algún recurso de manera lejana o remota, lo cual es de suma utilidad ya que en ocasiones se requiere manipularlos sin que se estar presente.

Este mecanismo es el más utilizado, por lo que si algún atacante consiguiera la contraseña, sería capaz de acceder a los recursos, a la información, suplantar la identidad obteniendo así algún beneficio de manera ilícita.

Es por esto que se define el término contraseña o clave como una forma de autenticación que utiliza información secreta para tener acceso a algún recurso, sistema o sitio.

Las contraseñas son como las llaves que se emplean normalmente para la apertura y cierre de puertas, cerraduras, candados que normalmente se utilizan para proteger casas, oficinas, autos, cajas de seguridad, etcétera. Sería ridículo perder las llaves o prestarlas a cualquier persona ya que eso tendría el riesgo de que alguien pudiera realizar algún acto mal intencionado como lo es el robo. En este caso las contraseñas funcionan de la misma manera.

Sin embargo, al igual que las cerraduras, candados y puertas, pueden ser forzadas o abiertas de manera ilícita o usando técnicas de cerrajería, los mecanismos para validar, que son lo equivalente a las puestas, candados y cerraduras, también sufren ataques.

Estos ataques consisten en adivinar las contraseñas, la prueba de múltiples combinaciones de datos asociados al usuario, como son fechas, nombres, eventos, frases, libros, mascotas y datos de personas cercanas al dueño de la contraseña o el usar combinaciones de datos e información de forma aleatoria y la creación de diccionarios de información son algunas de las técnicas más socorridas para obtener el acceso y así burlar los diversos mecanismos de seguridad que requieran una contraseña.

Con el fin de que la contraseña sea más fuerte, es decir, que el atacante requiera invertir más recursos y mucho más tiempo para obtener acceso, existe la gestión de contraseñas. La gestión de contraseñas es el coordinar los recursos disponibles para conseguir que una contraseña sea confidencial, es la utilización de técnicas y recomendaciones para lograr que una contraseña sea más confiable, que se mantenga en secreto y que aminore el riesgo de que el atacante pueda obtener el acceso. La gestión de contraseñas es de gran importancia

ya que por medio de ella se puede resguardar y proteger la información de una mejor manera.

Es importante el mencionar que no importa qué tan seguro sea el mecanismo de seguridad para el acceso, si no se hace uso de la gestión de contraseñas, el atacante podrá tener acceso de una manera relativamente sencilla y acceder a recursos, información, sitios, etcétera.

Para contar con una apropiada gestión de contraseñas, a continuación se mencionan algunas recomendaciones y técnicas para la creación y mejoramiento de la seguridad de las contraseñas que son más utilizadas en el acceso a los diferentes sistemas que requieren =ingresar alguna cadena de caracteres, como son el correo electrónico, cuentas de bancos, cuentas internet de cualquier tipo, etcétera.

- Evitar contraseñas cortas

El añadir más caracteres a una contraseña aumenta exponencialmente el grado de protección que ésta ofrece. Por esto es recomendable que la longitud mínima de una contraseña sea de seis dígitos.

- Memorizar las contraseñas

El evitar apuntar las contraseñas en alguna parte es una vulnerabilidad ya que existe el riesgo de que alguien pueda acceder a esa información y pueda hacer mal uso de ella. Por eso es recomendable que las contraseñas sean memorizadas.

- Tener una contraseña para cada recurso

Es recomendable el tener una contraseña por cada cuenta ya que si la contraseña llegara a ser obtenida de alguna forma, los recursos de los cuales se es responsable estarían en un riesgo inminente de ser accedidos.

- Evitar el uso de información contenida en diccionarios de cualquier clase o idioma

El hacer uso de palabras o información contenidas en cualquier diccionario o publicación en cualquier idioma puede ser utilizado por algún atacante para obtener el acceso.

- Cambiar la contraseña periódicamente

El cambiar la contraseña periódicamente tiene la ventaja de que si ésta fue obtenida se evita que exista algún tipo de ataque pasivo, con el cual el atacante pudiera obtener información valiosa para la planificación de un ataque activo. Es recomendable que la contraseña se cambie al menos cada 6 meses.

- Uso de mayúsculas, minúsculas, números y caracteres especiales.

El uso de múltiples caracteres complica que sea adivinada o vulnerada, ya que aumenta el número de combinaciones que un atacante tendría que probar para obtener el acceso.

Como se ha visto a lo largo de este capítulo, la seguridad informática abarca muchas áreas entre las que se encuentran las redes, el cifrado, las comunicaciones, entre otras.

Una de estas áreas es el desarrollo de políticas de seguridad, la cual tiene como uno de sus objetivos el crear lineamientos, estrategias, guías, normas que ayuden a las personas, las capaciten, y creen conciencia acerca de cómo manejar y cuidar de una mejor manera los recursos, bienes y la información.

La seguridad informática tiene como una de sus metas el proteger la información y bienes de las personas, pero es importante el remarcar que la seguridad depende en gran parte de las personas responsables y los dueños de la información y los bienes.

# Políticas de Seguridad

## 2. Políticas de seguridad

Las organizaciones a nivel mundial se han visto en la necesidad de formalizar la manera de actuar, reaccionar, y tratar con los diferentes sucesos, acontecimientos e influencia que rodean o afectan a éstas. Es por esto que se redacta una serie de lineamientos y normas para que los objetivos puedan ser alcanzados y así permitir la continuidad del trabajo dentro de las organizaciones.

Uno de los temas con más relevancia es el tema de la seguridad, dentro de cualquier tipo de organización, ésta tiene como objetivo el proteger un bien, es decir, la seguridad ofrece la confianza y tranquilidad de que no existe peligro alguno, sin embargo, esto no es del todo cierto, ya que el peligro nunca deja de ser inexistente. La seguridad ofrece un nivel de protección que minimiza el peligro, pero que no lo desaparece por completo.

En estos tiempos donde la globalización de las organizaciones es un hecho, las diferentes tecnologías han acelerado el intercambio, envío y transferencia de numerosos bienes, lo que conlleva un riesgo para cualquier organización la cual se ve forzada a implementar algún tipo de seguridad.

La evolución de las tecnologías de la información ha sido tal, que gracias a ellas en la actualidad el acceso y la transmisión de ésta se ha simplificado de manera substancial, un ejemplo de esto, es que en la actualidad es más fácil realizar desde compras hasta declaración de impuestos, sin embargo, el peligro ha aumentado ya que mediante este tipo de medios electrónicos hoy en día se pueden realizar transferencias de diversos tipos de bienes como son las divisas, las propiedades, también se pueden realizar compras, intercambio de información sensible, entre muchas otras más.

Por otro lado, la transferencia de cualquier tipo de información como lo es la transmisión de video, imágenes, voz, mensajes, y documentos electrónicos, así como el acceso a una gran fuente de información de cualquier tipo hace de las tecnologías de la información (TI) una valiosa e imprescindible herramienta para cualquier organización.

Es por ello que surge la necesidad de implementar algún tipo de seguridad enfocada a las diferentes tecnologías de la información, sin embargo, existe muy poca cultura acerca de la seguridad en este tipo de medios que son altamente utilizados a nivel mundial por medio de los cuales se transfiere una gran cantidad de información de todo tipo, éstos pueden ser utilizados por personas con intenciones de obtener algún beneficio de manera ilícita.

La cultura de la seguridad informática es generalmente un conocimiento basado en antivirus, firewalls y actualizaciones, lo cual es incorrecto ya que la seguridad de la información va mucho más allá de estos mecanismos que son de gran ayuda, sin embargo, no son garantía de un nivel apropiado de seguridad.

Es importante el destacar que cualquier organización que cuenta con políticas cuenta con una especie de lineamientos que ayudan para la toma de decisiones y su manejo dentro de la misma.

Una política es una declaración general de principios que permite cumplir ciertos objetivos propuestos. Esta declaración de principios está basada en los objetivos, misión y visión que la organización persigue, independientemente de su giro o tamaño (pequeña, mediana o grande). Por esto, es de suma importancia que la organización tenga bien claro su objetivo y sus alcances.

El no tener bien definidos estos puntos genera que la empresa no tenga dirección, no cuente con una meta y que el funcionamiento de la organización sea caótico. El no contar con una meta o un objetivo al cual se quiere llegar, hace que la organización no sepa dónde empezar, qué debe mejorar ni qué hacer, sería como navegar un barco sin rumbo.

Una definición formal del término política se muestra a continuación:

➤ Política

Una política es un conjunto de declaraciones, actividades, prácticas o planes orientados y diseñados para guiar o controlar la toma de decisiones en una organización para conseguir un objetivo o varios.

Las políticas que se definan dentro de cualquier organización son la forma en la que la organización controlará, trabajará, llevará a cabo y reaccionará ante las diferentes condiciones y acciones del entorno en el que se encuentre. Estas políticas marcan la manera en que la organización se relaciona con su entorno externo e interno, es decir, cómo manejan sus relaciones internas con las personas que laboran dentro de ella y cómo se relaciona externamente con otras organizaciones.

En este tipo de documentos se establecen varias políticas como son las de confidencialidad, derechos de autor, de forma de trabajo, económicas, de integridad, de seguridad, entre mu-



chas otras más, sin embargo, las que interesa analizar en este trabajo son las de seguridad, ya que se encargan de la preservación, el mantenimiento y la protección de los bienes de la empresa.

Dentro de las políticas de seguridad se abarcan muchas áreas que en ocasiones no se piensa que fueran parte de éstas, ya que en general se cree que la seguridad tiene que ver sólo con el acceso a las instalaciones, con la preservación de éstas y la vigilancia de las misma, sin embargo, esto no es así. Si el hecho del resguardo de sólo estos aspectos fuera suficiente, la implementación de seguridad en cualquier organización sería una tarea sencilla, sin embargo, ya que la seguridad no sólo abarca estos aspectos sino muchos otros diferentes, es por esto que diferentes organizaciones a nivel mundial tienen departamentos enfocados sólo hacia la seguridad.

Podemos mencionar el caso de nuestro país al tener diferentes organismos concernientes a la seguridad como los son:

- El Centro de Investigación y Seguridad Nacional (CISEN), que es un departamento desconcentrado de la Secretaría de Gobernación cuyo objetivo es la obtención, procesamiento y análisis de información en materia de seguridad nacional para México desde el ámbito civil.
- La Agencia Federal de Inteligencia (AFI), cuya misión es combatir de manera eficaz y profesional a las diferentes organizaciones de delincuencia organizada por medio del análisis de datos e información de las diferentes dependencias para con esto proteger y salvaguardar a México.

La seguridad es una necesidad fundamental que requiere se asignen recursos y no se tome a la ligera ya que el que una organización pueda seguir trabajando en alcanzar sus objetivos y metas depende mucho de esto. Existen casos de espionaje industrial que han ocasionado la pérdida de valiosos recursos, que mediante una apropiada implementación de seguridad hubiera podido ser evitada.

Es por esto que la seguridad en las organizaciones es ahora un tema muy común ya que con la globalización muchas de ellas se han internacionalizado, es decir, tienen presencia en diversas partes del mismo país e incluso del mundo, es por esto que en muchos de los países se ha convertido en una cuestión de seguridad nacional el contar con políticas de seguridad, ya que es imprescindible para la protección de los diferentes bienes, así como el di-

seño de mecanismos confiables para protegerlos de cualquier tipo de ataque. Uno de estos mecanismos son las políticas.

El implementar seguridad en una organización requiere una evaluación previa considerando ¿Qué es lo que se quiere proteger?, ¿De quién o de qué se quiere proteger?, y ¿Cómo se quiere proteger?

Este análisis que parece ser muy efímero y poco importante previo a la implementación de cualquier tipo de seguridad es la base de las políticas de seguridad, ya que sin éste no se tiene una certeza de los bienes a proteger ni de qué o de quién se va a protegerlos, de las diferentes políticas internas de la organización o políticas corporativas, de las metas y objetivos de la misma, así como los diferentes controles, medidas y la forma de trabajo que se pudiera ver afectada al implementar cualquier tipo de controles de seguridad.

Sin embargo, es importante el destacar que el rubro de la seguridad es poco apreciado dentro de las organizaciones ya que es una inversión que no reedita, es decir, no se obtiene ninguna ganancia, sino que por el contrario requiere una inversión significativa para capacitar al personal, así como tener expertos dentro de la rama para el mantenimiento, vigilancia, supervisión de los dispositivos y normas de la seguridad.

El contar con políticas de seguridad no es garantía alguna de que no habrá ningún tipo de incidente dentro de la organización, sin embargo, el contar con éstas ayudará a prevenir y a solucionar cualquier tipo de situación que se presente. De igual manera, al presentarse cualquier tipo de incidente las políticas apoyarán al restablecimiento de las actividades de la organización en un menor tiempo, lo que se traduce como menores pérdidas para ésta.

## **2.1 Definición de política de seguridad**

Las políticas de seguridad se encuentran contenidas dentro de las organizaciones aunque no se tenga un documento formal en el cual se estipulen o se describan las diferentes medidas acerca de la seguridad. En ocasiones las organizaciones contratan este tipo de servicios para no tener que lidiar con la formación de un departamento que se encargue de la seguridad dentro de la organización.

Esta creencia es incorrecta e incluso peligrosa, ya que aun cuando se contrate a otra organización para que apoye con las actividades de seguridad, la implementación, el monitoreo, el

mantenimiento e incluso hasta la limpieza de las instalaciones deben estar dentro de una normatividad, es decir, la contratación de organizaciones para el apoyo de la seguridad debe estar reglamentadas.

Es indispensable que la organización cuente con un documento reglamentario, pues en éste se contempla un conjunto de lineamientos que tiene como objetivo el proteger la organización de todo tipo de amenazas, tanto internas como externas, en él se deben contener normas de conducta, de término de relaciones laborales, delegación de responsabilidades, de subcontratación de servicios, planes de contingencia, y cualquier otra situación que sea posible; inclusive tomando en cuenta ideas que pueden ser consideradas como extremas (por ejemplo, el considerar ataques terroristas).

Por esto, es importante tener una idea muy clara de la función de las políticas de seguridad y sus alcances, lo anterior con el único propósito de aclarar que las políticas de seguridad no se enfocan en decir el cómo se deben implementar, qué herramientas se deben utilizar, o qué métodos de control deben implementarse dentro de la organización, las políticas de seguridad hablan sobre el qué se debe proteger y las restricciones que se deben poner o tener en cuenta para el mejor desempeño de los controles que tendrán como meta el alcanzar el objetivo de la organización.

El alcance de las políticas de seguridad es extenso, no sólo protege los bienes que parecen más relevantes, importantes y tangibles como las instalaciones, edificios, oficinas y equipo, sino que van más allá al proteger una diversidad de bienes que la organización posee, los cuales en ocasiones no se toman en cuenta pero que también son de suma relevancia para ésta, entre los que se encuentran: el nombre de la organización, marca, renombre o reputación, la propiedad intelectual, los recursos humanos ya que éstos son la parte encargada de realizar todo el trabajo de la organización, y que representa una inversión grande por el hecho de tener que capacitar continuamente al personal.

En ocasiones se comete el error de no considerar como parte de la organización a los recursos humanos, cuando éstos son una parte vital de la misma. De esta misma forma es necesario tener conciencia que este tipo de políticas de seguridad no asegura que no habrá incidentes; de hecho los habrá sin duda. Por esto, dichas políticas no deben sugerir que cuando ocurra un error los usuarios serán tratados con todo el peso de las leyes por la violación cometida. Deberán tener previstos tales acontecimientos y medidas para resolverlos.

El siguiente cuadro (Tabla 2.1) presenta un resumen general sobre las políticas de seguridad y de las ideas principales que se trataron acerca de ellas.

Tabla 2.1 Políticas de seguridad

<b>Políticas de seguridad</b>		
<b>Sí son</b>	<b>No son</b>	<b>Bienes a proteger</b>
<p>1. Respuestas a las preguntas:</p> <p>¿Qué es lo que se quiere proteger?</p> <p>¿De quién o de qué se quiere proteger?</p> <p>¿Cómo se quiere proteger?</p> <p>¿Qué se debe proteger?</p> <p>2. Restricciones que se deben tener en cuenta</p> <p>3. Limitantes de los controles a implementar</p>	<p>1. Cómo implementar la seguridad especificando qué tipo de controles, medidas, mecanismos, para la protección de los bienes</p> <p>2. Qué herramientas, sistemas, y equipos utilizar para la implementación de la seguridad</p>	<p>1. Instalaciones</p> <p>2. Equipos</p> <p>3. Edificios</p> <p>4. Recursos humanos</p> <p>5. Renombre o Reputación</p> <p>6. Marca</p> <p>7. Propiedad intelectual</p> <p>8. Información de cualquier tipo y formato</p> <p>9. Capacitación</p> <p>10. Experiencia</p>

Ideas principales sobre las políticas de seguridad. Tabla 2.1

Teniendo en cuenta todo lo anterior se puede definir este concepto de una manera más completa.

➤ Políticas de seguridad

Las políticas de seguridad son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos a los que se puede enfrentar. Permite identificar qué recursos son valiosos y qué medidas deben tomarse para prevenir, manejar las pérdidas, así como los siniestros que pueden tener un impacto sobre los bienes de la misma.

## 2.2 Definición de política de seguridad informática

Conforme las tecnologías de la información siguen su avance, las organizaciones se han visto en la necesidad de desarrollar políticas que ayuden a la protección de los bienes que incluyen a estas nuevas tecnologías. Al desarrollo de este tipo de políticas orientadas a la protección de las diferentes tecnologías de la información y a los bienes que incluyen, se le denomina políticas de seguridad informática.

Por otra parte, es necesario resaltar la creencia acerca de que este tipo de políticas sólo están orientadas a proteger la información contenida, tratada, procesada o almacenada por medios digitales, no obstante esto no es del todo correcto. Este tipo de pensamiento llega a causar confusión dentro de las organizaciones y puede llegar a causar desánimo por el hecho de que no sólo habría que desarrollar políticas de seguridad, sino que además hay que desarrollar políticas de seguridad informática.

Ideas como el pensar que las políticas de seguridad informática son un apartado o que tengan que desarrollarse aisladas de la organización u orientarse sólo hacia los medios digitales, o que sólo tienen que ver con las tecnologías de la información, son un error común.

El desarrollo de este tipo de políticas no debe considerarse de manera aislada, ya que la información de una organización no sólo les concierne a los medios digitales, sino que este tipo de políticas están enfocadas a la aplicación de la seguridad informática.

Las políticas de seguridad informática (PSI), se definen como la declaración general de principios, acuerdos, reglas y recomendaciones que permiten resguardar o proteger un recurso informático.

El sólo hablar acerca de recursos informáticos no es del todo correcto, ya que existe información sensible que no se encuentra únicamente en medios digitales o que concierne sólo a los recursos informáticos o son referentes a las diferentes tecnologías de la información. Existe información dentro de toda la organización que se cree que no es importante o que simplemente no se piensa acerca de la importancia de ella, como es toda aquella información que las personas que laboran dentro de la organización conocen.

Un ejemplo claro de este tipo de información que pareciera no ser relevante es que el personal que labora dentro de una organización tenga conocimiento de los diferentes horarios, claves personales, horarios de entrada y salida, números de teléfonos, nombres completos, correos electrónicos, direcciones y datos personales, salarios, días de pago, entre muchos.

Este tipo de información puede ser utilizada por personas para obtener algún tipo de beneficio o el planificar un ataque en contra de la organización y así conseguir un beneficio.

Es por esto que las políticas de seguridad y las políticas de seguridad informática están íntimamente ligadas por el hecho de que la información es uno de los bienes más importantes que las organizaciones tienen y que si no es protegida de manera adecuada, representa una vulnerabilidad para la organización que puede llegar a causar todo tipo de daños.

Las políticas de seguridad informática tienen como objetivo proteger todo tipo de información que tenga que ver con la organización, sus bienes, el personal que labora o con el que se comparte algún tipo de información, para que esta información no pueda ser utilizada para otro tipo de fines diferentes a los cuales está destinada. En ocasiones la información llega a ser más valiosa incluso que los otros bienes que la organización tiene, puede ser decisiva en la toma de decisiones las cuales pueden afectar en gran manera a la misma organización, así como a otras con las que se puede tener una relación de cualquier tipo.

El proteger la información de una organización es una meta complicada por el hecho de que la información se encuentra en diversas formas y formatos, es decir, la información que tiene o maneja el personal, la contenida en medios digitales, la que es procesada, transmitida y almacenada por los sistemas informáticos, la información vital que es almacenada en las instalaciones como pueden ser contratos, memorándums, correo de todo tipo, notas, manuales, documentación, etcétera, es por esto que las políticas de seguridad informática y las políticas de seguridad deben ser consideradas como un todo y no de manera separada. Sin embargo, el hacer énfasis en la informática delimita y hace que las políticas sean más puntuales, con una mejor organización o administradas de una mejor manera para ser más efectivas, además de poder abarcar algunas otras políticas que aparentemente pueden no estar relacionadas pero que son necesarias para tener un buen nivel de seguridad informática.

A diferencia de las políticas de seguridad, este tipo de políticas busca proteger cualquier tipo de información relacionada con la organización y que pueda ser usada para obtener un beneficio acosta de la misma.

Teniendo este panorama general sobre las políticas de seguridad informática es necesario el contar con una definición formal.

➤ Políticas de seguridad informática

Son parte de una estrategia en la que se establecen reglas, recomendaciones, estándares y normas que una organización utiliza para la implementación de medidas de seguridad informática para la protección de los diferentes bienes de la organización, enfocando este esfuerzo a implementar un nivel adecuado de seguridad informática, de tal manera que cualquier tipo de información sea empleada de manera adecuada. Así mismo describe las actividades aceptables, las sanciones que se aplicarán si éstas no son respetadas, el cómo es que la organización reaccionará, dará seguimiento y se reincorporará para seguir con sus actividades, además de crear conciencia en los usuarios acerca de la seguridad informática, capacitando de esta forma al usuario para la protección de cualquier tipo de información de la que sea responsable.

### **2.3 Objetivos de una política de seguridad**

En toda organización se debe comprender que una política de seguridad no es necesaria, sino que es una prioridad básica como es el tener personal que labore dentro de la organización; es por esto que los objetivos de las políticas de seguridad son el de contemplar, implementar y ejecutar las distintas disposiciones, lineamientos, normas, y recomendaciones para que de esta manera se obtenga un nivel de seguridad apropiado, es decir, que exista la seguridad mínima indispensable para que se puedan realizar las diferentes actividades que se necesiten de manera segura además de que la seguridad no interfiera o haga que estas actividades sean mucho más complicadas por el hecho de tenerla implementada dentro de las actividades.

Algunos de los objetivos de las políticas de seguridad son el de proteger a la organización de todo tipo de ataques que puedan generarse tanto de manera interna como externa, las diferentes situaciones que pudieran darse dentro de la organización, y sucesos fuera de control como son los fenómenos naturales, terremotos, huracanes, inundaciones, etcétera. De esta misma manera se busca que la organización pueda regresar a su actividad normal para continuar con sus actividades en el menor tiempo posible.

De igual forma se busca dar un buen nivel de seguridad para que el personal de la organización pueda sentirse seguro y protegido, de tal manera que se pueda laborar sin necesidad de verse afectado por las diferentes medidas implementadas para su seguridad, en otras palabras, poder trabajar sin que la seguridad afecte las diferentes actividades dentro de la organización teniendo un nivel de seguridad aceptable.

La mejor administración de los recursos para un mejor y más eficiente trabajo, es decir, la asignación efectiva de equipo y recursos según las necesidades y carga de trabajo que se tenga en ese momento. Esta asignación es importante ya que el asignar recursos de más o menos puede entorpecer el trabajo, este tipo de asignación no es sencillo debido a que involucra dar permisos y el acceso a diferentes recursos e información lo anterior puede causar incidentes de seguridad si no se considera el principio de mínimo privilegio que debe estar contenido dentro de las políticas de seguridad informática.

Por otro lado, las políticas de seguridad informática aclaran qué se está protegiendo y por qué, son las bases para la resolución e interpretación de conflictos que se puedan presentar en el futuro, por esto último, es importante que las políticas contengan procedimientos, ideas, bases y principios que abarquen todas las posibles situaciones y conflictos que aún no se presentan, esto conlleva a que las políticas no deben variar mucho a lo largo del tiempo.

Son la base para la implementación de medidas para la protección y mejor funcionamiento de la organización, describen actividades del personal y sus sanciones por no acatarlas, crean conciencia acerca de la seguridad informática, proveen un punto de partida para la identificación y el entendimiento de las metas a las que se quiere llegar como organización, como un todo.

De esta forma el capacitar al personal, que éste tenga conocimiento acerca de las políticas de seguridad informática, que posea una conciencia y conocimientos sobre la seguridad informática ayudan a la protección de la información personal de los usuarios y de la información que pertenece a la organización de la cual es responsable.

En otras palabras, una política de seguridad es una herramienta altamente efectiva para la protección de todos los bienes de una organización, sin embargo, existe una incongruencia, ya que pese a su relevancia, dichas políticas a menudo no son consideradas seriamente por los gestores empresariales o los directivos, sino hasta el momento en que la organización ha sufrido algún incidente de seguridad importante y se ha tenido algún tipo de pérdida que ha afectado a la organización.

Lo cierto es que la política más efectiva no es aquella que se desarrolla durante un momento de crisis, sino la que se construye, actualiza y comunica de manera continua después de una revisión sistemática de las necesidades de seguridad corporativas.



Las políticas de seguridad informática tienen como objetivo también el prevenir la pérdida de información, el uso adecuado y eficiente de los recursos informáticos, así como de los sistemas de cómputo.

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

El facilitar la auditoría, el control de la información y el uso de los recursos con los que cuenta la organización, permite que los encargados (administradores) de los distintos laboratorios y salas de cómputo 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 informática 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.

Estas políticas 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 cuentan, el acceso a las distintas áreas dentro de la organización, el prestigio de la organización, así como el proteger a los usuarios y su información personal.

En ocasiones parece ser que las políticas de seguridad informática 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.

A continuación se tiene un resumen sobre las ideas y acciones que los objetivos de las políticas de seguridad buscan en cualquier organización, además de ser de gran ayuda en la toma de decisiones.

### Objetivos de las políticas de seguridad

- ✓ Obtención de un nivel de seguridad adecuado para la organización.
- ✓ Resolución e interpretación de conflictos que se puedan presentar en el futuro.
- ✓ Protección contra ataques que puedan generarse tanto de manera interna como externa.
- ✓ Procedimientos, ideas, bases y principios que abarquen todas las posibles situaciones y conflictos que aún no se presentan.
- ✓ La implementación de medidas para la protección y mejor funcionamiento de la organización.
- ✓ Capacitación y concientización del personal acerca de las políticas y conocimientos sobre la seguridad informática.
- ✓ Prevención de la pérdida de información.
- ✓ Uso adecuado y eficiente de los recursos informáticos.
- ✓ Ayuda en la adquisición de equipo y software que requiere la organización para su mejor desempeño.
- ✓ Permite el tener procedimientos para eventualidades, conflictos, ampliaciones en la organización.
- ✓ Facilita la auditoría y el control de la información.
- ✓ Mejor administración y asignación de equipos a los usuarios según sus necesidades.

- ✓ Regulación de instalación, uso y acceso de los diferentes recursos informáticos. dependiendo de acuerdo con sus actividades y responsabilidades.

## 2.4 Definición y objetivos de las buenas prácticas

En toda organización existe una serie de recomendaciones o prácticas para el buen desempeño de las diferentes tareas o trabajos que se requieren hacer, es decir, principios que existen para el mejor desempeño de las actividades. Este tipo de recomendaciones surgen debido a la propia la experiencia o a la de un experto o personal que ya ha laborado y ha tenido que lidiar con ese tipo de situaciones.

Este tipo de prácticas se le llama buenas prácticas, las cuales son utilizadas en todo tipo de organizaciones y departamentos de cualquier organización para el mejor desempeño del personal que labora, sin embargo, este tipo de prácticas no son obligatorias.

Las buenas prácticas son recomendaciones o consejos que se le dan al personal durante su trabajo o al momento de su capacitación para que éste desarrolle de una mejor manera el trabajo, resuelva o evite problemas relacionados con las actividades a realizar. De esta manera no tiene que seguir u obedecer en su totalidad este tipo de prácticas que es deseable que siga, sin embargo, no es obligatorio conocerlas en su totalidad, que posea algún tipo de razón por la que éstas deben seguirse, no requiere que el personal esté capacitado en ellas o que las conozca.

Algunas veces este tipo de buenas prácticas tienen su fundamento en alguna política de seguridad de la misma organización o de alguna otra, o simplemente es una manera que se ha encontrado de ser efectiva, es decir, con base en la experiencia del personal en esa área o materia se han desarrollado ese tipo de prácticas.

Una definición formal de este concepto se muestra a continuación

### ➤ Buenas Prácticas

Son lineamientos, recomendaciones o prácticas de tipo no obligatorio que resultan ser efectivas para la realización de actividades, trabajos o tareas que se requieren desarrollar dentro

de la organización, las cuales tienen su base en políticas o en la experiencia en la realización de actividades.

Este tipo de documento en ocasiones es de gran ayuda para la rápida incorporación de personal a las organizaciones, sin embargo, tiene algunos inconvenientes como son el que el personal no debe seguir o respetarlos de manera obligatoria, no crean o generan conciencia en el usuario el cual sólo las sigue sin una razón que le dé sustento, lo que ocasiona que con el tiempo sean ignoradas o que no se sigan. No existe nadie que regularice o estandarice este tipo de reglas por lo que cada departamento o área puede tener maneras diferentes de realizar una misma tarea lo cual puede provocar conflictos o problemas internos en la organización.

Por otra parte, el poder incorporar a los usuarios de manera rápida a las actividades y no tener que capacitar de una manera formal hace que resulten altamente atractivas, sin embargo, para evitar problemas y conflictos internos éstas deben estar basadas en las políticas internas de la organización, es decir, que deben haber sido aprobadas por la misma organización como un documento anexo o una extensión para usos prácticos de las políticas de seguridad que se estén llevando a cabo dentro de la organización.

Las buenas prácticas no son un documento completo en el cual una organización pueda depender para resolver o reaccionar ante cualquier tipo incidente de seguridad, para el restablecimiento de las actividades o para informar y capacitar al personal a manera de que éste pueda tener un panorama general de lo que busca la organización al seguir este tipo de prácticas. Por otro lado no asigna ningún tipo de responsabilidades, es sólo un documento para que el personal pueda echar mano para realizar una actividad sencilla y básica sin necesidad de ser capacitado de manera formal.

A continuación se presentan un breve resumen sobre lo que se ha tratado acerca de las buenas prácticas a lo largo de este capítulo.

#### Buenas Prácticas

- ✓ Incorporar al personal de manera rápida a las actividades.
- ✓ Deben estar basadas y reguladas en las políticas de seguridad.

- ✓ No son de carácter obligatorio.
- ✓ Son recomendaciones para ayudar al usuario a realizar mejor sus actividades.
- ✓ Deben ser reguladas por las políticas de seguridad.
- ✓ Pueden estar basadas en la experiencia personal.
- ✓ No existe un sustento o razón de existencia.
- ✓ No hay responsabilidad alguna para que el usuario las respete.
- ✓ No delega responsabilidades.
- ✓ Ayuda al personal a la realización de actividades sencillas y básicas.

# Importancia de las políticas de seguridad

### 3. Importancia de las políticas de seguridad

Las políticas de seguridad son una estrategia efectiva para la protección de las organizaciones, es una necesidad básica e indispensable el proteger las actividades, el trabajo, los bienes (entre los cuales se encuentra la información entre muchos otros más), los recursos humanos por mencionar algunos. Es decir, si la empresa no cuidara o protegiera el producto de su trabajo, así como todo aquello que la conforma, en poco tiempo dejaría de existir o se disolvería.

Es por esto que el tener políticas de seguridad en las organizaciones es una manera de dar continuación y sustento a las diferentes actividades y trabajo que se realicen, de esta manera también se busca el dar alcance a los objetivos y metas particulares que dicha organización tenga definidos desde su creación.

Por lo general, este tipo de documento se menosprecia ya que no es considerado importante, se emplea como un requisito que se debe llenar; esto es en parte porque el documento en cuestión no fue realizado de una manera apropiada, es decir, está incompleto, es redundante o el contenido es irrelevante.

Cuando se tiene un documento con estas características se presenta la falta de apoyo por parte de los directivos que como consecuencia hace que los usuarios ignoren el documento cerrando el círculo y haciendo que éste sea sólo un documento más dentro de la organización el cual no tiene utilidad alguna, no obstante, es hasta cuando se presenta algún tipo de incidente que provoca pérdidas de algún tipo a la organización, que los directivos se dan cuenta de la importancia de las políticas de seguridad.

El que las políticas de seguridad estén implementadas de manera apropiada es una ventaja clara que facilita y permite que en el momento que se presente algún incidente, la organización tenga la capacidad de retomar el control de la situación limitando las pérdidas y el daño que dicho incidente pudiera causar.

La forma más efectiva en la que una organización puede estar lista para cualquier tipo de incidentes es el capacitar adecuadamente a su personal en el manejo de los diferentes bienes, recursos y la importancia que representa el que se sigan las políticas de seguridad, ya que mediante ellas se tendrá una mejor y más efectiva manera de utilizar y aprovechar los bienes de la organización para la realización de sus actividades, así como el control de diferentes situaciones que se puedan presentar.

Pero la capacitación no sólo ayuda a la mejor gestión y manejo de incidentes dentro de la empresa, esta capacitación crea una conciencia de la importancia de los bienes y de su manipulación tanto dentro como fuera de la organización.

El que el personal tenga una conciencia del alto valor de su información personal y el que tenga una apropiada gestión de ésta permite la mejor y más efectiva protección de la información a su cargo confiada por parte de la empresa así como la propia.

Un ejemplo de la falta de esta conciencia se encuentra en una nota publicada el 27 de enero del 2009 en la página del CERT UNAM.

En esta nota se menciona el hecho de que una persona de Nueva Zelanda compró un reproductor de música el cual tenía almacenado archivos sobre misiones y datos del personal militar perteneciente a las fuerzas armadas de los Estados Unidos. Una reportera de este país intentó contactar al personal militar mediante el uso de esta información, lo cual logró con suma facilidad, ocasionando que el gobierno de los Estados Unidos se comunicara con CNN para aceptar la existencia de dicho dispositivo, se confirmó que el gobierno no está protegiendo de manera adecuada la información. Expertos de ese mismo país comentaron que a pesar del esfuerzo realizado para la protección de información sensible, es un problema que está creciendo.

Este es un ejemplo claro de la falla en la implementación de políticas de seguridad dentro de este organismo y de qué tan peligroso puede ser el que información sensible no sea protegida de manera adecuada cuando ésta es transportada en un dispositivo de almacenamiento.

El no implementar adecuadamente o solo de manera parcial es un riesgo para la organización que se puede ver afectada por este tipo de errores ocasionados por la falta de conciencia o la falla en la capacitación correcta del personal. Es importante hacer énfasis en que las políticas son una necesidad básica que tienen las organizaciones para poder continuar con su trabajo, para el crecimiento y el alcance de sus metas y objetivos.

La falla en la capacitación para que el personal tome conciencia de la importancia que tiene dentro de la organización, es una vulnerabilidad que puede ser explotada y causar pérdidas cuantiosas que pueden ser evitadas.



En el siguiente diagrama (Figura 3.1) se presentan algunas de las ideas tratadas anteriormente.

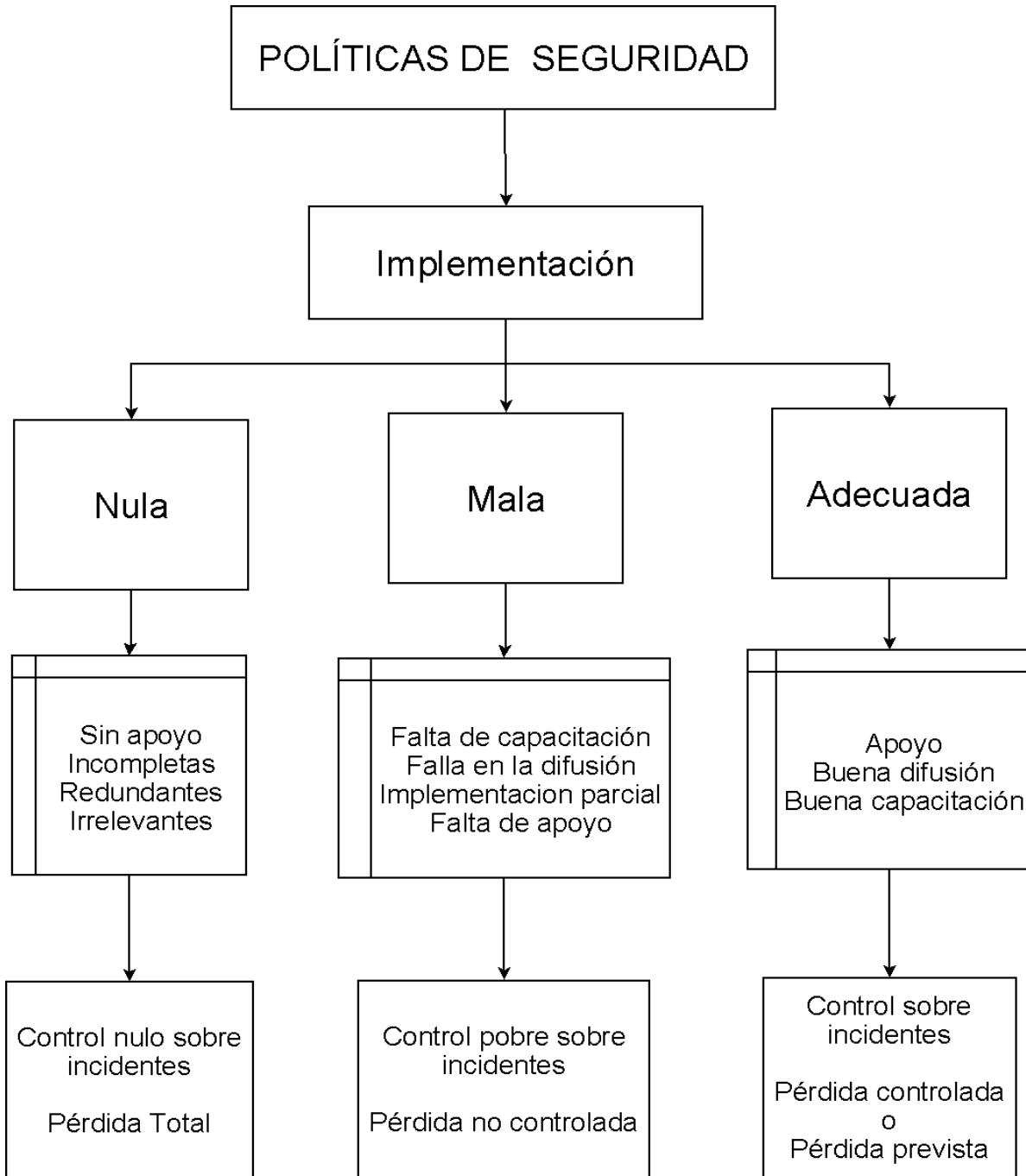


Figura 3.1 Fallas en la implementación de las políticas de seguridad

### 3.1 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 el 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 requiere que se desvíen va-

liosos recursos, por lo que se decide mejor el 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 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, el 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, es 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 seguridad apropiado.

### **3.2 Importancia de revisar periódicamente las políticas de seguridad**

El dar continuidad a un programa de seguridad, el cual consiste en la implementación de seguridad respetando y siguiendo las políticas de la organización para la obtención de un nivel apropiado de seguridad, es fundamental para el éxito de las medidas necesarias que se requieren, es el que exista un seguimiento del trabajo, es decir, que se le dé mantenimiento a todas las medidas y actividades que tienen que ver con la seguridad.

El iniciar un programa de seguridad no es sencillo, requiere que inicialmente se le asignen muchos recursos los cuales serán destinados principalmente a encontrar los diferentes bienes y servicios que son primordiales para la organización, desarrollo, revisión, actualización y difusión de las políticas, la capacitación del personal, el reevaluar y analizar procedimientos, problemas, actividades y posibles cambios en la seguridad, que se renueve el consejo de seguridad que es el encargado de la evaluación de decisiones con respecto a la seguridad, entre otros.

Iniciar un programa de seguridad al igual que muchos programas o proyectos asignándole más recursos al principio, con el paso del tiempo puede que dicha inversión de recursos siga siendo suficiente para que el programa continúe. El que posteriormente se requiera una menor cantidad de recursos, podría parecer una contradicción, sin embargo, no lo es, ya que conforme se implemente y se actualice, la cantidad de recursos se reduce, ya que no es necesario capacitar a todo el personal de manera intensiva puesto que ya fueron capacitados, lo cual representa una gran inversión de tiempo y recursos, no obstante es necesario que se les actualice lo cual es relativamente más sencillo que empezar desde cero, de esta misma manera se requiere el crear o renovar la infraestructura que será la encargada de dar continuidad, difusión, soporte, atención y mantenimiento a dicho programa.

Subsanar la seguridad en una organización no es una tarea sencilla, sin embargo, es una necesidad que debe suplirse, de lo contrario con el paso del tiempo, los pocos controles existentes pueden colapsar, lo cual traería consigo pérdidas para la organización.

En ocasiones las políticas de seguridad han sido olvidadas, es decir, existen pero por falta de actualización éstas han quedado obsoletas teniendo así un vacío en la normatividad e implementación de la seguridad, esto en ocasiones provoca que no haya una cohesión en las diferentes áreas o departamentos, forzando que cada área busque la manera de suplir sus necesidades de seguridad de manera independiente, lo cual crea desorden y confusión.

Por ejemplo, el uso de redes inalámbricas de manera no controlada puede causar interferencia entre ellas si éstas no están reguladas apropiadamente lo que puede producir falta de conectividad, interferencias con la señal, compra innecesaria de más equipos, de esta misma manera el que intrusos o usuarios puedan montar ataques desde una red abierta o mal configurada hacia la misma organización, entre otros.

La existencia de políticas de seguridad y su actualización de manera periódica genera y mantiene un orden y control general, el trabajo de manera conjunta y organizada entre los diferentes departamentos al tener una misma normatividad, es decir, aun cuando los distintos departamentos o áreas estén separados, pueden trabajar de manera colaborativa y más productiva, por otro lado facilita el soporte, mantenimiento, soluciones más efectivas, orientación, asistencia, mejor protección, pronta reacción a incidentes, mejor aprovechamiento de los recursos, entre otras.

Este documento se debe actualizar conforme la organización va cambiando, desarrollando y creciendo, así como implementando y adquiriendo nuevas tecnologías, para que esto suceda es necesario que se realice una revisión periódica y que ésta sea una actividad básica que siempre se encuentre presente, ya que este documento será clave en la implementación de la seguridad, la referencia que se busque cuando se configure un sistema, se requiera implementar algún control, al momento de capacitar al personal, al iniciar algún intercambio de información o en la protección de cualquier bien.

### **3.2.1 Proceso de revisión de las políticas de seguridad**

El proceso de revisión de las políticas de seguridad es un proceso cíclico que debe ser reiterado cada cierto tiempo con el fin de que las políticas sean más efectivas y se adapten a los diferentes cambios la organización, los cuales se dan por el avance de las diferentes tecnologías que se incorporan a ésta, el nuevo personal, nuevas relaciones de trabajo colaborativo, crecimiento de la misma organización, cambio de directivos, nuevos retos, investigación, el cambio de actividades, entre muchas otras más.

Antes de iniciar con el proceso de revisión es importante mencionar y hablar acerca del comité de seguridad, ya que es pieza importante en la revisión de las políticas así como la toma de decisiones dentro de cualquier organización.

El comité de seguridad es un grupo de trabajo que puede estar conformado por administradores, jefes de departamento o área, directivos, personal de seguridad así como gente exper-

ta en el tema que cumple con varias funciones con el fin de garantizar un buen nivel de seguridad dentro de la organización basado en las políticas de seguridad.

Algunas de las funciones del comité de seguridad son:

- Otorgar permisos para la realización de auditorías e investigaciones.
- Aprobación de medidas emergentes en caso de algún incidente grave.
- Sancionar al personal de la organización en caso de ser necesario.
- Presupuestar recursos necesarios para los diferentes programas de seguridad.
- Establecer proyectos especiales para identificar amenazas potenciales.
- Reportar a los directivos el estado de la seguridad dentro de la organización.
- Conducir investigaciones para deslindar responsabilidades en incidentes.
- Aprobación de las políticas de seguridad (actualizaciones, cambios y desarrollo).
- Análisis de situaciones, problemas, incidentes para su solución y prevención.
- Revisión y actualización de las políticas de seguridad.

Esta última actividad cuenta con tres puntos sumamente importantes:

### **1. Tiempo entre cada revisión**

El tiempo entre cada revisión debe ser entre seis meses y un año según lo maneja Scott Barman<sup>4</sup>, un experto en la rama de políticas de seguridad, él aclara que el tiempo para la

---

<sup>4</sup> Scott Barman, Writing information security policies, New riders, Capítulo 13.

realización de dicha revisión no es una regla, sin embargo, afirma que este periodo de tiempo es suficiente para descubrir y saber si las políticas implementadas están funcionando, qué tan efectivas son, cuáles no están funcionando y qué hay que cambiar.

Debe tomarse en cuenta que este periodo varía dependiendo de las necesidades de la organización, el personal con el que se dispone y algunos indicadores como son SLE, (Single Loss Expectancy) o la pérdida esperada, y el ARO (Annual Rate of Occurrence) o el índice anual de ocurrencia, estos índices hacen referencia a las pérdidas aceptables y a la estadística de incidentes que ocurren en un año.

## **2. Formación de un comité de revisión**

Teniendo en cuenta que el periodo ya se cumplió, es necesario formar un comité de revisión de las políticas, lo cual puede parecer redundante ya que ya se tiene un comité de seguridad sin embargo, es necesario y es una de las obligaciones del comité de seguridad.

El comité de revisión puede ser el mismo comité de seguridad, es importante que se tenga un contacto cercano con los administradores y el personal encargado de los diferentes laboratorios, departamentos, edificios, cualquier otro involucrado o quien quiera involucrarse en la revisión y que posea conocimiento sobre seguridad informática, incluso los diferentes usuarios pueden formar parte de la revisión.

Si todo el personal conoce las políticas de seguridad, es una clara ventaja que pueden realizar sugerencias que serán canalizadas de manera ordenada. Por ejemplo, si un usuario tiene una sugerencia, ésta puede realizarse de manera formal y bien fundamentada al administrador o jefe de área o departamento, quien la analizará y comentará con otros administradores o jefes, ellos elaborarán un reporte con las observaciones y comentarios que se hará llegar al comité de revisión el cual discutirá y tomará en cuenta para la actualización, este proceso facilita mucho la revisión al condensar y filtrar las observaciones acerca de las políticas, haciendo que todo el personal participe en la revisión.

## **3. Evaluación de las políticas implementadas**

Una parte importante de la revisión es la opinión de los encargados de la implementación de las políticas como lo son los administradores los cuales harán sus observaciones acerca

de éstas y de los distintos problemas con los cuales tienen que lidiar. Así mismo el hecho que ellos reporten incidentes que pasan en sus departamentos, problemas en la implementación, experiencia, y el cómo afectan las políticas en sus áreas, las diferentes necesidades de seguridad que ahora requieren que no estén contenidas en las políticas facilita la revisión.

El escuchar este tipo de comentarios, las auditorías que se hagan, respuesta a incidentes, todo tipo de problemas, nuevas tecnologías requeridas, necesidades de los diferentes departamentos, fallas en la seguridad, experiencia, los reportes de seguridad hacen que la revisión y actualización de las políticas de seguridad sean más efectivas.

Todas las áreas o departamentos de una organización deben participar activamente en la revisión, es conveniente realizar una junta con todos los involucrados explicando lo que se busca, cómo es que pueden participar, qué tan importantes son para la revisión y mencionando que sus comentarios serán tomados en cuenta por mínimos que sean ya que son importantes para la realización de la revisión, incluso es adecuado incrementar la participación e invitarlos a formar parte del comité de revisión.

Una revisión periódica puede ofrecer más claridad, ser más fácil de asimilar y entender así como explicar de mejor manera los procedimientos, considerar algunos que no lo estaban y adjuntar otros, de manera que el documento a lo largo del tiempo mejore para beneficio de la organización.

Las políticas de seguridad son un documento clave para que éstas puedan ser leídas por todo tipo de usuarios, de tal manera que sean entendidas y asimiladas fácilmente, que sean concretas y que no sean redundantes, incompletas e irrelevantes, el que puedan ser consultadas con facilidad por los usuarios en caso de duda o búsqueda de aclaraciones, es decir, que si algún usuario busca algún tema o párrafo en específico, pueda ser consultada la información de manera rápida y sencilla, el que sea un documento fruto del esfuerzo conjunto de toda una organización, permite que éste ayude de manera substancial al usuario cuando lo requiere o lo necesite, es una meta que la organización debe buscar constantemente.

Es por esto que este documento requiere una redacción apropiada, que sea una opción que ayude al usuario a resolver dudas, que sea una guía cuando se presente algún tipo de incidente, que pueda ser consultado como un documento serio, fácil de entender y no como un documento tan complejo, difícil de entender o con demasiados tecnicismos que nadie consulte; debe ser una meta que toda organización debe buscar.



### 3.3 Correcta redacción de las políticas de seguridad

Una buena redacción de las políticas de seguridad puede ser la forma 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, este tipo 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:

##### a) Prohibitiva

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

##### b) 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.<sup>5</sup>

Es importante mencionar que el escoger una filosofía no sólo es el hecho de optar por alguna de las dos filosofías ya explicadas, es el 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 cerrando cualquier vacío legal por pequeño que éste sea.

## **2. Establecer lo que se debe o necesita hacer y por qué, pero no él 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 de manera adecuada y bien definida sus responsabilidades y hasta dónde llegan éstas. Deben poder responder a las siguientes preguntas de manera sencilla.

---

<sup>5</sup> David Jarmon, A preparation guide to information security policies

[http://www.sans.org/reading\\_room/whitepapers/policyissues/preparation-guide-information-security-policies\\_503](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, chequeos 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 el 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.”<sup>6</sup> 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.

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

---

<sup>6</sup> S, Garfinkel, G. Spafford, Practical Unix & Internet Security, 3rd edition, pág.48

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 el de 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, no obstante, 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 de 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, el 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 el 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 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, el 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 pueden 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, el 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.

## **3.4 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 y salas de cómputo 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 cuentan, 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 el avisar y advertir al usuario sobre los peligros que existen, sino que es primordial el 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, el 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 buscan el aprovechamiento de todos los bienes y recursos de la organización, no obstante, 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 el 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 el 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. El que exista 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.

### **3.5 Las buenas prácticas y las políticas de seguridad**

Puede decirse que las buenas prácticas son parte de las políticas de seguridad ya que están basadas en ellas, es decir, los lineamientos o recomendaciones que son más socorridos, más utilizados, son un enfoque práctico de las políticas de seguridad, sin embargo, este tipo de lineamientos no tienen un carácter obligatorio de ninguna índole, además de no abarcar aspectos de manera total, es decir, sólo son consejos sobre cierta parte de un tema.

Por ejemplo las buenas prácticas pueden hablar sobre la gestión de contraseñas de manera aislada, es decir, hablar de cómo tener una contraseña fuerte, sin embargo, no es su objetivo que el usuario sea capacitado o que siga esta recomendación, no habla acerca de la impor-

tancia que tiene la información y cómo ésta puede afectar, no siguen lineamientos de redacción que pueden ayudar al usuario a entender su importancia, no hay nadie que las haga respetar, no intentan crear conciencia en el usuario que la puede o no seguir, sólo es un consejo, el cual es de manera muy general.

No obstante, las políticas de seguridad mencionan que los usuarios deben seguirlas, se marcan procedimientos acerca de los temas, deberes, qué es necesario hacer en caso de algún tipo de problema o incidente, es decir, la política de seguridad va más allá de sólo dar un consejo o recomendación.

Las buenas prácticas son conocidas también como “best practices” son una manera de protección, sin embargo, no requiere el involucrarse o capacitarse para seguirlas, son una manera práctica de resolver, prevenir o solucionar problemas sin tener que saber el entorno del mismo problema.

Existe una gran variedad de buenas prácticas para todo tipo actividades como son las ventas, seguridad, administración, para mejorar los estudios, etcétera, pero es pertinente el aclarar que no existe una entidad, u organización que las apoye de manera directa, es decir, que este tipo de prácticas o consejos pueden ser basados en políticas de seguridad de empresas, experiencia, los buenos resultados que se obtuvieron al seguirlas pero el que las difunde no puede garantizar que siguiéndolas se obtengan buenos resultados al implementarlas, en otras palabras, pueden traer buenos resultados pero a su vez pueden afectar otras áreas.

Las políticas de seguridad son específicas o muy especializadas para los procedimientos, casos, actividades que se desarrollen en la organización en cuestión, incluso se menciona qué características deben tener los recursos al implementar alguna política, no obstante, las buenas prácticas son generales por lo que pueden variar los resultados que se obtengan cuando éstas se sigan.

Solucionar los problemas de raíz es una característica básica que poseen las políticas, no intentan sólo resolver la situación por la que se está pasando, sino que van más allá y trabajar en la solución a futuro para evitar la repetición del incidente.

No es el objetivo de esta parte desacreditar las buenas prácticas sino es el mostrar que las buenas prácticas pueden ser buenas a corto plazo, ya que no resuelven el problema de raíz y que por otro lado las políticas de seguridad buscan mejorar no sólo una parte de los problemas sino que son una solución integral que tiene como meta el proteger todos los ámbi-

tos de la organización, trabajan en dar una solución a futuro y evitar que vuelvan a cometerse los mismos errores.

El que los usuarios tengan y se promuevan las buenas prácticas, es conveniente ya que se tiene cierta cultura de lo que es adecuado y lo que no debe hacerse en ciertos casos, sin embargo, es mejor contar con políticas específicas que ayuden a la resolución de problemas, incidentes y situaciones que se pueden dar dentro de cualquier ambiente de trabajo.

Contar con políticas de seguridad es una forma más completa y más efectiva de proteger a una organización, ya que el seguirlas trae un beneficio común, es bueno para toda la organización y no sólo para el que las sigue, siendo ésta una gran diferencia existente entre las buenas prácticas y las políticas. Contar con políticas es una ventaja ya que también en éstas se describe cómo manejar distintas situaciones que pueden llegar a ocurrir como son los fenómenos naturales, entre los que se encuentran los terremotos, las inundaciones, erupciones volcánicas, tormentas eléctricas, otros casos como fallas en el suministro eléctrico, incendios, atentados terroristas, asaltos, etcétera.

Es por esto, las políticas ofrecen una solución integral a diversas situaciones que pueden llegar a ocurrir donde lo que se busca es proteger la organización de este tipo de situaciones mediante planes de contingencia.

### **3.6 Plan de contingencia**

La existencia de incidentes catastróficos ha sido un acontecimiento que se ha presentado a lo largo de toda la historia, siempre se ha tenido que lidiar con fenómenos naturales, catástrofes e incidentes que han derivado en pérdidas cuantiosas de bienes y recursos.

Después de cada tragedia comienza un programa de reconstrucción que toma mucho tiempo y una inversión significativa de recursos para que las actividades de ese lugar vuelvan a la normalidad, lo que era antes de aquella catástrofe.

Evitar este tipo de sucesos y otros como lo son los ataques terroristas, sabotajes, epidemias, etcétera, es imposible y no predecible hasta ahora, con esto en mente se han diseñado e implementado planes que buscan el retomar el control o parte de él, aminorar los daños, proteger los recursos y bienes de la mejor manera posible y volver a la normalidad en el menor tiempo posible. Este tipo de acciones que buscan retomar el control de una situación

emergente, prever este tipo de situaciones y estar listo para afrontarlas, se le llama 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.”<sup>7</sup>

A continuación se define este concepto de manera formal

➤ Plan de contingencia

Es la planificación de acciones ante algún tipo de situación que afecte de manera considerable las actividades normales de la organización con el fin de proteger, controlar, reaccionar de tal forma que las actividades, bienes, y personal sean afectados en lo menos posible y restablecer los servicios o actividades en el menor tiempo posible.

El contar con un plan de contingencia es una parte esencial dentro de las políticas de seguridad éste lleva por meta la protección de la organización, el control de los daños así como el restablecimiento de la organización a su estado previo.

Este tipo de estrategia para la protección de la organización debe ser claro en cuanto a la descripción del tipo de incidente o situación y cómo afecte a las diferentes actividades, además de describir las diferentes acciones que se deben implementar, qué se debe hacer, y cómo reaccionar.

Tener este tipo de precauciones es parte de la protección que ofrecen las políticas de seguridad al proteger a la organización de los posibles desastres o incidentes que no ocurren con frecuencia o que no han ocurrido del todo, sin embargo, se tiene contemplada una serie de acciones para contrarrestar o reaccionar ante dichos acontecimientos que pueden generar la pérdida o destrucción total de la organización.

---

<sup>7</sup> <http://sistemas.dgsca.unam.mx>

### 3.6.1 Fases de un plan de contingencias

Existe una metodología para el desarrollo, implementación y mantenimiento de un plan de contingencias, el cual debe contar con ciertas características que se buscan para lograr un buen diseño de éste, las fases que lo conforman son:

#### 1. Fase de diseño

La fase de diseño de un plan de contingencias consiste en el análisis de las diferentes variables que rodean a los servicios, actividades y bienes fundamentales que requiere una organización para poder seguir en el negocio o no ir a la quiebra. En toda organización existen factores críticos que son necesarios para que la organización pueda subsistir.

En esta fase se analizan y encuentran este tipo de factores críticos que permitirán que la organización pueda subsistir y continuar, así como aquellas variables que afecten a la organización de manera severa y cómo poder controlarlas, neutralizarlas o minimizarlas lo más que se puedan de manera viable.

Es importante mencionar que en esta fase el estudio debe determinar la capacidad en cuanto al tiempo que la organización puede asumir la paralización parcial y total, así como la duración máxima de éstas, de la misma forma los tiempos de reacción ante una contingencia y el restablecimiento o la duración del periodo en el que se reanudarán las actividades de manera normal.

Una definición formal de la fase de diseño se describe como la realización de un estudio en el cual se analizan los servicios, actividades y bienes vitales para que la organización, así como las variables que los afectan, para proponer una solución viable que minimice el daño de dichas variables.

#### 2. Fase de implantación

La fase de implantación o también llamado desarrollo de un plan, consiste en la implementación del plan de contingencias que es la etapa en la que todo el planeamiento y diseño de la fase anterior se lleva a cabo. Se realizan las diferentes modificaciones que son requeridas

para cumplir con el diseño, así mismo se realizan las pruebas para cerciorarse de que la implementación está funcionando de manera adecuada, es decir, que la implementación fue exitosa y que todo funciona adecuadamente.

Parte importante de esta fase es la capacitación del personal de la organización en lo concerniente al plan de contingencias, como son el uso de extintores, primeros auxilios, conocimiento de las rutas de evacuación, los diversos procedimientos necesarios a realizar, así como en el conocimiento de los números de emergencia y los servicios de emergencia.

Una definición formal de la fase de implantación consiste en implementar las diferentes medidas que son el resultado de la fase del diseño, así como en la capacitación del personal en el mismo.

Es importante aclarar que la implantación de un plan de contingencias contempla tanto la reacción ante alguna situación como la restauración de las actividades.

### **3. Fase de mantenimiento**

El mantenimiento de un plan de contingencias consiste en dar seguimiento a las medidas planeadas y a las ya implementadas, realizar mantenimiento preventivo y correctivo de los diferentes equipos necesarios en caso de la ocurrencia de alguna situación, también incluye la capacitación permanente del personal, la realización de pruebas, todo tipo de simulacros con el fin de evaluar el desempeño de la reacción ante una emergencia.

A continuación se tiene una definición formal de la fase de mantenimiento; es la serie de diversas acciones por medio de las cuales se busca conservar las diferentes medidas implementadas a lo largo del tiempo, de manera que al presentarse una contingencia, se pueda reaccionar adecuadamente.

La fase de mantenimiento es de suma importancia, ya que sin ésta, todo el trabajo no podría perdurar o conservarse y estar listo en el momento en el que una contingencia llegara a presentarse.



### 3.6.2 Características de un plan de contingencias

Como en todo proyecto o plan, se debe tener una clara idea de qué se quiere hacer, qué se necesita, cuáles son las necesidades a suplir. Sabiendo esto y teniendo una clara idea se procede al diseño de éste que si se diseña de manera correcta puede facilitar y simplificar mucho todo.

El diseñar o planear este tipo de estrategias y procedimientos, así como el prever todo los incidentes que podrían darse en el entorno de la organización no es tarea fácil, ya que deben cumplirse con ciertas características para que sea una plan eficiente y funcional.

Tomar en cuenta las siguientes características en el diseño de un plan de contingencias puede ser muy benéfico para la organización ya que la implementación y el mantenimiento deben ser tomados en cuenta para que el producto sea óptimo, algunas de las características que se deben tener en mente al momento de diseñar son las siguientes:

#### a) Funcionalidad

El plan de contingencias debe ser funcional, es decir, que sea posible implementarlo, que cubra las necesidades requeridas y que los resultados esperados sean óptimos, es decir, que los resultados de la implementación sean buenos en relación con las necesidades.

#### b) Relación Costo - Efectividad

Esta parte se refiere a que los recursos necesarios para la implementación del plan diseñado sean acordes con la eficiencia y efectividad, que los beneficios obtenidos del costo de la inversión sean buenos.

#### c) Flexibilidad

El que un plan de contingencia pueda ser generalizado, que éste pueda ser utilizado de manera genérica o que no varíe mucho y pueda ser adaptado para cualquier tipo de desastre o incidente refleja la flexibilidad que es necesaria en este tipo de estrategia.

#### d) Facilidad de mantenimiento

El mantenimiento que debe tener el plan, debe ser bajo, se requiere que su mantenimiento no sea muy complicado y que no requiera recursos o ingresos extras, aun cuando es necesario que esté listo para cuando sea requerido.

Este tipo de características son deseables en todo plan de contingencias, no obstante, esto no necesariamente debe ser de esta manera, en ocasiones un plan de contingencia requiere recursos para su implementación o para su mantenimiento periódico aunque el uso de este plan no sea requerido en mucho tiempo, debe estar ahí listo para cuando se necesite.

#### e) Programa de pruebas

En este punto es necesario mencionar que el mantenimiento debe incluir un programa de pruebas para tener la seguridad de que los mecanismos implementados son los adecuados y de que funcionan perfectamente.

#### f) Continuidad de la organización

El que la organización vuelva a la normalidad en todas sus actividades debe ser uno de los puntos que se debe tomar en cuenta cuando se diseña un plan de contingencias ya que es necesario que la organización restablezca sus funciones y vuelva a la normalidad en el menor tiempo posible ante la presencia de una eventualidad.

#### g) Respuesta organizada

El que el personal tenga la capacidad de reacción ante una eventualidad como lo es una catástrofe, es prueba de que existe una buena capacitación mediante la cual cada persona tiene una responsabilidad bien definida y sabe qué y cómo debe hacer al presentarse cierta situación. Lo cual hace que la respuesta del personal de la organización sea ordenada, rápida y efectiva ante cualquier eventualidad.

Seguir y buscar estas características mientras se diseña un plan de contingencias garantiza que este plan tenga éxito y que la organización esté protegida de una mejor forma, sin embargo, existen algunos puntos a considerar y que todo plan de contingencias debe contener

ya que es necesario que se tenga un panorama general de las necesidades que se tienen para poder suplirlas y que el plan sea exitoso.

La realización de un análisis de los bienes, recursos y servicios que la organización tiene y presta es necesaria para poder contar con un diseño integral que proteja a la organización de manera que nada quede sin ser tomado en cuenta, algunas acciones que ayudan a realizar dicho análisis son:

1. Evaluación y análisis de los bienes críticos o más vulnerables a las situaciones o desastres, de tal forma que se tenga una idea clara de las necesidades de dichos bienes y cómo pudieran ser afectados.
2. El establecimiento de un periodo de recuperación, de tal forma que se conozcan los servicios y actividades que son vitales para la organización, el tiempo máximo en que se necesita el recuperarlos para la minimización de las pérdidas.
3. El tener bien definidas las diferentes actividades necesarias para que la organización pueda seguir si no de manera total a sus actividades, sí de manera básica, así mismo el tener definidas y categorizadas las actividades para un regreso progresivo a la normalidad.

La necesidad de tener un tipo de metodología en la que todas las actividades, procedimientos, las diversas acciones, la forma en que se establecen lleven un orden, es necesaria dentro de toda organización para el mejor control, gestión, y administración de éstos.

Estándares a considerar  
para la redacción de las  
políticas de seguridad

## **4. Estándares a considerar para la redacción de las políticas de seguridad**

A través del tiempo las organizaciones han desarrollado metodologías y estrategias para trabajar así como desarrollar diversas actividades de manera más organizada y más eficiente; esto aunado a la necesidad de un trabajo de manera colaborativa con otras áreas, departamentos, grupos de trabajo e incluso con otras organizaciones, al tener que compartir, intercambiar, usar, y complementar tareas crea la necesidad de tener criterios, lineamientos y especificaciones para que exista la interoperabilidad.

La existencia de un orden o una estructura facilita que diversos y diferentes grupos puedan realizar trabajo de manera conjunta, esto se debe a que se busca que los grupos de trabajo sean multidisciplinarios.

Es por esto que existe la necesidad de la estandarización de procedimientos, criterios, términos, lineamientos y normas en el desarrollo de productos, actividades y en la forma de trabajo conjunto, es decir, el definir una serie de normas y especificaciones permite que diversos grupos de trabajo puedan trabajar de manera más productiva y organizada. A este tipo de estrategia cuyo objetivo es la interoperabilidad entre diversos grupos de trabajo u organizaciones es denominada estándar.

En el área de seguridad informática existen estándares los cuales son un compendio de recomendaciones que se deben tomar en cuenta al momento de implementar algún tipo de seguridad, sin embargo, aún no existe algún estándar para la redacción de las políticas de seguridad informática, que como se ha tratado en los capítulos anteriores, es sumamente importante para cualquier organización.

La redacción de las políticas de seguridad puede parecer poco importante, sin embargo, el seguir ciertos principios es en realidad una ventaja para una organización, por el hecho de tener la información de manera más organizada y estructurada, facilita su manejo, esto aunado a una estandarización de términos, evita problemas y confusiones, además mejora y agiliza la búsqueda de información así como su consulta y edición.

Tener o llevar un orden (estandarización) en la redacción de las políticas de seguridad es importante ya que el hacerlo asegura que el trabajo y esfuerzo conjunto de las diferentes áreas o departamentos conformados por administradores, personal de seguridad, administrativos y otros expertos en la rama sea más efectivo, y claro para los usuarios que en ocasiones carecen o desconocen de conocimientos relacionados con la seguridad informática.

Un documento claro y que posea una estructura bien definida, de manera que el personal de una organización pueda realizar búsquedas en el documento, consultar dicha información de manera confiable, es una de las metas de las políticas de seguridad, de esta manera facilita el que usuarios, administradores, jefes, directivos, y demás personal que labora en la organización confíen, estén conscientes de la importancia de este documento y conozcan la estructura del documento con el fin de facilitar la revisión, su modificación y la actualización de las políticas.

El que una organización tenga este tipo de documento, es una tarea difícil que por lo general se deja al final por ser una parte tediosa, sin embargo, el contar con documentos bien estructurados es una ventaja clara cuando se requiere realizar alguna actividad, implementación, capacitación, y si se presenta un incidente de seguridad el cual requiere una respuesta rápida por parte del personal así como para la integración de personal a algún proyecto, área o departamento.

#### **4.1 Definición de estándar**

Una documentación sólida donde estén contenidos los diferentes criterios, normas y lineamientos mediante las cuales se regulen los procedimientos y actividades dentro de una organización es indispensable para que se pueda tener una mejor gestión, colaboración, búsqueda, coordinación entre otras muchas más actividades.

Los documentos donde se describen y detallan los procedimientos, actividades, la organización y la operación de una organización con el objetivo de coordinar diversas áreas o departamentos para la realización de ciertas actividades se llaman normatividad o estandarización de procedimientos. Este tipo de documentos parece ser una parte muy formal y tediosa, sin embargo, es sumamente necesaria y útil cuando una organización se expande, crece, tiene algún problema, incidente, cuando existe la necesidad de trabajar de manera conjunta o colaborativa con otra, la adquisición de equipo, contratar o capacitar nuevo personal que se integra, etcétera.

Contar con estándares que ayuden a la integración y la interoperabilidad de departamentos o áreas de una organización, así como a la toma de decisiones y la respuesta a incidentes, es parte de las ventajas de esta metodología. Tener estándares permite dar continuidad, seguimiento, mejora, mantenimiento, actualización, simplificación e interoperabilidad de las diversas actividades, trabajos y productos.

Al trabajar con este tipo de metodologías es enriquecedor para el personal por el hecho de aprender y adquirir conocimientos, es decir, una base de conocimientos básicos que todos comparten, un mismo vocabulario (en ocasiones algunos conceptos pueden manejarse de manera distinta, lo que puede llegar a causar confusión), es decir, una unificación en conceptos, metodologías, procedimientos, de manera que se facilite y agilice el trabajo.

La existencia de un estándar ayuda a que el personal que ingresa a una organización se incorpore, que ayude al crecimiento y al alcance de los objetivos de la organización de una manera más dinámica, de la misma forma el que exista la continuidad de un trabajo o la necesidad de suplir ciertas necesidades existentes así como la no dependencia de un grupo o persona para la realización de cierto trabajo, que nadie más sabe cómo hacerlo.

Es pertinente el aclarar que un estándar es un sinónimo de la palabra norma, es decir, estándar es una palabra proveniente del idioma inglés que con el paso del tiempo se ha incorporado al castellano. No obstante que dichas palabras significan lo mismo, la palabra estándar es utilizada cuando se requiere formalidad, esto es, el uso que tiene de manera internacional, es decir, la palabra estándar es usada para denotar más importancia, una formalidad más rigurosa pese a que las dos significan exactamente lo mismo.

A continuación se define este concepto de manera formal.

➤ Estándar

Es una estructura bien definida de criterios, especificaciones y lineamientos en la que se describen procedimientos, características, metodologías, referencias, y definiciones para establecer una uniformidad en el desarrollo de actividades y trabajo de manera conjunta.

Basarse en un estándar en ocasiones puede crear descontento por el hecho de requerir formalismo para diversas actividades, sin embargo, esto no es del todo correcto, pues existen ventajas como se mencionan a continuación: la existencia de estándares implica el desarrollo de actividades de manera más ordenada, se busca que todo el personal que labore en la organización pueda dar un seguimiento al trabajo previo, es decir, que no requiera la inversión de mucho tiempo para encontrar la información necesaria al desarrollar algún trabajo o actividad necesaria, con esto se busca que la curva de aprendizaje se disminuya de manera considerable.

## 4.2 Estándares que existen respecto a las políticas de seguridad

Los estándares existentes a nivel internacional que hacen referencia de manera directa a las políticas de seguridad informática, es decir, que tratan o abordan estos temas son las normas ISO 27001 e ISM<sup>3</sup> (Information Security Management Maturity Model, lo que se puede traducir como Gestión de Modelos de Madurez de la Seguridad de la Información), también conocida como ISM3 que es la abreviación y mezcla de sus siglas en inglés por contener al último de esta tres palabras que inician con la letra M.

### a) ISO/IEC 27001<sup>8</sup>

La norma ISO/IEC 27001 que es una colaboración entre la Organización Internacional de Estándares y de la Comisión Internacional de Electrotécnica publicada en el 2005, es un esfuerzo conjunto dirigido a la estandarización de los controles requeridos para el establecimiento y mantenimiento, así como para la mejora en los Sistemas de Gestión de la Seguridad Informática (SGSI), que es el término central manejado por esta norma cuya finalidad es el gestionar, administrar o encargarse de la seguridad informática mediante un proceso sistemático y documentado para llevar un orden

Esta norma busca que una organización tenga un nivel adecuado de seguridad en el cual se conozcan los riesgos a los que la organización está expuesta, se asuman, gestionen, y se minimicen en lo posible de manera estructurada, ordenada, documentada y eficiente.

Para clarificar más la idea de los SGSI en el contexto de la norma ISO 27001, se puede definir de la siguiente manera:

- Es el conjunto de políticas relacionadas con el manejo, administración, dirección, y gestión de la seguridad informática.

### Metodología para la mejora continua

En este tipo de metodología busca la efectividad y eficiencia del proceso de gestión de la seguridad informática dentro de la organización, también busca la adaptación a los cambios que surjan en la organización de manera interna y externa con el paso del tiempo, expresa-

---

<sup>8</sup> <http://www.iso27001security.com/>, 2009



do de otra manera, el enfoque de esta metodología es la mejora continua de los procesos y de su administración.

Para la obtención de esta mejora continua esta metodología establece las siguientes fases.

1. Planear
2. Hacer
3. Verificar
4. Actuar

### **1. Planear (Establecimiento del SGSI)**

Establecer objetivos, procesos y procedimientos que requieren políticas de manera que el riesgo sea reducido y pueda ser manejable, con esto se busca que las políticas diseñadas sean acorde con los objetivos propuestos.

### **2. Hacer (Implementación del SGSI)**

Se busca el implementar y operar la política a través de los procesos, controles y procedimientos necesarios.

### **3. Verificar (Verificación del SGSI)**

Evaluar, comprobar, medir y verificar el desempeño de la implementación realizada en comparación con la política realizando un reporte para su documentación y revisión por parte de la gerencia de la organización.

### **4. Actuar (Mantenimiento del SGSI)**

Consiste en la corrección y prevención de las acciones basadas en los resultados de la auditoría realizada en conjunto con toda la información relevante al tema como pueden ser reportes, observaciones, notas o propuestas.

En el caso de la planeación, ésta consiste en el diseño de políticas necesarias basadas en el análisis previo y en una evaluación de la problemática en cuestión. Seguido de esta fase se tiene la implementación que consiste en la ejecución de los diversos controles ya diseñados, a continuación se comprueba y revisa que la solución al problema sea efectiva a través de una comparación entre los resultados obtenidos y los resultados esperados.

Una vez realizada esta evaluación se procede a la última fase, la cual consiste en el análisis de los datos obtenidos para la realización de los cambios en caso de ser necesarios, en caso contrario se procede a depurar y filtrar aún más los resultados para con esto poder encontrar alguna parte que se pueda mejorar. (Ver figura 4.1)

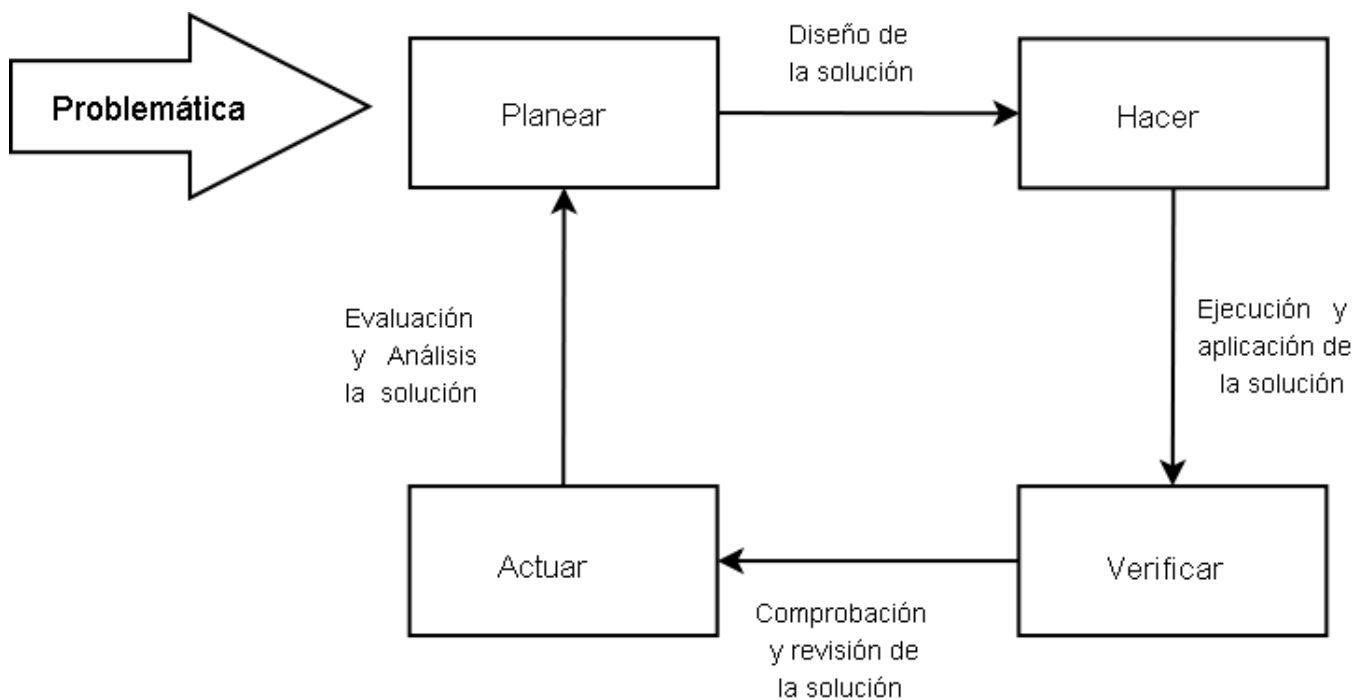


Figura 4.1 Fases de la metodología para la mejora continua.

La norma ISO 27001 es una norma auditable que busca la seguridad de la información y no sólo de los sistemas informáticos, esta norma maneja que la protección de la información no sólo se limita a los archivos digitales, sino a todo tipo de información (Capítulo 1.1

Conceptos básico de la seguridad informática). La norma define este concepto de la siguiente manera:

“Se entiende por información a todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.”<sup>9</sup>

Crear una conciencia de la importancia de la seguridad, crear documentación adecuada conforme se avanza en la implementación y mejoramiento de la seguridad, así como tener los controles que se requieren para tener un nivel apropiado de seguridad son algunas metas y objetivos de esta norma.

#### **b) ISM<sup>3</sup>** <sup>10</sup>

En el caso de ISM<sup>3</sup> o ISM3, es un estándar que busca la creación de sistemas de gestión de seguridad basados en procesos, es decir, busca detectar procesos o actividades dentro de la organización que afecten la productividad, la calidad, la eficiencia o causen algún efecto negativo dentro de ésta. Esta metodología se basa en niveles de madurez (cinco niveles), que son la inversión y alcance de un nivel aceptable de seguridad con la función de cubrir las diversas necesidades de seguridad, invirtiendo en ésta de manera rentable, por lo que es una metodología bastante flexible.

ISM<sup>3</sup> es compatible con diversos estándares a nivel internacional como son ISO 27001 y la serie ISO 9000 sobre la calidad del servicio, además este estándar busca aprovechar documentos, políticas y trabajos previos para la mejora de la seguridad y la eficiencia en los procesos.

Algunas de las ventajas que ofrece es que trabaja basado en procesos que buscan ser medibles para así poder cuantificar la eficacia de éstos, es decir, busca la creación de normas, indicadores o políticas medibles para ayudar a la organización, otra ventaja es que no se requiere una gran inversión, por lo que puede ser una opción para todo tipo de organizaciones que ya tienen un trabajo previo con respecto a la seguridad y que quieren mejorarla.

---

<sup>9</sup> [http://www.iso27000.es/doc\\_sgsi\\_all.htm](http://www.iso27000.es/doc_sgsi_all.htm)

<sup>10</sup> <http://www.ism3.com/>

Las recomendaciones de este estándar son de gran ayuda para el desarrollo y para la mejora en el desempeño de la seguridad dentro una organización, sin embargo se debe ya tener un trabajo previo a esto. Esta metodología no requiere un análisis de riesgos, lo que agiliza y baja los costos de la seguridad, no obstante es importante tomar en cuenta que al no realizar un análisis a profundidad deja muchas vulnerabilidades sin descubrir, lo que puede causar un incidente grave.

El uso conjunto de estas dos estrategias para la implementación y desarrollo de seguridad en la organización en conjunto es posible, ya que ISM<sup>3</sup> es compatible con la norma ISO 27001, es decir, los controles de esta norma buscan el desarrollo paulatino de las medidas contenidas en la ISO 27001.

### **c) Estándares y recomendaciones respecto a la redacción de las Políticas de seguridad informática (PSI)**

Estas estrategias se encargan de nombrar y describir objetivos y metas, tipos de controles que son necesarios, puntos a contener dentro de las políticas, entre otros. No obstante, no existe un estándar en cuanto a la redacción que éstas deben seguir, como existe en otras áreas, tal es el caso del tipo de controles que se debe tener implementados dentro de una organización, es decir, se conoce lo que se quiere hacer y a dónde se quiere llegar pero no se sabe el cómo.

Es por esto que expertos en la rama de la seguridad informática, especializados en la parte de consultoría sobre políticas de seguridad, han publicado documentos para la revisión, redacción y desarrollo de las mismas, esto aunado a los estándares internacionales relacionados a las políticas, ya mencionados, son de gran ayuda para alcanzar este objetivo.

Los estándares internacionales como la norma ISO 27001 y la ISM<sup>3</sup> hacen mención de los controles de seguridad, políticas, terminología, recomendaciones y definiciones que deben estar contenidos en la documentación para un sistema de gestión de seguridad o SGSI. En el caso de la norma ISO 27001, se trata el tema de políticas de seguridad informática y en el cual se describen de manera general los objetivos y los controles que deben tener, pero no menciona el cómo redactar dicho documento.

En esta parte entrarían las recomendaciones de expertos en el tema de la seguridad, que han desarrollado diversas estrategias, recomendaciones, metodologías para la redacción de las políticas, así como para su revisión y mejoramiento, de estos artículos, escritos y publica-

ciones es de donde se puede echar mano para el establecimiento de un estándar interno o marco de trabajo para la organización.

Algunos de los documento revisados en este trabajo son publicaciones de diversas organizaciones como el SANS, el CERT, Universidades y Gobiernos de España, Francia, Inglaterra y del continente Americano, Microsoft, Symantec, entre otros, así como publicaciones y artículos de consultores expertos en esta rama entre los que están, Scott Barman, Gordon “Fyodor” Lyon, Dancho Danchev, David J. lineman, Simson Garfinkel, Gene Spafford, Alan Shwartz, por mencionar algunos de ellos.

Sin embargo, hay una clara necesidad de estandarizar o de crear un documento que de manera formal pueda contener las recomendaciones más importantes basadas en estas publicaciones desarrolladas por los expertos, de manera que puedan ser utilizados para el mejoramiento y desarrollo de políticas de una manera más estructurada, sencilla, rápida y de manera eficiente que satisfaga las necesidades de seguridad de la organización.

El desarrollo de políticas de seguridad como estándares para la redacción de las políticas de seguridad de una organización varía dependiendo del autor, sin embargo, el objetivo de este documento es el hacer un compendio de las principales y más efectivas estrategias para el desarrollo de un estándar respecto a la redacción de las políticas de seguridad.

Con base en esto se realizó la revisión de diversas publicaciones las cuales resultaron en una serie de recomendaciones vistas en el capítulo anterior. (Figura 4.2)

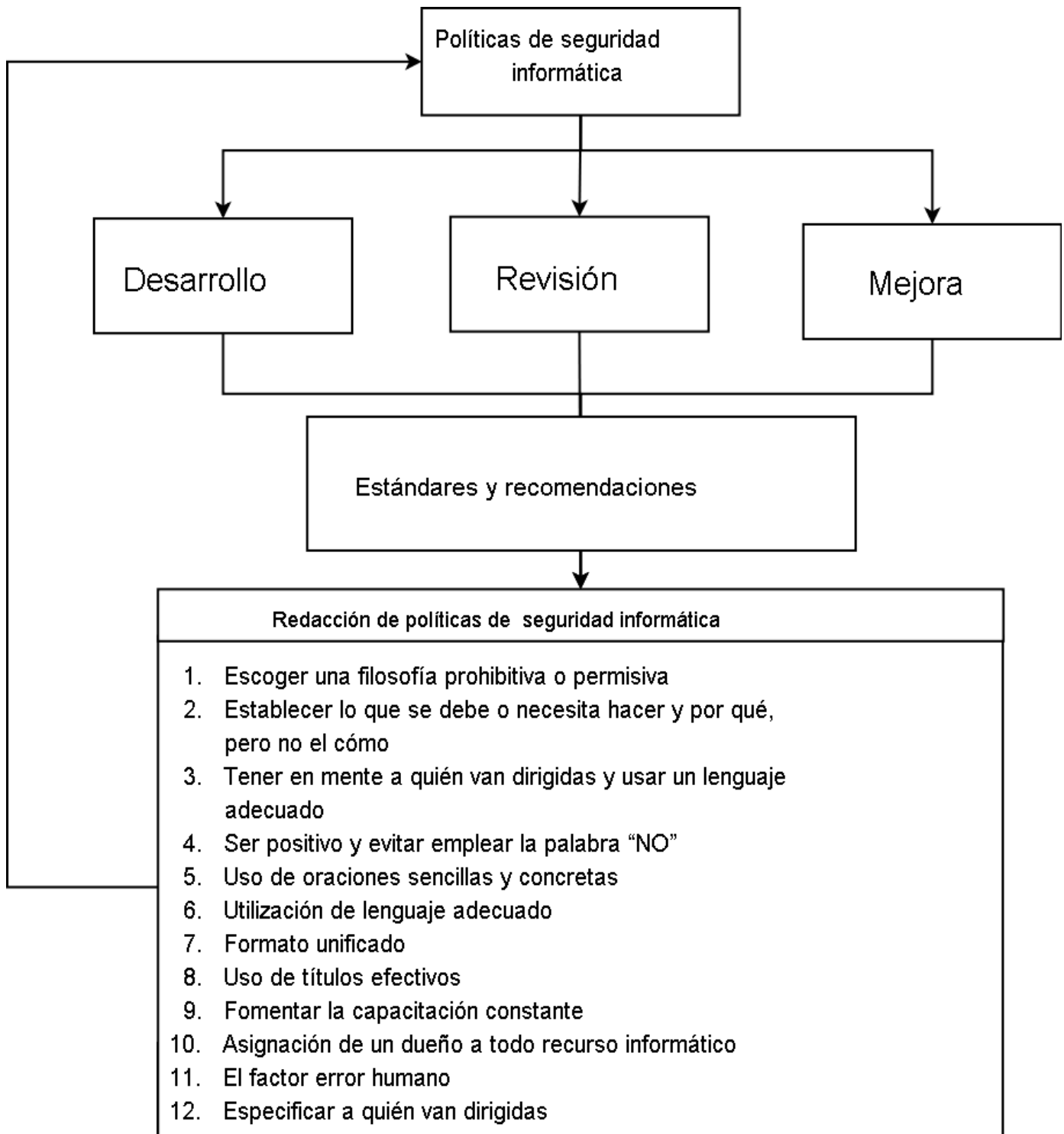


Figura 4.2 Proceso mediante el cual se busca el desarrollo, revisión y mejora de las PSI.

### 4.3 Estándares a considerar en las políticas de la Facultad de Ingeniería

En la actualidad la existencia de un estándar o recomendaciones con respecto al desarrollo y mantenimiento de políticas para la Facultad de Ingeniería (FI), es inexistente por el momento. Para el tiempo (marzo 2003), en el que las políticas que se tienen vigentes actualmente se desarrollaron fueron un gran avance y un gran aporte de los administradores, responsables, directivos y demás personal que se vio envuelto en el proceso para su desarrollo.

Hoy la actualización es necesaria ya que con el paso del tiempo han surgido y se han comercializado (popularizado), diferentes tecnologías que en las políticas actuales no se contemplan, el crecimiento de las redes, la diversidad y especialización de los departamentos, la existencia de nuevos laboratorios y centros de cómputo, la demanda de servicios informáticos.

Las necesidades creadas por la disminución de la productividad, la contaminación de las redes por diferentes tipos de malware, incidentes de seguridad, la generación del tráfico excesivo creado por programas de “peer-to-peer” (P2P), hacía que redes completas colapsaran y que por lo consiguiente tuvieran que ser sacadas fuera de la red, esto aunado a las violaciones que se daban a la propiedad intelectual, acoso, violencia, amenazas, y difamación de manera electrónica, requerían una respuesta inmediata. Por este motivo se decidió el realizar un documento el cual norme y dé respuesta a este tipo de problemas que se venía agravando con el paso del tiempo.

Con el fin de apoyar a la creación de este tipo de documentos surgió un trabajo de tesis titulado:

“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”<sup>11</sup>

En este documento también se anexaron otros como el código de ética informática, el código deontológico en la informática y el código de ética universitario con el fin de que tanto el personal como el usuario final siguiera estos códigos en caso de haber algún punto no considerado dentro de las políticas y que todo el personal por ser parte de la FI tenga en

---

<sup>11</sup> Roberto Carlos Zúñiga Ramírez y Yesenia Carrera Fournier, Estrategias, procedimientos y políticas para implementar la seguridad informática en organizaciones con sistemas Linux red hat caso : unidad de servicios de computo académico de la Facultad de Ingeniería, Tesis UNAM 2003

mente un comportamiento ético y correcto al desarrollar cualquier actividad dentro y fuera de ella, ya que es un representante de la misma.

Este trabajo cuyo resultado fueron las políticas vigentes en cómputo para la FI, tiene como objetivo principal buscar que el usuario haga buen uso de los equipos y recursos computacionales que se le confían, no obstante, el término de seguridad en cómputo hace referencia a una parte de la seguridad informática, la cual sólo busca proteger todo tipo de equipos relacionados con el cómputo.

La seguridad informática difiere de la seguridad en cómputo, ya que ésta última tiene un campo de acción menor, así como objetivos y metas más concretas, es necesario dejar claro que la seguridad en cómputo es una rama de la seguridad informática por lo que comparte las mismas definiciones y bases.

Sin embargo, el hecho de limitar las políticas a un campo menor es una medida establecida con el fin de que las sub-organizaciones que conforman la FI (divisiones, departamentos, y áreas) puedan tener mayor flexibilidad en su trabajo, es decir, que cada una de ellas pueda ser independiente una de la otra, por esto cada una de estas sub-organizaciones cuenta con su propio personal para satisfacer sus necesidades en cuanto al cómputo, por esto, años más tarde se decidió la creación de un organismo independiente que fuera el encargado de la vigilancia de su cumplimiento, el cual busca apoyar, ayudar y coordinar los trabajos en el área de la seguridad.

Este organismo cuyo objetivo es el de ayudar a coordinar, vigilar, asesorar y responder a los incidentes es el Departamento de Seguridad en Cómputo de la FI (DSCFI), el cual capacita y presta servicios para el buen funcionamiento de los equipos y recursos computacionales.

De esta misma forma se creó el Comité Asesor de Cómputo (CACFI) que 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, busca 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.<sup>12</sup>

---

<sup>12</sup> [http://www.ingenieria.unam.mx/cacfi/documentos/art\\_comite.pdf](http://www.ingenieria.unam.mx/cacfi/documentos/art_comite.pdf), 2009



## **Consideraciones para la creación de políticas de seguridad en la Facultad de Ingeniería**

La seguridad informática y la seguridad en cómputo son dos términos que con frecuencia son confundidos por los usuarios, sin embargo, son sinónimos. La seguridad en cómputo es una parte de la seguridad informática, es decir, la seguridad en cómputo forma parte de la seguridad informática, sin embargo, ésta se enfoca principalmente en informar, asesorar, desarrollar políticas y procedimientos así como prestar diferentes servicios de seguridad con la finalidad de reducir los incidentes y problemas de seguridad en equipos de cómputo o asociados a ellos.

Esta rama de la seguridad informática está más enfocada a la seguridad de los equipos de cómputo y recursos informáticos por ser éstos las herramientas más utilizadas para el procesamiento, almacenamiento y transmisión de la información, sin embargo, aun cuando la seguridad en cómputo abarca muchas o la mayor parte de todas las áreas de la seguridad informática, ésta tiene un campo más limitado.

Por lo anterior, definiciones como el de información limitan su campo de acción por lo que la información no asociada o no necesaria para el buen funcionamiento de los recursos informáticos o equipos de cómputo no tiene mucho peso.

Con el fin de ejemplificar esta discrepancia, la información que el usuario tiene sobre datos referentes a la organización como son: horarios de entrada y salida, el lugar donde se guardan llaves, horarios, entradas a las instalaciones, números e información personal sobre los empleados que laboran y datos asociados a ellos, procedimientos no documentados necesarios para el buen funcionamiento de la organización, entre otros, es información que cada sub-organización maneja de manera interna, lo cual es parte de la independencia de la que se hablaba.

Este tipo de consideraciones fueron analizadas al momento de la realización de las políticas de seguridad que se encuentran vigentes, ya que al diseñar y desarrollar este tipo de documentos se deben analizar factores con el fin de que las actividades, trabajos y tareas que se desarrollan en la organización sean afectadas de manera mínima o nula.

Algunas otras consideraciones que se tomaron en cuenta al desarrollar las políticas de seguridad fueron la relación de los sindicatos presentes en la FI, el costo económico y los cambios internos en caso de la creación de un organismo que estuviera a cargo de la seguridad de manera centralizada, la diversidad de actividades que se desarrollan dentro de la organi-

zación, la discrepancia en ideas sobre la seguridad, la falta de recursos y la necesidad de éstos para dedicarlos a la seguridad, la desidia y la falta de interés en temas de seguridad informática. Por lo anterior, se creó y desarrolló el modelo que se tiene actualmente, el cual busca la mejora continua de la seguridad dentro de la FI.

Para la revisión de las políticas fue necesario conocer y recopilar información sobre el origen, las consideraciones hechas por parte del equipo que las elaboró, las limitaciones existentes, las necesidades actuales, el trabajo, actividades y funcionamiento del Departamento de Seguridad en Cómputo (DSCFI), así como el del Comité Asesor de Cómputo (CACFI), de la misma forma las observaciones de administradores que laboran en distintos laboratorios. Esto con el fin de conocer el entorno y las variables asociadas a las políticas vigentes de manera que el trabajo tenga una continuidad.

Se tomaron en cuenta las recomendaciones y observaciones de estándares como ISM3 el cual maneja que el nivel más bajo para una organización como la FI, debe ser el nivel 2 (por el tamaño, la necesidad de seguridad y el rubro de la organización, éste debe ser el nivel mínimo para una organización de este tipo).

Las estrategias, metodologías, trabajos y actividades que se mencionan en este estándar son desarrolladas por el DSCFI y el CACFI que trabajan de manera conjunta con las demás divisiones con el fin de mantener un nivel apropiado de seguridad, sin embargo, es necesario el hecho de que exista más difusión en temas de seguridad dentro de la FI, así como una mejor comunicación con los administradores y encargados de laboratorios pues algunos desconocen la existencia o en caso de conocerla, ignoran el contenido del documento.

Algunas de las acciones necesarias que maneja el ISM3 son el monitoreo, el cual en las PSC de la FI fue uno de los puntos que se actualizó con el fin de clarificar su importancia y su propósito, esto es, el análisis del tráfico en las redes así como su monitoreo con el fin de detectar amenazas, corregir y prevenir problemas de diferentes índoles en la red de la FI.

De la misma forma ISM3 define, maneja y clasifica términos como son:

a) Objetivos de la seguridad → Continuidad, Prevención de pérdidas en activos, Rentabilidad, Mantenimiento del renombre de la organización, Protección del derecho de autor, Protección de la privacidad.

b) Tipos de Amenazas → Error Humano, Incompetencia, Fraude, Corrupción,

c) Metas de la seguridad → En este caso se manejan estadísticas como por ejemplo el alcanzar tasas de robos y pérdidas económicas del 1% anuales.

Con la finalidad de actualizar las políticas se revisó el estándar ISO 27001 e ISM3 en sus partes concernientes a políticas de seguridad y se tomaron en cuenta las observaciones, publicaciones y artículos de expertos y personal que labora en la FI (DSCFI, administradores y responsables de distintos laboratorios), con la finalidad de realizar una propuesta de actualización, la cual sea analizada por el CACFI para su modificación en caso de ser necesaria y posteriormente aprobada.

#### **4.4 Revisión de las políticas de seguridad informática de la Facultad de Ingeniería**

La revisión de las PSC que se presenta en este trabajo tiene como finalidad la realización de una propuesta de actualización que busca ser de ayuda a los administradores, responsables y encargados. La base y justificación de los cambios realizados para la actualización de las políticas de seguridad son con base en la investigación realizada ya previamente presentada.

Por otra parte también se pretende el sentar una base y manual para futuras revisiones y actualizaciones para dicha políticas, las cuales tendrán que ir cambiando y mejorando paulatinamente con el paso del tiempo. Es importante aclarar que siempre existirán fallas y vacíos por llenar, sin embargo, el objetivo de este documento es minimizar esas fallas al proponer una metodología para mejorar y crear conciencia de la importancia que éstas tienen para la organización.

Este documento busca ofrecer una ayuda clara para las distintas áreas, departamentos, laboratorios y divisiones para el desarrollo, mantenimiento y mejoramiento de reglamentos internos, políticas, o normatividades.

Algunos de los puntos más importantes para esta revisión de las PSI de la FI son los siguientes:

✓ **Redacción de las políticas con base en las recomendaciones ya mencionadas.**

La revisión de las políticas usando recomendaciones tiene como finalidad hacer que la lectura de éstas sea más fácil de entender, además de evitar interpretaciones personales haciendo que el documento sea lo más claro posible.

✓ **Incluir en las PSI un apartado sobre la gestión de contraseñas.**

El incluir un apartado sobre la gestión de contraseñas que describe las estrategias para la protección de éstas que son mecanismos para el acceso a recursos de todo tipo como son el correo electrónico, cuentas bancarias, cuentas en equipos de cómputo, información personal entre otras. Conocer las técnicas, recomendaciones y estrategias para la protección de contraseñas evita y minimiza el que puedan ser utilizadas para cometer ilícitos o utilizarlas de manera indebida para ocasionar distintos tipos de pérdidas.

✓ **Incluir políticas para las redes inalámbricas.**

La falta de políticas que contengan recomendaciones y regulen el uso, administración y crecimiento de las redes inalámbricas son necesarias por el hecho de ser un punto desde el cual se pudiera presentar algún incidente de seguridad. Por otro lado, tener políticas que gestionen de manera apropiada estas redes permite tener un mejor aprovechamiento de las mismas.

✓ **Esclarecer las funciones que tiene el departamento de seguridad en cómputo como organismo independiente existente en la Facultad de Ingeniería.**

La función del departamento de seguridad en cómputo como un organismo independiente de cualquier área, que cuenta con personal capacitado, dar apoyo, respuesta y seguimiento ante un incidente de seguridad, así como asesoría y apoyo técnico cuando sea requerido.

✓ **Realizar un documento más claro y accesible para usuarios con un menor conocimiento de la seguridad informática.**

El que usuarios ajenos al área de la informática y el cómputo sean capaces de entender la importancia de toda la seguridad de la información, con el fin de que hagan buen uso y protejan de manera adecuada todos los bienes que les son confiado o asignados así como los propios, es un principio básico que es necesario en estos tiempos en que la tecnología se vuelve más popular para la realización de cualquier trámite, pago, consulta, etcétera.

✓ **Crear una conciencia en todos los usuarios acerca de la seguridad informática.**

Hacer que los usuarios sepan qué tan importante es su información (número de cuenta, cuentas de correo electrónico, RFC, fecha de nacimiento, dirección, datos de sus familiares, números telefónicos, horarios, cuentas bancarias y bienes en general), cómo protegerla, su uso correcto, cómo reaccionar en caso de algún incidente de seguridad, son consecuencias de la creación de una conciencia acerca de la seguridad informática.

✓ **Incluir a las nuevas tecnologías.**

El que nuevas tecnologías estén contempladas y tengan un procedimiento para que puedan ser implementadas es necesario para minimizar y prevenir algún mal uso, interferencia con otras tecnologías, o el que su utilización pueda causar algún tipo de problemas.

✓ **Incluir políticas para entidades externas.**

Las medidas en caso de presentarse la necesidad de trabajar de manera colaborativa o de requerir la contratación de personal externo para realizar algún tipo de actividad, es un evento que se presenta con más frecuencia. Esto implica compartir recursos informáticos e información con personas externas, por lo que es necesaria la existencia de normas que regulen estos eventos.

✓ **Incluir apartados sobre las buenas prácticas**

El incluir buenas prácticas dentro de este documento busca que responsables y demás personal tengan en cuenta dichas recomendaciones con el fin de mejorar la seguridad y el aprovechamiento de los recursos dentro de sus actividades.

## 4.5 Estandarización de las políticas de seguridad informática de la de la Facultad de Ingeniería

La estandarización de las PSI busca que exista la interoperabilidad y el trabajo colaborativo dentro de la organización, es decir, que haya una mejor comunicación entre las distintas áreas, divisiones, dependencias, departamentos y laboratorios que conforman la FI.

Uno de los objetivos de este trabajo es realizar una propuesta para tener un estándar para la redacción de las PSI, esta recopilación busca facilitar, unificar, simplificar la redacción de las políticas con el fin de mejorar su contenido y hacer que éste sea más sencillo para usuarios con poco conocimiento en el área de cómputo, busca también crear conciencia de la importancia de la información y la manera correcta para su utilización.

El concepto de estandarización dentro de este contexto se puede definir de la siguiente manera:

### ➤ Estandarización

Es la creación, elaboración, redacción, o esclarecimiento de normas y procedimientos dentro de una organización cuyo objetivo es el de simplificar, unificar y especificar con el fin de garantizar el acoplamiento de los distintos organismos que lo conforman.

Las políticas de seguridad en cómputo (PSC) de la FI, aun cuando no están actualizadas comprenden muchos puntos y controles mencionados en la norma ISO 27001 que actualmente está vigente, la cual fue publicada en el 2005, es decir, la estructura y las políticas contenidas son acorde y siguen las indicaciones actuales de la norma ISO 27001, por mencionar algunas de ellas están las siguientes:

- La gestión de Activos → Inventarios, uso apropiado, propiedad de los activos.
- Seguridad de los recursos humanos → Roles y responsabilidad, selección y términos, condiciones de empleo.

- Seguridad física y ambiental → Perímetro de seguridad física, seguridad de oficinas, habitaciones y medios, protección contra amenazas externas y ambientales.
- Seguridad del equipo → Ubicación y protección del equipo, servicios públicos, mantenimiento de equipo.
- Entrega de servicio → Monitoreo y revisión de los servicios de terceros
- Protección contra software malicioso y código móvil → Controles contra software malicioso
- Respaldo → Respaldo de la información
- Gestión de seguridad en redes → Controles de red, seguridad de los servicios de red.
- Monitoreo → Registro de auditoría, registro de fallas.
- Control de Acceso → Política de control de acceso, gestión de privilegios, gestión de la clave de usuario.

Los controles mencionados contenidos en la norma ISO 27001 no son los únicos que están considerados dentro de las PSI de la FI, por lo que el documento que se tiene vigente desde el 2003 es un buen documento ya que contempla muchos de los controles y políticas que se mencionan en una norma posterior (ISO 27001 publicada en el 2005).

Es importante que los administradores y usuarios en general lean todo este documento y no solo el apartado de políticas ya que muchos de los controles que se manejan en el estándar ISO 27001 están incluidos en los postulados y en los códigos de ética. En esta parte del documento se hace referencia a la calidad del trabajo, las responsabilidades sobre el desarrollo de software, el trato hacia los usuarios, la capacitación del personal, la actitud de servicio y los valores deseables en el personal que labora.

Las PSC que se encuentran vigentes están íntimamente relacionadas con las PSI y aun cuando tienen un campo de acción más limitado, estas hacen mención y buscan el poder abarcar otras áreas y campos mediante los códigos, postulados, y principios contenidos los cuales amplían su campo de acción buscando el proteger de una mejor manera los recursos y la información de manera más integral.

## **4.6 Redacción de las políticas de seguridad informática de la Facultad de Ingeniería**

La redacción de las PSC de la FI consistirá en la revisión de las políticas que actualmente se tienen siguiendo las recomendaciones para la correcta redacción de las PSI, las recomendaciones hechas por el jefe del departamento de seguridad en cómputo Ing. Rafael Sandoval Vázquez, y el jefe del departamento de redes y operación de servidores el Ing. Noé Cruz Marín, así como otros interesados en el tema.

Con esto se busca la existencia de un documento actualizado, incluyendo las nuevas tecnologías que se han estado implementando dentro de la FI, se busca también que los usuarios en general tengan un documento que puedan consultar de manera más clara y de manera más rápida.

Por otra parte se desea tener una mejor estructura que ayude a la búsqueda más eficiente y efectiva de temas de interés, de tal manera que el usuario pueda ir directamente al apartado de su interés y que el contenido quede lo más claro posible sin lugar a interpretaciones personales o dudas de ningún tipo.

El que esta información que sólo se busca cuando se presenta un incidente o algún problema sea una lectura más fácil de realizar para un usuario ajeno a la rama de la seguridad informática y que con la lectura obtenga así un conocimiento básico para proteger los bienes a su custodia de una mejor forma así como los propios.

Por otro lado con esto se busca incluir a las PSC de la FI un anexo donde se especifiquen las recomendaciones para la redacción y desarrollo de las PSI las cuales son importantes para la continuidad del trabajo que se viene realizando. Con esto se busca que el usuario este más involucrado en los temas de seguridad que a futuro serán una herramienta muy útil para su vida y desarrollo profesional.



# Revisión de las políticas de seguridad informática de la Facultad de Ingeniería

## **5. Revisión de las políticas de seguridad informática de la Facultad de Ingeniería**

La revisión de las políticas de seguridad es una de las etapas necesarias una vez que las políticas ya están funcionando dentro de una organización, no obstante el tiempo que transcurre desde que éstas ya están implementadas dentro de la organización hasta su primera revisión es variable, ya que no existe un tiempo determinado.

Este periodo de tiempo no está estipulado, sin embargo, el ingeniero y analista de sistemas de seguridad informática Scott Barman opina que la revisión de las políticas de seguridad debe estar dentro de un lapso de entre 6 meses y un año, por el hecho de ser tiempo suficiente para encontrar patrones que requieren algún tipo de ajuste.

El periodo de revisión de las políticas debe ser establecido por el comité de seguridad de manera empírica, dependiendo de diversos factores que afectan a la organización entre los que se encuentran la experiencia del personal de seguridad, las necesidades de seguridad que se tengan, cambios en la organización, el alza en número de incidentes, entre otros.

De esta forma las organizaciones (universidades en Australia y en Estados Unidos), teniendo en mente el hecho de darle seguimiento de manera continua y de manera permanente han ideado una metodología o estrategia mediante la cual se pretende el mejorar las PSI, involucrando a todos los usuarios de manera que ellos junto con responsables, administradores y personal de seguridad informática realicen modificaciones de una manera más dinámica.

Para que esta metodología funcione, todos los usuarios deben haber sido capacitados previamente en las PSI, una vez capacitados todos los usuarios pueden participar en la propuesta de modificaciones, ajustes o cambios para la mejora de las PSI. Las propuestas y observaciones deben pasar primeramente por un primer filtro, el cual consiste en la revisión de dicha propuesta por parte del administrador o responsable donde surgió la propuesta.

Una vez que el personal responsable y administradores acuerdan que la propuesta es viable y que ésta es en beneficio para la organización, acuerdan entregar el trabajo al personal de seguridad que revisa, evalúa, analiza y estudia las observaciones para elaborar una propuesta la cual será presentada al comité de seguridad para su aprobación. (Figura 5.1)

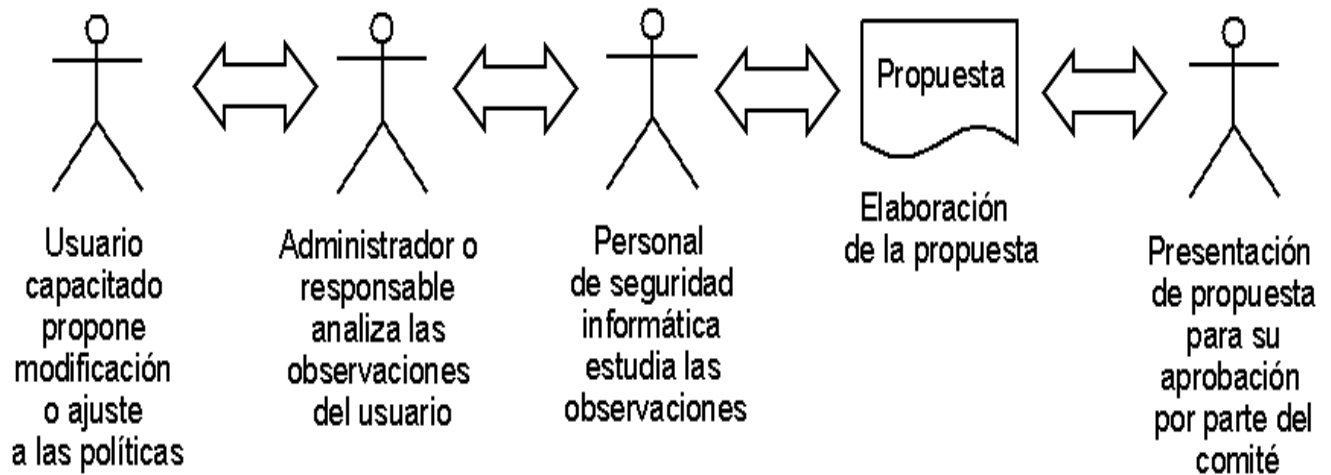


Figura 5.1 Metodología dinámica para la modificación y actualización de políticas.

Esta estrategia está encaminada a la realización de modificaciones pequeñas que consiste en hacer correcciones, pequeñas actualizaciones y ajustes mínimos con el fin de mejorar el documento, hacer que éste sea más claro, incluir algún detalle o algún dato, también puede consistir en actualizaciones respecto a términos relacionados con el tema, etcétera.

La realización de políticas emergentes y cambios es una posibilidad en esta estrategia al encontrarse alguna vulnerabilidad no contemplada con anterioridad que al ser analizada y estudiada por el personal de seguridad fuera de un alto riesgo para la organización.

Es necesario dejar claro que las observaciones o propuestas en ocasiones son hechas principalmente por administradores o personal responsable de implementar las PSI ya que dicho personal es el que tendrá que lidiar y estar más en contacto con los protocolos, recomendaciones, normas, políticas, problemas e inconvenientes que las PSI pudieran causar pues en ocasiones las políticas pueden hacer que las actividades resulten más complicadas por lo que puede ser caso de modificación con el fin de agilizar, facilitar o simplificar dicho proceso.

La segunda estrategia utilizada para la actualización y revisión de las políticas es aquella que es planificada e incluye o requiere que un grupo de trabajo revise, estudie y analice la situación actual de la organización con la finalidad de realizar una propuesta o generar un reporte con ideas, observaciones, políticas, normas o recomendaciones que serán analizadas con el fin de aprobarlas posteriormente por el comité.

Para esta estrategia se busca encontrar posibles problemas o situaciones que se estén presentado en la organización que en un futuro pudieran ser causa de un incidente grave que por medio de su inclusión en las PSI pudiera evitarse, es decir, previene posibles incidentes que pudieran haber quedado fuera en el desarrollo o revisión anterior.

El uso de estas dos estrategias en conjunto o la combinación de ellas para la actualización y revisión de las PSI es una manera efectiva de mantener este documento vigente ya que con una se requiere un trabajo continuo que ofrece como resultado un documento de mejor calidad y que en caso de encontrar algún posible problema, ofrece la posibilidad de corregir dicho error, con la otra se tiene un plan programado que se va trabajando con tiempo y que puede alimentarse con observaciones, notas, información, reportes obtenidos de la primera estrategia.

Existe por último otra estrategia para la revisión de las PSI que se presenta cuando una organización sufre cambios significativos internos o externos, cuando es afectada por agentes o situaciones externas que la obligan a reaccionar o por incidentes graves que afecten sus actividades.

Este tipo de agentes que se llegan a presentar en ocasiones pueden desencadenar una nueva política o una revisión de manera emergente que tiene como objetivo amortiguar los efectos para que la organización pueda seguir adelante. Algunas de éstas pueden ser provocadas por diversas causas, entre las cuales están las siguientes.

- Cambios externos en la organización.
- Cambios en la política de gobierno o legislación.
- Cambios internos dentro de la organización.
- Incidentes recurrentes o graves que afecten a la organización.

Una verificación emergente no busca revisar todas las PSI, sólo reaccionar ante éstas y poder realizar los cambios necesarios para disminuir el impacto del fenómeno o variante que pone en peligro afecta a la organización. Como consecuencia de la presencia de cambio que afecta considerablemente a la organización, suele resultar en la implementación del plan de contingencias durante un tiempo, sin embargo, la revisión de emergencia busca crear o generar una nueva política o serie de ellas que ayuden a la organización a reaccionar

ante dicha situación de tal manera que ésta vuelva a la normalidad y que los cambios sufridos afecten mínimamente las actividades.

A continuación se presenta una tabla que contiene algunas de las ideas más representativas de las tres estrategias para la revisión actualización y modificación de las PSI. (Tabla 5.1)

Tabla 5.1 Estrategias para la revisión, modificación y actualización de las políticas de seguridad

<b>Tipo de estrategia</b>	<b>Ventajas</b>	<b>Desventajas</b>
Dinámica	Participación de todos los usuarios Modificaciones emergentes Corrección de errores	Modificaciones no muy grandes Mas trabajo para administradores
Planificada	Revisión completa de las PSI Estudio, análisis y respuesta a problemáticas que afectan la organización.	Carga más fuerte de trabajo Errores u omisiones serán corregidos hasta la próxima revisión.
Emergente	Modificación para hacer frente a la emergencia y así afrontar la situación	Modificaciones o creación de nuevas políticas sólo destinadas a amortiguar los efectos provocados por un suceso inesperado

La etapa que comprende la revisión de las políticas es un proceso permanente, en otras palabras, tiene que ser un trabajo constante que no tiene fin y que debe realizarse dentro de la organización, con esto no se puede asegurar que no existirán fallas o que no se presentarán incidentes de ningún tipo.

“Even the best policy writers will omit something because it is impossible to predict everything that could happen.”<sup>13</sup>

Esta frase en inglés puede explicarse en español en el siguiente párrafo:

Aun contando con el mejor personal y expertos en la rama de las PSI, se cometerán errores y omitirán puntos, ya que es imposible poder predecir lo que podría llegar a pasar. Siempre existirán fallas en el documento que tendrán que ser depuradas, ajustadas, cambiadas o desarrolladas.

Por lo anterior, la revisión de las PSI es un trabajo continuo y vital para el mantenimiento de un buen nivel de seguridad dentro de cualquier organización, el cual traerá consigo muchas ventajas ya antes mencionadas en este trabajo.

El no realizar la revisión, la actualización o la falta de mantenimiento hace que los usuarios menosprecien y no tomen de manera seria las PSI, esto provocará que con el paso del tiempo los usuarios ignoren este documento hasta que se presente algún incidente grave con repercusiones para la organización.

Esta situación genera pérdidas para la organización, ya que el trabajo y los recursos invertidos para la capacitación del personal se pierden al no contar con una programa de seguridad que carece de una metodología que realice una actualización o una revisión de las PSI, actividad que es igual de importante que los trabajos de capacitación, vigilancia, monitoreo e implementación.

La seguridad informática es trabajo de toda la organización, esto es, debe ser un trabajo continuo que incluye a todos los usuarios (administradores, directivos, personal técnico, operativo, mantenimiento, etcétera), debe ser un proceso proactivo, permanente, constante, que siempre tenga por objetivo estar preparado en caso de cualquier incidente y no un proceso reactivo que sólo actúe o dé respuesta cuando un incidente se presente.

---

<sup>13</sup>Scott Barman, Writing information security policies, New riders, pag. 170.

## **5.1 Por qué es importante una revisión de las políticas de seguridad informática de la Facultad de Ingeniería**

Realizar una revisión de las PSI o PSC de la FI es de gran utilidad ya que el documento actualizado beneficiará a la organización de diversas maneras, algunas de ellas se mencionan y explican a continuación:

### **a) Gestión y aprovechamiento de los recursos**

Tener conocimiento del porqué de las medidas que se implementan y para qué se colocan dentro de una organización facilita el proceso de planificación, diseño, organización y control de actividades con el fin de aprovechar de una mejor manera los recursos informáticos, humanos, y demás activos.

### **b) Mayor difusión**

Contar con la capacidad de proporcionar información a todo tipo de usuarios con el fin de que se capaciten, conozcan y sepan de las políticas, recomendaciones, buenas prácticas, de las nuevas tecnologías, de la importancia de su información personal y de la cual son responsables, tendrá efectos positivos para la organización.

### **c) Capacitación de los usuarios**

Usuarios bien capacitados son capaces de mejorar los procesos, cuidar de una mejor forma los equipos y la información que se les confía tanto para la organización como para la propia, de manera que las pérdidas, malos manejos, errores, e incidentes de todo tipo disminuyan.

### **d) Compra o adquisición de equipo**

Las PSI contienen recomendaciones que al momento de adquirir un equipo se deben tener en cuenta con el fin de cumplir ciertos requerimientos, por esto, la compra de equipo debe ser evaluada no sólo en el costo económico sino también en qué tan bueno y efectivo será para el trabajo en el que se utilizará.

### **e) Minimización de posibles incidentes**

El que se contengan nuevas políticas, recomendaciones, buenas prácticas y artículos que ayuden a los usuarios en general a saber lo importante que es el tener conocimiento acerca de la seguridad informática, es decir, una capacitación adecuada con la cual al paso del tiempo se cree una conciencia que minimizará los incidentes.

La capacitación de usuarios en general es de gran importancia ya que incidentes y problemas pueden ser evitados y corregidos mediante una capacitación adecuada. Este tipo de beneficios obtenidos por la difusión y capacitación de los usuarios es importante; un ejemplo de esto es una unidad de médicos cuyas actividades requieren el uso de equipos personales de cómputo.

Con cierta frecuencia se presentan problemas con sus equipos a causa del malware, el cual se propaga al usar memorias USB (USB flash drive), para copiar y transferir archivos de un equipo a otro. Este malware es difícil de erradicar, hace las computadoras más lentas y en algunas ocasiones se presenta la pérdida o eliminación de archivos de las mismas, por esto, es conveniente que uno de los médicos que realiza actividades sea capacitado acerca de los diferentes tipos de malware, el cómo se propaga este tipo en específico, como evitarlo, las repercusiones y consecuencias así como las medidas que puede tomar en caso de que algún equipo esté infectado.

Como resultado de la capacitación es posible notar cómo disminuyen los incidentes y las fallas en los equipos, es posible que él prestara ayuda a los colegas que acudieran a él en caso de contaminarse con algún tipo de malware.<sup>14</sup>

De la misma forma, capacitar a los usuarios acerca de la seguridad informática y la importancia que tiene es de gran ayuda para tener la capacidad de prevenir y reaccionar ante incidentes que por mínimos que éstos sean pueden afectar de manera grave las actividades.

La actualización de las PSC de la FI es de gran importancia ya que se busca que los usuarios en general creen una conciencia sobre estos temas, lo cual ayudará a prevenir accidentes y capacitará a éstos para reaccionar de manera adecuada ante los posibles incidentes que se llegaran a presentar. Es importante añadir que los usuarios en general seguirán procedimientos establecidos por expertos en la rama de la seguridad informática, que en caso de

---

<sup>14</sup> Ver apéndice 6, carta expedida por el médico capacitado.



que estos procedimientos llegaran a fallar, podrán ayudar o auxiliar para resolver dicho problema.

Las PSC de la FI vigentes, datan del año 2003, por lo que no han sido revisadas y actualizadas por cerca de seis años, lo que es una vulnerabilidad y está totalmente en contra de todo lo planteado anteriormente.

La falta de actualización de las políticas en un principio puede causar cierto sentimiento de inseguridad en los usuarios por la falta de actualización en el documento, no obstante, con el paso del tiempo puede llegar a no ocurrir ningún tipo de incidente en el mejor de los casos, lo que provocará confusión y menosprecio por las políticas. Sin embargo, en el momento que se presente un incidente, el usuario recurrirá a ellas para responder al mismo, lo que se hubiera podido evitar al tener una conciencia de la importancia de las PSI.

Al no contar con un programa que contemple la revisión de las PSI es posible que éstas se consideren o se hagan obsoletas, poco fiables e inservibles en algunos casos al momento de implementar algún programa de seguridad, al configurar un servidor, mecanismo de seguridad o herramienta para el monitoreo de una red.

Esta falta de lineamientos para la implementación o configuración de cualquier equipo, software, cuentas, etcétera, hace que el personal pueda configurar de manera incorrecta estas aplicaciones, dejando así a la organización expuesta a cualquier tipo de incidente de seguridad que pudiera darse por un error humano o de manera intencional.

Un ejemplo de esto sería dejar la cuenta de administrador de un servidor de manera abierta o incluso que todos los administradores o personal pudieran acceder a dicha cuenta, lo que ocasionaría la pérdida de información en todas sus formas como son la edición o corrupción de archivos, borrado, copia de archivos personales, acceso a información personal, infección por malware, entre muchos más. Esto podría causar un incidente grave en caso de contener información importante para una organización como un banco.

En el caso concreto de la FI, la falta de normatividad en cuanto a las redes inalámbricas ha creado que dichas redes crezcan de manera descontrolada y que los equipos no estén protegidos ni configurados de manera adecuada. Esto puede provocar que usuarios no autorizados usen estas redes para otros propósitos totalmente ajenos a los que se buscan.

La actualización de las PSC de la FI es una necesidad para el buen funcionamiento, ya que por medio de éstas, el departamento de cómputo de seguridad (DSC), implementa medidas necesarias para la protección de los equipos que funcionan dentro de la facultad así como la

información que contienen éstos y algunos servicios que se prestan para la atención a los alumnos, académicos y directivos.

El buen funcionamiento y aprovechamiento de los recursos que tiene la FI dependen de la aplicación de las PSI que buscan que los recursos estén disponibles para su uso por parte de todos los que integran la facultad.

En ocasiones ignorar o no seguir los lineamientos que se estipulan en las políticas respecto al uso apropiado de los recursos, puede crear problemas dentro de la facultad, un ejemplo de esto es el conectar programas P2P, así como las violaciones a los derechos de autor que son actos que perjudican a la facultad al tener que desviar recursos para solucionar este tipo de incidentes, o al consumir gran parte del ancho de banda en dicha conexión lo cual puede inhabilitar o crear problemas en la red.

Muchos de los incidentes que se presentan podrían ser evitados si los usuarios tuvieran noción o idea de qué tanto pueden perjudicar sus acciones a la FI. Las PSI buscan crear esta conciencia en el usuario con el fin de protegerlo por ser parte de este organismo, esto significa que el usuario forma parte de esta organización aun cuando no se encuentre dentro de sus instalaciones o aun cuando navega por internet sigue siendo parte y representante de la facultad.

Por esto, es que el usuario debe concientizarse de que todo el tiempo, dentro y fuera de las instalaciones, en su proceder y actuar, forma parte de la FI. No obstante esto es en lo último que piensa el usuario (personal que labora o desempeña alguna actividad dentro de la FI, alumno, académico, directivo, personal de mantenimiento, etcétera), cuando realiza alguna acción contenida o no dentro de las PSI.

Este documento que no sólo comprende a personas que laboran con equipos de cómputo y que erróneamente se piensa que está orientado a una parte de la FI, sino que contrariamente a este pensamiento, las PSI están dirigidas a todo aquel que realiza alguna actividad dentro la facultad y que busca proteger todo tipo de bienes (incluyendo la información de todo tipo, recursos, prestigio y nombre, entre otros).

Las PSI deben ser un documento que esté en un ciclo de mejora continua y que sea una guía para los usuarios que busque enseñar y mostrar cuán importante es su información y los recursos que la FI pone a su cuidado. Estos lineamientos y recomendaciones deben poder ayudar a la disminución de todo tipo de incidentes haciendo que éstos sean evitados en lo posible.

Con la revisión de este documento de manera continua se busca mejorar la seguridad dentro del campus y que los recursos, actividades y demás bienes sean protegidos de manera adecuada para garantizar la continuidad del trabajo que se está realizando.

## 5.2 Actualización de las políticas de seguridad informática de la FI

La revisión de las PSC es necesaria para la actualización de este documento ya que actualmente existe una falta de normatividad que podría dar lugar a posibles incidentes, por esto es necesario realizar la actualización del documento que incluya los cambios necesarios para evitar así esos posibles percances que afecten a la FI.

Las fallas o errores en la redacción dentro de las PSC pueden crear vacíos o faltas de normatividad que ocasionan actividades que pueden afectar o causar algún tipo de problemática que afecte a la FI, por esto es necesario realizar los cambios indispensables a este documento para que sea lo más claro posible y no cause ningún tipo de confusión.

Desde que se tiene este documento se han realizado trabajos que no están contemplados en el mismo como la formación del Departamento de Seguridad en Cómputo (DSC), dedicado a la seguridad informática cuya función es el asesorar y brindar seguridad a las redes de cómputo de la FI.

No obstante, es necesario agregar que los asignados para hacer respetar las PSI dentro de la FI son los responsables de cada área y que la función del DSC es la de vigilar, monitorear, notificar y auxiliar a las diferentes áreas, divisiones y departamentos, ya que al ser una organización tan grande y que al prestar diferentes servicios dentro de ella, se estructuró por divisiones, las cuales están a su vez organizadas en sub-organizaciones más pequeñas (áreas, departamentos y laboratorios). Por este motivo, el encargado de hacer respetar las PSC es el responsable de cada área, departamento o laboratorio.<sup>15</sup>

El DSC es el encargado de vigilar y monitorear el tráfico de las redes de la FI, él está preparado para dar seguimiento y responder en caso de presentarse un incidente de seguridad no grave, para el cual se procede a notificar al jefe de área, quien, dependiendo de los procedimientos, dará respuesta al incidente, contando de antemano con el DSC que puede proporcionar asistencia en caso de ser requerida. Si se presenta un incidente de alto impacto o

---

<sup>15</sup> La transcripción de las entrevistas realizadas a los ingenieros encargados pueden consultarse en el apéndice 1.

grave éste se transfiera como un caso especial que deberá atenderse por el Comité de Seguridad de la FI (CACFI).<sup>16</sup>

Por otra parte, es importante añadir que dentro de los servicios que presta a la FI el DSC es el de realizar revisiones, auditorías y análisis forenses en caso de ser solicitados éstos por parte de los responsables del área, departamentos, y administradores de laboratorios, ya que cuenta con el personal calificado para la realización de estas actividades.

Otro punto que se debe incluir en las PSI es la realización de una política sobre las redes inalámbricas que han proliferado en la FI de manera no controlada. La falta de gestión de estas redes es tratada en otro trabajo de tesis<sup>17</sup> que hace mención y un análisis de esta problemática. De este trabajo se desprenden algunas recomendaciones las cuales serán utilizadas para el desarrollo de políticas para las redes inalámbricas (WIFI).

Es necesario también actualizar las políticas con base en los cambios que han surgido dentro de la dependencia, tal es el caso del manejo de los términos empleados que han variado con los cambios internos en la estructura de la misma facultad. Además de esto, para la revisión se aplicarán las recomendaciones para la redacción de las PSI vistas en el capítulo 3.

De la misma forma se crearon algunas políticas y buenas prácticas referentes a las áreas de colaboración conjunta, tecnologías emergentes, actualización de políticas y gestiones de contraseña entre otros.

### **5.3 Propuesta para la modificación de las políticas de seguridad informática de la Facultad de Ingeniería**

La elaboración de esta propuesta, la cual es una revisión de las políticas que actualmente están vigentes, consiste en una actualización de términos basados en los cambios existentes dentro de la organización, además de la aplicación de las diferentes recomendaciones sobre la correcta redacción de las PSI vistas en el capítulo 3.

---

<sup>16</sup> <http://www.ingenieria.unam.mx/cacfi/paginas/presentacion.html>

<sup>17</sup> Guerrero Martínez Edson Armando, Gestión de redes inalámbricas en la Facultad de Ingeniería.

La propuesta aquí presentada fue elaborada con base en diversas recomendaciones que deben estar en todas las PSI, como son los controles contenidos en las normas ISO 27001 y la ISM<sup>3</sup> en la parte referente a políticas. También se revisó el trabajo previo por parte del ingeniero Edson Armando Guerrero Martínez cuyo trabajo de tesis es acerca de la gestión y la problemática de las redes inalámbricas en la FI.

En su trabajo de tesis, el ingeniero Edson Guerrero, realizó un análisis sobre la problemática de la proliferación de las redes inalámbricas en la FI y cómo es que éstas pueden llegar a causar algún tipo de incidente, así como los riesgos que conlleva la falta de una gestión adecuada de estas redes. Además realizó una serie de recomendaciones y redactó un compendio de buenas prácticas, las cuales contribuyeron con la redacción de las políticas sobre las redes inalámbricas.

De igual forma se realizaron entrevistas a los ingenieros Rafael Sandoval Vázquez que es jefe del departamento de seguridad en cómputo y a Noé Cruz Marín, jefe del departamento de redes y operación de servidores, los cuales realizaron observaciones y recomendaciones que fueron tomadas en cuenta para la edición, modificación y actualización de este documento.

Se obtuvo también información sobre los usuarios de la FI para complementar la elaboración de esta propuesta mediante la realización de una encuesta cuyo objetivo es la obtención de datos acerca de qué tanto conocimiento sobre el tema tienen los usuarios, qué capacitación tienen, la preparación en temas de seguridad informática, si tienen noción de la existencia de las PSC de la FI, entre otras.

La encuesta fue aplicada a poco más de 200 alumnos pertenecientes a todas y a diferentes semestres de las carreras que se imparten en la Facultad de Ingeniería durante el semestre 2010-1, presentándose a continuación algunos de los resultados.<sup>18</sup>

#### ***a) Seguridad Informática***

Poco más del 60% de los encuestado definen o entienden por seguridad informática el uso o implementación de mecanismos para la seguridad, confidencialidad y protección de información, datos y equipos, es decir, las respuestas de los encuestados están asociadas a la implementación de mecanismos de protección para las diversas tecnologías de la información (TI), las redes, los sistemas de cómputo y sistemas informáticos, así como para la pro-

---

<sup>18</sup> La encuesta que se aplicó, así como los resultados de ésta pueden verse en los apéndices 2 y 3 respectivamente.

tección de toda la información almacenada, transmitida y accedida por medios digitales. A continuación se presentan algunas de las respuestas de los entrevistados a la pregunta ¿Qué es la seguridad informática?

- Son sistemas informáticos que impiden conocer datos los cuales no comparto
- Es proteger la información personal contra virus y/o programas que deterioran o borran ésta
- Tener antivirus en mi computadora así como vigilancia en la red y uso de antispyware
- Seguridad en las computadoras contra hackers y otros

Acercas de los objetivos y la importancia de la seguridad informática, las diversas respuestas son en su mayoría asociadas a la protección de la información digital contenida en dispositivos electrónicos y sistemas de cómputo con el 60%, a éste le sigue conservar la integridad de la información digital la cual abarca cuentas de bancos, registros escolares, información personal. Figuran también los ataques por virus, gusanos, troyanos, y toda clase de malware, así como intrusiones por parte de expertos en la materia de informática (hackers).

#### ***b) Políticas de seguridades informáticas y buenas prácticas***

Los datos obtenidos acerca del conocimiento de esta área muestran que cerca de un 54% de los encuestados considera que la FI tiene un buen nivel de seguridad, sin embargo, cuando fueron cuestionados acerca de si tenían conocimiento sobre qué eran las buenas prácticas, el 64.5% contestó que no sabía lo que eran, de la misma forma los encuestados indicaron con un 60.5% no saber o no tener conocimiento sobre qué son las PSI.

Con esto en mente los usuarios fueron interrogados con respecto a su conocimiento de reglamentos internos en laboratorios, centros de cómputo, a lo cual sólo un 41% de ellos contestó tener noción o conocimiento acerca de éstos.

Cabe señalar que en cuanto a la existencia de las PSC de la FI, el 87.5% de ellos respondieron no conocer nada al respecto, dato que es muy interesante ya que muestra que la difusión y capacitación con respeto al tema es mínima.

Estos resultados muestran la falta de capacitación de la comunidad de la FI, no obstante, es necesario mencionar que conforme los encuestados son de semestres más avanzados su conocimiento respecto al tema mejora notablemente, principalmente los relacionados con las carreras de computación, eléctrica electrónica, y telecomunicaciones, ya que estas carreras son las que están más en contacto con las tecnologías de la información (TI).

Con la información obtenida de encuestas y entrevistas, observaciones, recomendaciones, los cambios y modificaciones serán tomados en cuenta para la elaboración de la propuesta de modificación a las PSC de la FI, la cual tendrá que ser analizada y modificada en caso de ser necesario para su aprobación por el Consejo Académico en Cómputo de la Facultad de Ingeniería (CACFI), que es el órgano encargado de realizar las revisiones y actualizaciones a este documento tan importante.

#### **5.4 Reestructuración y redacción de las políticas de seguridad informática**

La reestructuración de las políticas es importante, pues con una mejor estructura se busca que la información pueda ser encontrada de manera más fácil y rápida por todo tipo de usuarios que la requieran para la realización de sus actividades.

De esta forma la reestructuración busca hacer más eficientes los procesos no sólo de búsqueda y consulta sino también de actualización y modificación del documento al llevar un orden en cuanto a los tiempos, al proceso de autorización por parte de los responsables, al evitar confusiones con términos de manera que éstos sean claros, determinar las responsabilidades que tiene cada parte, entre otras.

Esto aunado a una buena redacción que esté dirigida a la comunidad de tal manera que tenga un nivel adecuado en cuanto al uso del lenguaje, sin entrar en tecnicismos que hagan que el documento sea tedioso y difícil de entender para un usuario que no posea conocimientos avanzados en el área, buscando siempre que la lectura de éste no represente un problema o que el lector tenga que pasar mucho tiempo para poder entenderlo.

Al considerar a los usuarios (toda la comunidad de la FI) a los que va dirigido y qué tan importantes son para la organización, el que se entienda que la seguridad informática empieza y es posible gracias al esfuerzo de todos y que los lineamientos, recomendaciones, normas, reglamentos, políticas y buenas prácticas son necesarios para que todas las activi-

dades, trabajos, investigaciones, etcétera, deben seguirse todo el tiempo y no sólo cuando esté presente el administrador, responsable o encargado, ya que al hacer excepciones es cuando se puede presentar algún incidente.

Este tipo de incidentes que parecen inocentes y que hacen que los usuarios vean a las PSI como normas absurdas pasan todo el tiempo, un ejemplo de esto es cuando la secretaria del jefe sabe su clave para entrar a la computadora o para acceder a ciertos recursos, lo cual se podría justificar ya que en caso de que el jefe no esté, la secretaria puede realizar ciertas actividades, sin embargo, el que ella tenga la clave es una violación clara de las PSI, ya que podría encontrar información a la que no debe acceder, autorizar movimientos, o bien puede causar algún incidente al no tener la capacitación adecuada.

Una solución para esta situación sería la creación de una política que autorizara a la secretaria para la realización de ciertas actividades, las cuales serían supervisadas por el jefe y no proveer la clave de acceso o contraseña, ya que el uso de éstas es personal.

El uso de contraseñas puede ser comparado con el uso del cepillo de dientes, en otras palabras, una persona no le prestaría su cepillo de dientes a otra, aun cuando ésta no tuviera, o incluso cuando la otra requiera usarlo, la persona en cuestión tendría que conseguir uno nuevo. Es lo mismo y funciona de igual forma con las contraseñas.

Esta reestructuración busca también crear y hacer hincapié en que los lectores entiendan la importancia de las políticas, buenas prácticas, los protocolos para el manejo, uso de todas las tecnologías y cómo es que éstas benefician, ayudan y aplican a todos los recursos que la FI les proporciona.

Finalmente para la revisión de las PSC de la Facultad de Ingeniería se tomaron en cuenta los puntos, recomendaciones, y lineamientos mencionados a lo largo de este capítulo con el fin de realizar una propuesta, la cual se anexa en este trabajo con el título “Propuesta de Revisión, Actualización y Difusión de Las Políticas de Seguridad en Cómputo para la Facultad de Ingeniería”<sup>19</sup>

---

<sup>19</sup> Propuesta de Revisión, Actualización y Difusión de Las Políticas de Seguridad en Cómputo para la Facultad de Ingeniería puede consultarse en el apéndice 4.



# Difusión de las políticas de seguridad informática de la Facultad de Ingeniería

## 6. Difusión de las políticas de seguridad informática de la Facultad de Ingeniería

La difusión de las PSI es parte indispensable dentro de cualquier programa de seguridad informática que se quiera implementar por el hecho de requerir que todos y cada uno de los que conforman la organización formen parte de este esfuerzo conjunto para la generación de un buen nivel de seguridad, el cual trae consigo ventajas para el mejor aprovechamiento de los recursos informáticos de la misma forma al evitar diversos tipos de incidentes.

Se podría pensar que difundir las políticas de seguridad a todo el personal es el equivalente a entregar información que cualquiera pudiera usar para la realización de un ataque, sin embargo, esto no es así.

Para aclarar esta idea se puede decir que publicar las políticas de seguridad es como colocar un cartel para que todos los habitantes de un edificio estén enterados de la importancia de seguir reglas como son: que al salir deben cerrar con llave y que en el caso de que alguno de ellos perdiera dicha llave debe avisar de inmediato al responsable de la puerta.

Esta información contrariamente a lo que se piensa no proporciona algún dato que pueda ser utilizado por algún atacante, sino que por el contrario, le notifica que la puerta está cerrada y que en caso de conseguir o robar alguna llave esto haría que los habitantes informaran de la situación para la realización de acciones preventivas o que corrigieran dicho error.

Al igual que el cartel en el edificio el cual contiene las reglas, explica la importancia de los lineamientos contenidos en él y que puede ser visto por todo el mundo (habitantes, vecinos, invitados y extraños), las políticas de seguridad establecen lo que se debe o necesita y el porqué, pero no establecen el cómo<sup>20</sup>.

Al no establecer el cómo, qué herramientas, dispositivos, y en qué forma se realizó la implementación dificulta la tarea de un atacante al desconocer los tipos de tecnologías, marcas, dispositivos, y herramientas que fueron utilizadas para la implementación de las políticas, esto aunado al conocimiento de la existencia de diversas medidas preventivas y reactivas complica y dificulta más la tarea del atacante, lo que pudiera hacer que éste perdiera su interés por la complejidad, y el costo necesario para la realización de un ataque.

---

<sup>20</sup> Capítulo 3 en el apartado 3.3 Correcta redacción de las políticas de seguridad.

La etapa de difusión consiste en propagar, divulgar y difundir las PSI, así como sus objetivos, metas y beneficios con el fin de crear conciencia en todo el personal de la organización acerca de lo importante que es que se sigan y se respeten aun cuando el personal no se encuentre dentro de la organización.

Para que se cumpla esta etapa es necesario que se tenga en cuenta que existen usuarios, los cuales no tienen un conocimiento básico o poseen limitaciones con respecto al lenguaje relacionado con los temas de la seguridad informática, por lo cual es necesario el uso de un lenguaje, así como términos adecuados mediante el cual estos usuarios puedan comprender a cabalidad, de manera que se les facilite la curva de aprendizaje.

De esta forma al buscar que dichos usuarios entiendan de una manera general estos temas es un gran avance en la etapa de difusión, no obstante es necesario también el motivar a estos usuarios a querer aprender acerca del tema, a que estén interesados de manera que puedan ser capacitados de una mejor y más rápida forma.

Con el fin de motivar y hacer esto posible es necesario mostrar las ventajas o beneficios que se obtienen al seguir las políticas de seguridad, es decir, se debe mostrar a los usuarios la parte práctica en la cual se muestre la eficacia de esta estrategia que busca el no sólo proteger a la organización, sino que va aun más allá protegiendo los activos personales de cada usuario.

Por lo anterior se puede afirmar que la difusión consiste en divulgar la información y el conocimiento acerca de las políticas de seguridad desde un punto más práctico y amistoso, es decir, que busque acercar estos temas al usuario de una manera amigable con el objetivo de motivar a todo tipo de usuario para que se capacite, respete y promueva el uso de las PSI en todo momento tanto dentro como fuera de la organización.

Sin embargo, en ocasiones esto no se llega a concretar, por diversas razones como son la falta de tiempo, de recursos, la falta de personal, la falta de apoyo por parte de la organización, o por fallas en la estrategia de difusión. Los resultados obtenidos provenientes de fallas en programa de difusión son el ver a las PSI como una pérdida total o parcial de tiempo y de recursos por el hecho de que los usuarios no siguen y respetan las políticas, esto en otras palabras; seguir y respetar procedimientos, lineamientos y normas que el usuario califica como “molestas y poco prácticas”.

La falta de resultados es uno de los principales argumentos que pueden ser usados para desacreditar la efectividad de las políticas de seguridad por el hecho de que la gente piensa que esta estrategia resolverá y hará desaparecer cualquier tipo de problema asociado con la se-

seguridad informática, como pasa cuando alguien tiene problemas con los distintos tipos de malware (virus, gusanos principalmente), se piensa que al instalar un antivirus resolverá todos los problemas que tiene el equipo, sin embargo, esto no es así, ya que en caso de que el antivirus no resolviera los problemas, el usuario decide cambiar de antivirus por el hecho de que éste no es efectivo.

En el caso de las PSI, los resultados y la efectividad dependen en gran manera de la participación y capacitación adecuada de todo el personal que conforma la organización ya que en la manera en que cada individuo entienda la importancia de la información que le fue confiada para la realización de su trabajo, así como la propia, estará directamente relacionada con el nivel de seguridad, es decir, entre mejor capacitación y participación del personal haya, el nivel de seguridad será mucho más alto.

Por lo anterior, es necesario que en cualquier organización exista una capacitación adecuada<sup>21</sup> (Tabla 6.1), la cual depende en gran parte de que exista un programa de difusión que tenga el objetivo de acercar al usuario a las PSI.

Tabla 6.1 Casos que se presentan al capacitar al usuario.

<b>Capacitación</b>		
Buena	Mala	Errónea
Bien capacitado tiene una clara idea de lo importante que es la información.	Está expuesto a un posible incidente por no tener una buena capacitación.	Actúa con temor ante cualquier tipo de actividad con la idea de que todo el mundo es un posible atacante que busca robar o destruir su información.
Sabe cómo proteger los activos o bienes tanto propios como los que la organización confía en él.	Propensión a cometer errores que pueden facilitar la pérdida, destrucción, mal uso de la información o el facilitar un incidente.	

<sup>21</sup> Capítulo 3, apartado 3.4 Puntos importantes a considerar en las políticas de seguridad, sobre las ventajas asociadas a un buen documento.

## 6.1 Propuestas para una mejor difusión

La realización de una propuesta efectiva para la difusión de las PSI que provea al usuario con el conocimiento necesario para entender acerca de estos temas y que pueda hacer frente a incidentes de manera que pueda realizar y aplicar medidas preventivas así como reaccionar ante incidentes que puedan acontecer en el futuro.

Con el objetivo de realizar una propuesta efectiva es necesario la obtención de observaciones, comentarios y la retroalimentación por parte del personal de la organización respecto a los conocimientos sobre estos temas, cuáles son las medidas que ellos realizan al tener algún tipo de incidente, dónde sería un buen lugar para almacenar, consultar y distribuir información relacionada con estos temas, etcétera.

El recopilar información del estado de capacitación, conocimiento y actividades del personal es sumamente importante para la realización de un buen programa de difusión. Es por esto que se buscó la obtención de esta información a través de entrevistas a responsables de la seguridad informática, así como encuestas aplicadas a la población en general de la Facultad de Ingeniería con el fin de realizar una buena propuesta.

Para la realización de esta etapa se recomiendan las siguientes acciones, con base en las observaciones realizadas anteriormente, así como de los resultados obtenidos de la aplicación de la encuesta<sup>22</sup>:

### 1. Uso de publicidad

El uso de publicidad que contenga información concreta acerca de las PSC de la Facultad de Ingeniería (FI), esta información puede ser una dirección electrónica donde se encuentre una página, esto con el fin de que la información que contenga este cartel sólo sea para informar al usuario acerca del lugar donde se puede encontrar dicha información, sin embargo, es necesario que el cartel contenga información acerca del tema que indique lo que encontrará y para qué es, así como alguna ilustración acorde con el tema que pueda dar una idea y atrape la atención del usuario.

---

<sup>22</sup> Pueden consultarse los documentos en los apéndices 1, 3 y 2 respectivamente.

Un ejemplo de este tipo de carteles o publicidad se muestra a continuación, en la cual se hace mención de una serie de fallas que pueden evitarse. (Figura 6.1).



**INGENIERIA**  
**FI**

**¿Problemas con tus archivos?**  
**¿Tu computadora actúa de manera extraña?**  
**¿Tu contraseña de correo electrónico es tu fecha de nacimiento o tu número de cuenta?**

**La solución...**

**PSC-FI**

**[www.ingenieria.unam.mx/psc-fi.html](http://www.ingenieria.unam.mx/psc-fi.html)**

The advertisement features the Faculty of Engineering (FI) logo at the top left. Below it are three questions in bold black text. To the right of the questions is a green padlock icon. Below the questions is a USB drive with a skull and crossbones, and several blue virus-like icons. The text 'La solución...' is centered, followed by 'PSC-FI' in red. At the bottom, the website URL is provided in bold black text.

Figura 6.1 Publicidad para difusión de las PSC-FI

Este tipo de errores que los usuarios cometen y los problemas más comunes con los que los usuarios tienen que batallar son una fuente de ideas que se pueden utilizar para ayudar a la difusión y atrapar la atención de los usuarios con el fin de que visiten y conozcan el sitio donde puedan consultar las políticas.

Este tipo de publicidad debe ser puesta en lugares donde exista una gran afluencia de usuarios, es decir, en lugares donde exista un tránsito abundante o en lugares establecidos para la difusión de otro tipo de publicidad donde normalmente los usuarios acudan en busca de información de algún otro tipo.

Con este objetivo la encuesta<sup>23</sup> aplicada a alumnos de la Facultad de Ingeniería (FI), reveló que uno de los lugares donde los alumnos se enteran de información concerniente a diversas actividades además de ser uno de los lugares más frecuentado por los alumnos es la biblioteca, por lo que éste sería un buen lugar para colocar publicidad. De la misma forma se puede realizar algún tipo de publicidad en la página principal de la Facultad donde se

<sup>23</sup> Apéndice 2, Encuesta aplicada a alumnos de la FI, UNAM.

busque y el visitante pueda consultar dicha información en una página especializada acerca del tema.

Algunos otros lugares en donde la comunidad de la Facultad de Ingeniería (FI) busca o se entera de diversos avisos son la entrada principal del Edificio Principal, los lugares que se tienen para colocar publicidad (pizarrones), la entrada de los laboratorios, pasillos y en los salones.

## 2. Pláticas, campañas, conferencias y seminarios

El dar pláticas introductorias a los profesores y académicos de toda la Facultad de Ingeniería (FI), es una de las maneras en las que se puede propagar y capacitar a una buena parte del personal ya que a través de ésta todo el conocimiento llega a los alumnos. Los procedimientos, las acciones y las medidas que los académicos tomen y comenten al momento de trabajar con los alumnos ayudarán a los alumnos y demás personal que labora con los académicos a entender y a consultar las Políticas de Seguridad en cómputo de la Facultad de Ingeniería (PSC-FI).

Estas pláticas pueden ser también impartidas a los alumnos y personal administrativo a lo largo de campañas cada semestre, las cuales abarquen los temas relacionados con las PSI así como temas asociados a la Seguridad Informática, éstos deben ser abordados de manera práctica, es decir, deben ser enfocados a usuarios con un conocimiento muy básico o casi nulo que ayude a comprender acerca de ellos, en otras palabras facilitar el aprendizaje de cierto conocimiento básico con el fin de acercar más a los usuarios a las políticas y a la seguridad informática y que éstos no tomen a las PSC-FI como un documento más.

A lo largo de esta campaña debe fomentarse el uso y consulta de las PSC-FI, además es necesaria la realización de mesas redondas, seminarios o talleres en los cuales los usuarios puedan participar más activamente para comentar sus dudas e inquietudes acerca del tema, las cuales deben ser esclarecidas y contestadas.

Los talleres y seminarios pueden ser organizados por las diferentes divisiones a lo largo del semestre en coordinación con expertos del tema con el fin de que se puedan realizar diferentes actividades como capacitación de personal, desarrollo de políticas, difusión de las mismas, aclaración de dudas, revisión de políticas internas o reglamentos, entre otras.

### 3. Sitio WEB

Como parte de este trabajo se diseñó y construyó un sitio web, el cual tiene como meta ser una herramienta para la difusión de las PSC-FI, con este propósito se ideó que el diseño de dicho sitio esté enfocado a la simplicidad, buscando que auxilie al usuario en la búsqueda, capacitación y enseñanza de información de manera que no sea ajena o tediosa para los usuarios sino que sea una herramienta práctica que promueva el uso y consulta de los documentos (PSC-FI) para la prevención, solución, corrección, e implementación de medidas que ayuden a establecer un nivel apropiado de seguridad informática.

Para la etapa de diseño de la página se siguió la normatividad web<sup>24</sup>, la cual regula la información contenida en las páginas, el uso de logotipos, las imágenes, así como el establecimiento de lineamientos y recomendaciones para el diseño de las mismas. Tomando en cuenta lo anterior y que el sitio que se estaba diseñando contendría información que el usuario debe ver de una manera respetuosa y a la vez ligada con la formalidad de la organización, se optó por el uso de los colores rojo y blanco, por el hecho de ser éstos colores asociados con la Facultad de Ingeniería además de estar presentes en la página principal.

El diseño que se eligió para el sitio fue escogido con base en que lo principal de éste es la información contenida, por lo que se decidió que el contenido debía estar a la izquierda, de manera que el usuario enfocará su atención en esa parte. Se decidió colocar un menú principal en la parte superior que no cambiara para facilitar la navegación dentro del sitio y un menú auxiliar, el cual se encuentra en la parte derecha conteniendo vínculos (links) que tuvieran información asociada con el contenido de la página.

A continuación se muestra un esbozo de la estructura definida anteriormente, (Figura 6.2).

---

<sup>24</sup> <http://www.ingenieria.unam.mx/cacfi/documentos/normatividadweb.pdf>, 2010



Logo FI	Título de la página	Logo UNAM
Menú principal		
Contenido		Menú de navegación
Pie de página		

Figura 6.2 Diseño de la página web

### **Estructura general y organización del sitio.**

El menú principal está estructurado para poder ir a las 4 páginas principales, las cuales están auxiliadas por el menú de navegación que puede o no cambiar dependiendo del contenido del sitio con la finalidad de proporcionar rapidez al momento de buscar información.

A continuación se presenta una breve descripción de las 4 páginas principales y sus contenidos.

#### **1. Inicio**

Es la página inicial en la cual se tiene la bienvenida al sitio, un resumen sobre lo que éste contiene y un mapa general, por último tiene un apartado sobre los requerimientos del sitio.

#### **2. PSC-FI**

Dentro de esta página se encuentra un breve resumen acerca de las PSC-FI, su filosofía, y su objetivo general, también contiene un mapa que ayuda al usuario a navegar por este documento. Cada una de las partes en las que fue estructurado este documento cuenta con una breve descripción con el fin de agilizar la búsqueda de información por parte del usuario, es decir, se facilita la consulta de información.

Se decidió que las PSC-FI fueran estructuradas en 4 partes las cuales son:

**a. Generalidades**

Contiene documentos que tratan acerca de las políticas como la filosofía a seguir, el organismo responsable del documento, los servicios de seguridad que se buscan con la implementación de las políticas.

**b. Políticas**

A lo largo de esta parte se tratan las políticas a implementar dentro de la FI, además de las sanciones aplicables para cada caso.

**c. Buenas prácticas**

Esta parte tiene las recomendaciones para el uso e implementación de algunas de las tecnologías, surge como apoyo para las políticas.

**d. Códigos de ética**

Los códigos de ética son lineamientos que deben seguir el personal y la comunidad en general de la FI, estos códigos contemplan la actitud y la normatividad a seguir por toda la comunidad en todo momento.

**e. Gestión de contraseñas**

Con el objetivo de una mejor organización se buscó que hubiera un apartado el cual pudiera ser de ayuda para la gestión de las contraseñas ya que es uno de los recursos más utilizados de acceso y autenticación.

**f. Glosario**

Es un compendio de definiciones con el fin de esclarecer algunos términos utilizados.

### 3. FAQ

En esta parte se tienen las Frequently Asked Questions (FAQ), lo que en español se puede traducir como preguntas frecuentes, las cuales buscan dar respuesta a las dudas que le puedan surgir al usuario al navegar o ingresar a la página.

### 4. Descargas

La página contiene documentos y archivos como las PSC-FI, una guía para el desarrollo de PSI, un formato para reportar incidentes de seguridad, entre otros.

## **Herramientas y tecnologías utilizadas para la construcción del sitio.**

Para la realización del sitio se tomaron en cuenta diversas consideraciones como el uso de las tonalidades en los colores, un ejemplo de esto es que el fondo, el cual no es completamente blanco ya que un fondo blanco contrasta mucho y puede ser molesto. En cuanto a las tonalidades de los colores utilizados están asociados con la seriedad y sobriedad por el hecho de que el sitio contendrá información que el usuario no debe tomar a la ligera, de manera que esto debe verse reflejado a lo largo de todo el sitio.

En la construcción de este sitio se decidió el uso de Cascading Style Sheets (CSS) u hojas de estilo CSS con la idea de dar estructura al documento, ya que este tipo de código es compatible con todos los navegadores, además de ser un recurso muy socorrido por los programadores de páginas HTML o páginas WEB.

La programación de la hoja de estilo fue de manera externa, es decir, el archivo CSS está referido a cada una de las páginas HTML, con lo que se obtuvo una ventaja al reducir el código, otra ventaja es que al tener un solo archivo CSS se puede cambiar una gran variante en las características del sitio con sólo modificar ese archivo.

Por las ventajas y características que proporciona el uso de las hojas de estilo se decidió su uso, la cual fue programada en bloc de notas o editor de archivo de texto plano.

Las páginas fueron desarrolladas en editores de texto plano, al igual que se realizó con las hojas de estilo CSS, en este caso son archivos HTML y la aplicación (verificador de contraseñas), fue realizado en Macromedia Flash esto con el objetivo de que fuera más agradable para el usuario, además de ser uno de los programas más utilizados en los sitios WEB.

Un punto importante al respecto del uso de esta herramienta para la realización del verificador de contraseñas fue el que Macromedia Flash ofrece software gratuito a los usuarios para la ejecución este tipo de aplicaciones en los diversos navegadores. Esta aplicación tiene el objetivo de ser una herramienta para la ayuda del usuario en el tema de gestión de contraseñas por lo que dentro del sitio se ofrece al usuario el poder descargar un archivo ejecutable para su uso personal.

Por otra parte los archivos a descargar fueron exportados a archivos PDF, ya que el software para leer este tipo de archivos también es gratuito y muy usado para la lectura y consulta en la publicación de artículos, libros electrónicos, reportes, lecturas diversas, etcétera.

Se buscó también que el sitio tuviera un motor de búsqueda interno, es decir, que fuera independiente, además de ser gratuito, por lo que se decidió el uso de PHP para la implementación de búsquedas de información dentro de las páginas del sitio.

Estas tecnologías y herramientas fueron usadas por no presentar costo alguno para los usuarios ni para la organización, además de que son compatibles con los distintos navegadores en sus versiones más recientes, algunos de los navegadores más populares son: Internet Explorer de Microsoft, Mozilla Firefox por Mozilla Corporation, Chrome de Google, Safari de Mac OS X y Opera de Opera Software.

Para que esto fuera posible el código utilizado en el sitio es compatible con estos exploradores en sus versiones más recientes, sin embargo, es recomendable el uso de Mozilla Firefox para la navegación en este sitio, no obstante, cabe aclarar que el sitio es totalmente compatible con el uso de Internet Explorer como explorador, el cual es aun el navegador de internet más utilizado.

Es importante mencionar que para la correcta ejecución del sitio se recomienda que se autorice el uso de los scripts y se instalen algunas aplicaciones como son el Adobe Flash Player (para la correcta ejecución del verificador de contraseñas) y el Adobe Acrobat Reader (para la lectura de algunos documentos). Este tipo de requerimientos ya están contemplados dentro del sitio por lo que el usuario puede consultar y recibir ayuda para la descarga de estas aplicaciones.

Con respecto a la organización y estructuración del contenido de las políticas se procedió a reunir y reorganizar o reestructurar la información acerca de las políticas de seguridad a manera de crear el sitio con el objetivo de que la navegación a través de éste sea lo más funcional, es decir, que el usuario pueda navegar por el sitio y encontrar la información de

la forma más directa y rápida. En la siguiente figura se muestra una vista previa de una de las páginas (Figura 6.3).



## Políticas de Seguridad en Cómputo de la Facultad de Ingeniería (PSC-FI)



---

INICIO
PSC-FI
FAQ
DESCARGAS

Políticas de seguridad en cómputo para la facultad de ingeniería

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.

Estas 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 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 estas se busca el 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.



[Mapa PSC-FI](#)

BÚSQUEDA

SECCIONES PSC-FI

- [Generalidades](#)
- [Políticas](#)
- [Buenas prácticas](#)
- [Códigos de ética](#)
- [Gestión de contraseñas](#)
- [Verificador de contraseñas](#)
- [Glosario](#)

Propuesta de Revisión, Actualización y Difusión de Las Políticas de Seguridad en Cómputo para la Facultad de Ingeniería.  
 Página elaborada por: Moisés Alvarado Hermida y Gibran Toríz Díaz Contreras  
 Asesora de tesis: M.C. Cintia Quezada Reyes

Figura 6.3 Vista previa de la página

## **6.2 Actualización periódica de las políticas de seguridad informática de la Facultad de Ingeniería**

En la realización de una actualización de las PSI de la FI, (PSC-FI) es necesario definir una estrategia para la actualización que establezca un tiempo de revisión por el hecho de buscar más la efectividad y funcionalidad que el cumplimiento de una planificación, por lo cual es necesario aclarar que una actualización es parte de un programa de mantenimiento de políticas el cual consta de varias etapas que se han descrito a lo largo de este trabajo.

Las etapas del mantenimiento y desarrollo de políticas de seguridad son:

1. Análisis y estudio
2. Desarrollo de las PSI
3. Difusión e implementación
4. Monitoreo y evaluación
5. Revisión y actualización

Este ciclo es necesario para la mejora continua de las PSI, y es indispensable que aun cuando se crea que es una etapa de ellas se considere como un todo y se lleve a cabo de manera eficiente, práctica, y detallada ya que dependiendo de la calidad con la que se lleve a cabo será directamente relacionada con los resultados que se obtendrán, es por esto que cada una de estas etapas no deben verse como elementos o parte sino como parte de un todo ya que en la medida en que cada una de estas etapas sea realizada, estará directamente asociada con los resultados.

A continuación se hace un breve resumen de este ciclo.

La primera etapa es el análisis y estudio de la organización en la cual se busca el saber qué se quiere proteger y de qué o quién se quiere proteger, ya terminada esta etapa se continúa con el desarrollo de políticas en la cual con la información recopilada se procede a la realización de normas, reglamentos, lineamientos, buenas prácticas, etcétera.

Terminadas estas dos etapas se procede a difundir las políticas creadas para que los usuarios y los administradores procedan a implementar dichas políticas dentro de sus centros de trabajo y laboratorios. Una vez implementadas las políticas viene la etapa de monitoreo y evaluación, en esta etapa las políticas implementadas son evaluadas por los usuarios, es decir, si son apropiadas, si causan conflicto en los procesos o actividades que desempeñan los usuarios, si requieren algún tipo de cambio o las políticas no funcionan y deben ser modificadas.

En esta etapa se realizan reportes que son enviados a los encargados de la seguridad y expertos que evalúan el desempeño de las políticas para rediseñar, modificar o realizar cambios que serán presentados ante un comité el cual estudiará dichos reportes para revisión o actualización de las PSI.

En la última etapa se tienen las observaciones, reportes y las evaluaciones que serán tomadas en cuenta por un comité que realizará la revisión, de manera que pueda corregir, cambiar o desarrollar nuevas políticas.

Es importante el mencionar que el comité encargado de la revisión y actualización evaluará toda la información obtenida y determinará a cuál de las cinco etapas debe recurrir de manera que se solucione y corrija el problema, es decir, desde esta última etapa se puede ir a cualquiera de las anteriores para continuar el ciclo de manera normal, pasando por las etapas faltantes esto con la meta de mejorar, cambiar o corregir las PSI.

Para ilustrar el ciclo del que se está hablando supóngase que al terminar se encuentra en la última etapa (Revisión o actualización) y la evaluación determinó que existió una falla en la difusión e implantación por lo que para eso es necesario volver a dicha etapa para la realización de acciones correctivas, por lo que después de realizar dichas acciones se procedería a la etapa de Monitoreo y evaluación (que es la etapa siguiente), una vez concluida ésta, se pasaría a la última etapa evaluando la nueva información recopilada proveniente de las acciones previamente tomadas pudiendo así nuevamente saltar a alguna de las etapas anteriores. En la Figura 6.4 se presenta un esquema de este ciclo.

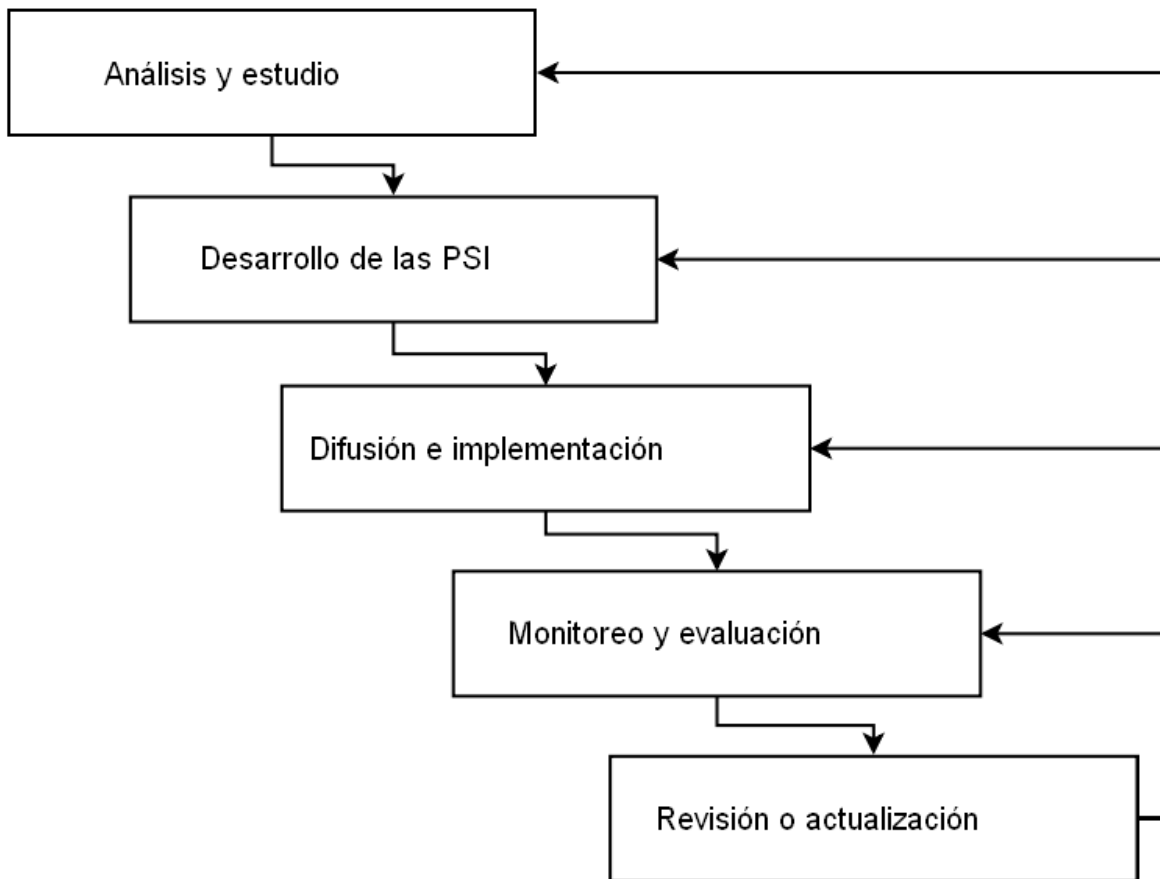


Figura 6.4 Ciclo de mantenimiento y desarrollo de las PSI

Un aspecto importante que se debe establecer para que este ciclo de mejora funcione, es la estrategia que se seguirá para la realización de la actualización o revisión de las PSI ya que dependiendo de la estrategia que fije la organización será cómo y qué tan rápido se dará este ciclo.

En el caso de la realización de una actualización periódica de las PSC-FI, se propone una estrategia mixta la cual constaría el uso de los 3 tipos de estrategias<sup>25</sup>, las cuales se resumen a continuación.

<sup>25</sup> Capítulo 5. Revisión de las políticas de seguridad informática de la FI.



1. Revisiones planificadas o periódicas las cuales son propuestas por el personal del CACFI cada cierto tiempo.
2. Revisiones o actualizaciones dinámicas promovidas por usuarios, administradores o personal mediante reportes evaluados por el DSC-FI y presentados al CACFI en caso de ser requerido un cambio o corrección.
3. Revisiones emergentes, las cuales pueden ocurrir en caso de un incidente muy grave que ponga en riesgo a la organización y que requiera de la respuesta inmediata.

Utilizar una estrategia mixta permite que la Facultad de Ingeniería (FI), pueda realizar cambios, correcciones y mejoras a los documentos (PSC-FI) de manera más flexible, lo que beneficiaría enormemente por el hecho de contar con un programa de mejoramiento continuo de las PSI, permitiendo así que las políticas avancen junto con el desarrollo tecnológico.

Si esta estrategia fuese aprobada se tendría la necesidad de capacitar a los administradores principalmente para poder implementarla con el fin de que ellos colaboraran con esta estrategia, la cual depende en gran medida de las observaciones, reportes y comentarios generados por la implementación y difusión de las PSC-FI.

La actualización y revisión de las políticas debe ser un esfuerzo conjunto y coordinado con un fin común, el cual consiste en monitorear, evaluar, proponer, capacitar al personal y dar seguimiento a este trabajo con el fin de mejorar continuamente el nivel de seguridad en la organización, el cual resultará en la reducción de todo tipo de incidentes dentro de las instalaciones, de la misma forma se busca que al capacitar adecuadamente a los usuarios acerca de las PSI, los incidentes en los equipos asociados (equipos de alumnos, académicos y demás personal), también disminuyan.

Si los usuarios siguen y respetan las PSI tanto dentro de la Facultad de Ingeniería (FI) como fuera de ella protegerán de una mejor y más eficiente forma los activos de los usuarios así como los recursos informáticos entre los cuales se encuentran todo tipo de cuentas como son, las bancarias, de correo electrónico, para acceso a servidores, así como las cuentas usadas para la compra y venta de artículos por internet entre otras.

Con el fin de tener las PSC-FI con una mayor disponibilidad, un sitio WEB presenta ventajas como son el ahorro en la impresión del documento, la disponibilidad en cuanto a horario

y descarga, facilitando así la consulta; la cual puede hacerse desde cualquier equipo conectado a internet.

Otra de las ventajas es la facilidad de cambios y actualización de la información, la cual puede ser modificada de manera repetitiva e ilimitada, además de tener un gran potencial para la difusión, la cual lo hace uno de los mejores medios para que los usuarios puedan acceder y consultar la información contenida en el sitio.

El acceso y la disponibilidad de la información hace que un sitio WEB sea una buena estrategia para la difusión de las políticas de seguridad, por lo anterior se propone el dar mantenimiento constante a la página que contendrá las PSC-FI con el fin de darle continuidad al trabajo que se realiza sobre las PSI en la Facultad de Ingeniería (FI).

# Conclusiones

## Conclusiones

La implementación de políticas de seguridad informática en una organización es una solución integral que no sólo busca proteger, preservar, administrar de una manera eficiente todo tipo de recursos con los que cuenta una organización, sino que también busca dar solución, prevenir, evitar, controlar y minimizar los daños de incidentes que afectan a la organización, por esto, preparar y capacitar al personal en temas asociados a la seguridad informática y cómo hacer frente a incidentes que se llegarán a presentar con el fin de responder de una manera adecuada es una de las principales metas de esta estrategia.

Contrariamente a lo que podría pensarse como un obstáculo para la realización de las diversas actividades por el hecho de ser necesario seguir y respetar lineamientos, recomendaciones, reglas, normas o protocolos, que pudieran entorpecer los procesos, actividades y trabajo que se realiza es una idea errónea por el hecho de que previamente a la implementación de las políticas se realiza un análisis o estudio ya que esta estrategia tiene como uno de sus principios no interferir o interferir lo menos posible en los procesos y actividades que se realizan en la organización.

Por otra parte es necesario capacitar al personal para que éste pueda tomar un papel activo dentro de la organización de manera que aplique este conocimiento en las diversas actividades que realiza dentro y fuera de la organización con el propósito de proteger de una forma adecuada la información que se le confía, así como la propia.

Contar con una buena implementación de políticas de seguridad informática debe ser un punto clave en toda organización, de lo contrario se habrá caído nuevamente en un error que puede perjudicar y causar pérdidas graves que pudieran haberse prevenido, sin embargo, es necesario destacar que para que dicha implementación sea efectiva debe tener el apoyo y participación de todas las áreas, departamentos o ramas que integran la organización.

Las políticas de seguridad informática son la base para todo programa de seguridad por lo que es necesario contar con una documentación adecuada la cual debe contener un programa de difusión, monitoreo, revisión y actualización como parte de un ciclo para el mantenimiento de esta estrategia, esto es, que exista un ciclo de mejora continua ya que en la medida en que cada una de las fases de mantenimiento y desarrollo de las políticas de seguridad informática sean desarrolladas se tendrá un mejor resultado. (Figura C.1).

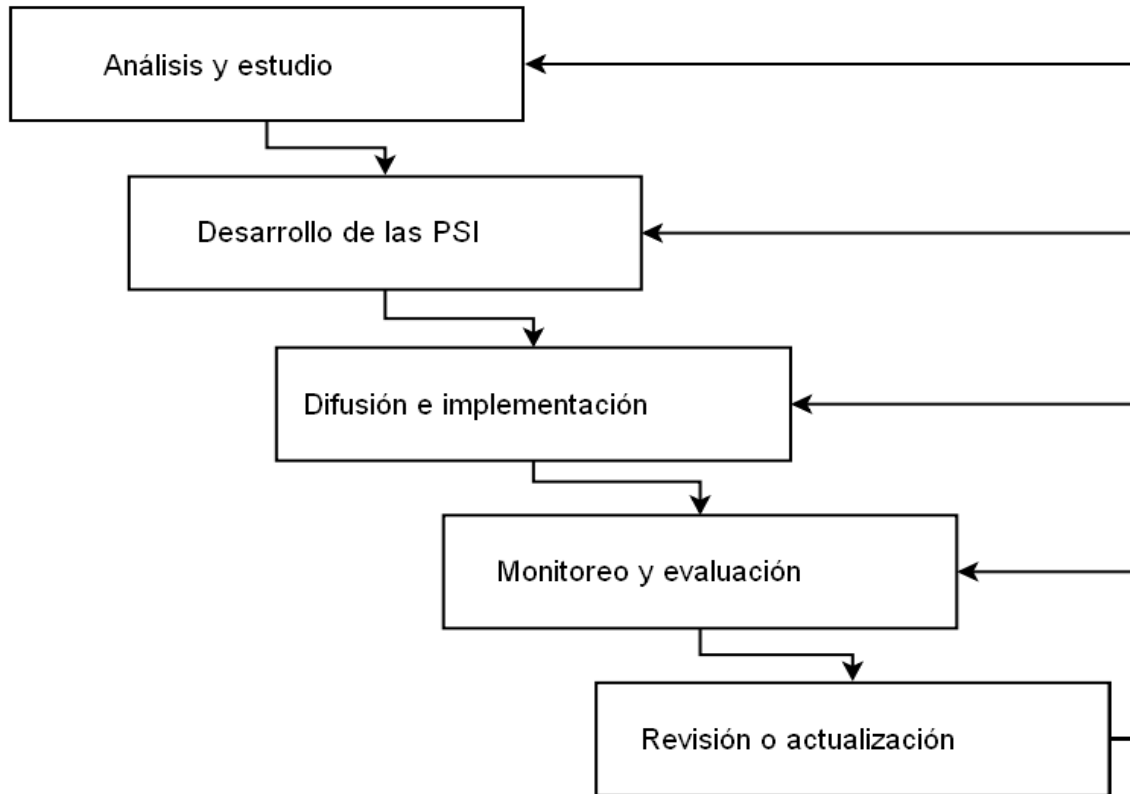


Figura C.1 Ciclo de mantenimiento y desarrollo de las Políticas de Seguridad Informática (PSI).

La investigación realizada fue aplicada para el caso particular de la Facultad de Ingeniería (FI), es decir, se realizó una revisión y actualización de las políticas de seguridad en cómputo, la cual consistió en la aplicación de lineamientos y recomendaciones para el desarrollo de políticas con el fin de que el documento que se tiene sea más completo, actualizado y claro, esto aunado a una propuesta de difusión que consiste en la creación de una página web que está diseñada con la finalidad de que el usuario pueda consultar las políticas de seguridad de una manera más sencilla y rápida.

Con la idea de tener una mejor difusión de esta información, este documento contiene también diferentes recomendaciones para ayudar a la propagación y divulgación del conocimiento sobre el área de la seguridad informática en la comunidad que conforma la Facultad de Ingeniería (FI).

Además de la realización de esta propuesta, la investigación presenta una serie de recomendaciones y lineamientos que pueden ser apoyo para el desarrollo y revisión de políticas o

reglamentos complementarios por parte de las diferentes áreas, departamentos o divisiones que la conforman.

Se proponen también diversas estrategias para la realización de revisiones y actualizaciones posteriores a las Políticas de Seguridad en Cómputo de la Facultad de Ingeniería (PSC-FI), con el objetivo de que los responsables de la seguridad informática o en cómputo implementen una metodología de mejora continua de manera que los procesos en la implementación, así como los diferentes servicios y actividades que se realizan en la organización para el mantenimiento de un nivel adecuado de seguridad informática mejoren y puedan incorporar cambios de manera más dinámica y en menor tiempo.



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 hacía 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”<sup>26</sup>**

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

---

<sup>26</sup> 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 serían?

**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 auditoría 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 “sniffee” ya que es un término ilícito y usar el término de análisis de vulnerabilidades ya que las palabras escaneo y “sniffee” 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 realizó un trabajo de tesis acerca de este tema el cual contiene un análisis sobre este tema.<sup>27</sup>**

**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.**

---

<sup>27</sup> 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 puede consultar?

**No se publican pero debe existir 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 serían 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

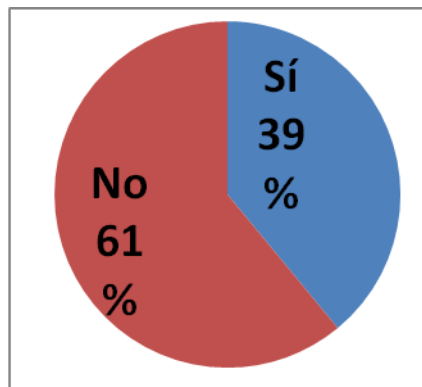
## Apéndice 3

**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<sup>28</sup> 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-

<sup>28</sup> 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% contestó que la seguridad informática tenía que ver con la implementación de seguridad en las Tecnologías de la Información (TI), 5% contestó 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.

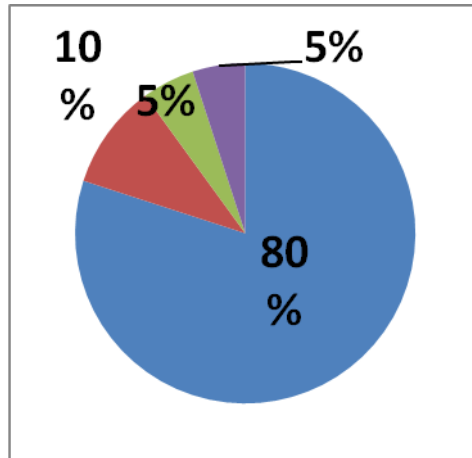
A continuación se presenta una breve síntesis de los porcentajes mencionados. (Ver gráfica 1.2).

80% - Protección de información personal de virus y atacantes.

10% - Implementación de seguridad en las Tecnologías de la Información (TI).

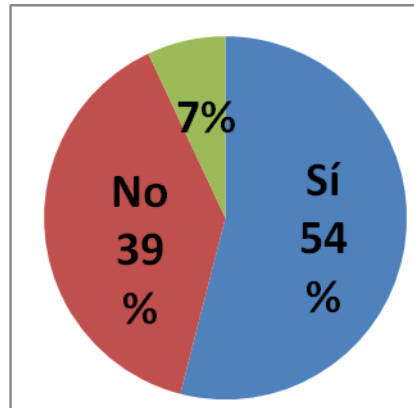
5% - No sabe o no tiene conocimiento.

5% - Está relacionada con la protección de todo tipo de activos de una organización



Gráfica 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 resultó 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)

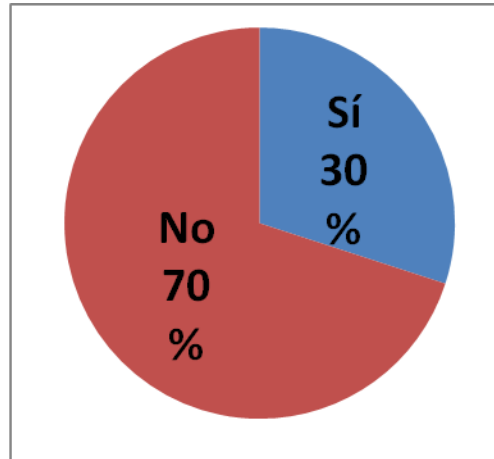


Gráfica 1.3 La existencia de un buen nivel de seguridad dentro de la Facultad de Ingeniería (FI).

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).



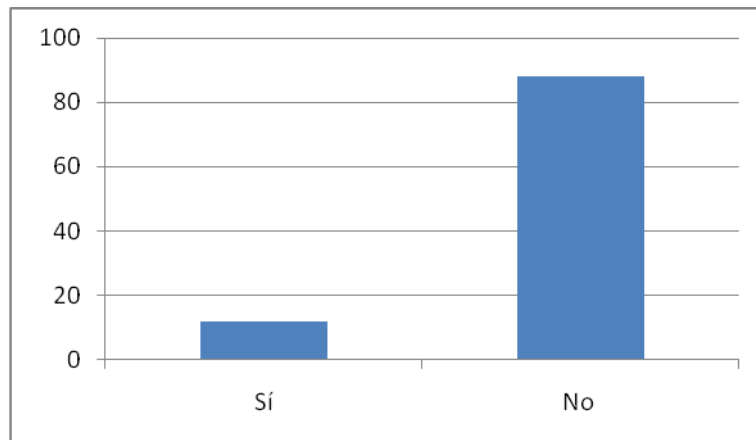
Gráfica 1.4 Acceso a redes internas de la Facultad de Ingeniería.

La población fue cuestionada acerca de su conocimiento sobre la existencia de reglamentos internos para los distintos laboratorios y solo el 30% contestó 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, pérdida 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 afirmó tener algún conocimiento sobre estas. (Gráfica 1.5).

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

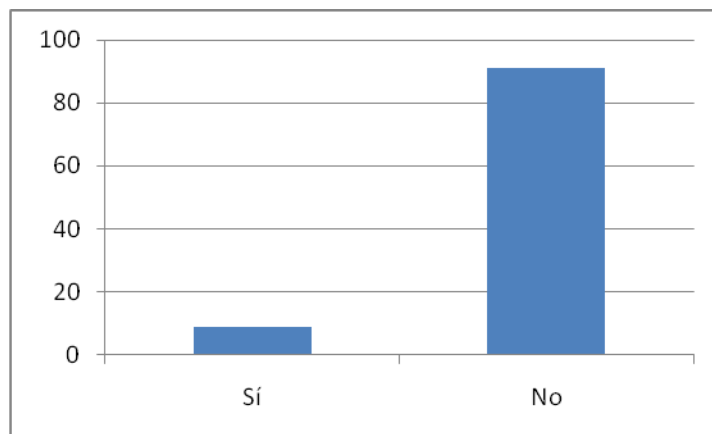


Gráfica 1.5 Conocimiento sobre la existencia de las PSI dentro de la Facultad de Ingeniería

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 la 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

Responsables de la elaboración, aprobación y autorización.  
Historial del documento.  
Introducción.  
Seguridad en cómputo.  
Factores críticos.  
Filosofía de políticas de seguridad.  
Comité asesor de cómputo de la Facultad de Ingeniería.  
Integrantes del CACFI.  
Departamento de Seguridad en Cómputo de la Facultad de Ingeniería.

### Sección de Políticas

Responsabilidades del usuario.  
Políticas de seguridad física.  
Políticas de reglamentos internos.  
Políticas de contraseñas.  
Políticas de control de acceso.  
Políticas de uso adecuado.  
Políticas de respaldos.  
Políticas de correo electrónico.  
Políticas de desarrollo de software.  
Políticas de contabilidad del sistema.  
Políticas de uso de direcciones IP.  
Políticas de sitios web.  
Políticas para redes inalámbricas.  
Políticas de tecnologías emergentes.  
Políticas de contratación y finalización de relaciones laborales de recursos humanos en sistemas informáticos.  
Políticas de colaboración conjunta.  
Actualización de las políticas.  
Políticas referentes a la auditoría.  
Políticas sobre incidentes graves.  
Políticas del plan de contingencias.  
Sanciones

### Incidentes de Seguridad

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

<p><b>Elaboró</b></p>  <p>_____</p> <p><b>Firma</b>  <b>Responsable de la elaboración y edición del documento</b></p>	<p><b>Aprobó</b></p>  <p>_____</p> <p><b>Firma</b>  <b>Responsable del departamento de seguridad en cómputo</b></p>	<p><b>Autorizó</b></p>  <p>_____</p> <p><b>Firma</b>  <b>Responsable 4del CACFI</b></p>
---	---	---

### 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
<b>Facultad de ingeniería, UNAM</b>	<b>Toda la comunidad de la Facultad de Ingeniería</b>

## 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.
- Respalidar 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<sup>29</sup>**

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.

---

<sup>29</sup> [http://www.ingenieria.unam.mx/cacfi/documentos/art\\_comite.pdf](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 Dis-  
tancia

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 Indus-  
trial

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 Humanidades

## **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<sup>30</sup>

---

<sup>30</sup> <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 debe 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)<sup>31</sup>.
  
- 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.

---

<sup>31</sup> <http://www.ingenieria.unam.mx/cacfi/documentos/normatividadweb.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 sitios web o páginas de internet que operen en cualquier equipo de la Facultad de Ingeniería.

### **Políticas:**

- Las sitios WEB además deben seguir con las normas, lineamientos y recomendaciones establecidas por la Facultad de Ingeniería (véase Normatividad WEB)<sup>32</sup>.
- 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.

---

<sup>32</sup> <http://www.ingenieria.unam.mx/cacfi/documentos/normatividadweb.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 predefinido 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, et- cétera).

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.

<b>Actividad ilícita</b>	<b>Sanción</b>
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.”<sup>33</sup>

“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.”<sup>34</sup>

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.

---

<sup>33</sup> <http://sistemas.dgsca.unam.mx>, 2003

<sup>34</sup> 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)

<b>Análisis de Riesgo</b>	<b>Impacto Económico</b>
<ol style="list-style-type: none"> <li>1. Identificación de amenazas.</li> <li>2. Análisis de la probabilidad de materialización de la amenaza</li> <li>3. Selección de amenazas.</li> <li>4. Identificación de entornos amenazados.</li> <li>5. Identificación de servicios afectados.</li> <li>6. Estimación del impacto económico por paralización de cada servicio.</li> <li>7. Selección de los servicios a cubrir.</li> <li>8. Selección final del ámbito del plan.</li> <li>9. Identificación de alternativas para los entornos.</li> <li>10. Selección de alternativas.</li> <li>11. Diseño de estrategias de respaldo.</li> <li>12. Selección de la estrategia de respaldo.</li> </ol>	<ol style="list-style-type: none"> <li>1. Identificación de servicios finales.</li> <li>2. Análisis del impacto. En estas metodologías se evalúan los daños económicos y de imagen y otros aspectos ajenos a los económicos.</li> <li>3. Selección de servicios críticos.</li> <li>4. Determinación de recursos de soporte.</li> <li>5. Identificación de alternativas para entornos.</li> <li>6. Selección de alternativas.</li> <li>7. Diseño de estrategias globales de respaldo.</li> <li>8. Selección de la estrategia global de respaldo.</li> </ol>

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 irre recuperables.

- 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 ~~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:

<b>Contraseña</b>	<b>Acerca de la contraseña</b>
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 intrascendente 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.”<sup>35</sup>

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.”<sup>36</sup>

“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.”<sup>37</sup>

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

---

<sup>35</sup> Garza de Flores, *Ética*, 1993 Ed. Alhambra Mexicana.

<sup>36</sup> Lozano V, Rodríguez, *Ética*, Ed. Alhambra Mexicana, 1986

<sup>37</sup> 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<sup>38</sup>, 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 un 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.

---

<sup>38</sup> 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 un 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 esfuerzos.

*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 cuidado 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 falta 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 puede 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.<sup>39</sup>

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:

---

<sup>39</sup> David Jarmon, A preparation guide to information security policies

[http://www.sans.org/reading\\_room/whitepapers/policyissues/preparation-guide-information-security-policies\\_503](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.”<sup>40</sup> 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.

---

<sup>40</sup> 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 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 cuentan, 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**

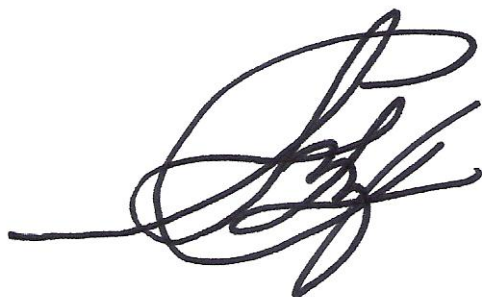
Hospital Regional "Lic. Adolfo López Mateos"  
Av. Universidad # 1321  
Col. Florida, Delegación Álvaro Obregón  
C.P. 01030, México, D.F.  
[www.hospitallopezmateos.org](http://www.hospitallopezmateos.org)

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

A handwritten signature in black ink, appearing to be 'CSL', written in a cursive style.



Universidad Nacional Autónoma de México

Facultad de Ingeniería

**Apéndice 7**

**Reporte de incidente de seguridad informática**

## Reporte de incidente de seguridad informática<sup>41</sup>

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:

---

<sup>41</sup> 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

<input type="checkbox"/>	Uso indebido de información.	<input type="checkbox"/>	Cambio en la configuración del equipo.
<input type="checkbox"/>	Uso inadecuado de recursos informáticos.	<input type="checkbox"/>	Ataque o infección de malware, o código malicioso (virus, gusanos, troyanos, etc.)
<input type="checkbox"/>	Divulgación no autorizada de información personal.	<input type="checkbox"/>	Acceso o intento de acceso a un sistema informático.
<input type="checkbox"/>	Acceso o intrusión física.	<input type="checkbox"/>	Pérdida o destrucción no autorizada de información.
<input type="checkbox"/>	Ingeniería social.	<input type="checkbox"/>	Interrupción en los servicios de red.
<input type="checkbox"/>	Uso indebido de correo electrónico institucional.	<input type="checkbox"/>	Anomalía o vulnerabilidad técnica del software.
<input type="checkbox"/>	Modificación de información de un sitio o página.	<input type="checkbox"/>	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	<input type="checkbox"/>	No	<input type="checkbox"/>
¿El recurso afectado tiene conexión con la organización?	Sí	<input type="checkbox"/>	No	<input type="checkbox"/>
¿El recurso afectado tiene conexión a internet?	Sí	<input type="checkbox"/>	No	<input type="checkbox"/>
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<sup>3</sup> (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.

**Trojanos**

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.

# Bibliografía

## Bibliografía

**Barman Scott**, Writing information Security Policies, New Riders.

**Garfinkel Simson, Spafford Gene, Schwartz Alan**, Practical Unix & Internet Security, O'Reilly, Third edition.

**Patrick D. Howard**, The Security Policy Life Cycle: Functions and Responsibilities, CRC Press 2007.

**Gordon “Fyodor” Lyon**, Nmap Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning, December 2008

**Guerrero Martínez, Edson Armando**. Gestión de redes inalámbricas en la Facultad de ingeniería, Tesis Licenciatura (Ingeniero en Computación)-UNAM, Facultad de Ingeniería México 2009.

**Tipton Harold F.** Information Security management Handbook, Sixth Edition, CISSP, CRC Press.

**Peltier Thomas R.** Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management, Auerbach Publications.

**Bacik Sandy**, Building an Effective Information Security Policy Architecture, CRC Press.

**Steafanek George L.** information Security Best Practices: 205 Basic Rules, Butterworth Heine-  
mann.

**Yhan Gregory**, ISO 17799: Scope and implementation – Part 1 Security Policy, MCAD.net, CISSP.

**Roberto Carlos Zúñiga Ramírez y Yesenia Carrera Fournier**, 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, Tesis Licenciatura, UNAM, Facultad de Ingeniería, México 2003

## **Mesografía**

### **UNAM CERT**

<http://www.cert.org.mx/>

### **SANS Institute**

<http://www.sans.org>

### **SANS Institute InfoSec Reading Room**

[http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/)

### **Security In An Open Environment Such As A University?**

[http://www.sans.org/reading\\_room/whitepapers/policyissues/security-open-environment-university\\_1570](http://www.sans.org/reading_room/whitepapers/policyissues/security-open-environment-university_1570), 2009

### **Understanding the Importance of and Implementing Internal Security Measures**

[http://www.sans.org/reading\\_room/whitepapers/policyissues/understanding-importance-implementing-internal-security-measures\\_1901](http://www.sans.org/reading_room/whitepapers/policyissues/understanding-importance-implementing-internal-security-measures_1901), 2009

### **Creating an Information Systems Security Policy**

[http://www.sans.org/reading\\_room/whitepapers/policyissues/creating-information-systems-security-policy\\_534](http://www.sans.org/reading_room/whitepapers/policyissues/creating-information-systems-security-policy_534), 2009

### **An Overview of Corporate Computer User Policy**

[http://www.sans.org/reading\\_room/whitepapers/policyissues/overview-corporate-computer-user-policy\\_535](http://www.sans.org/reading_room/whitepapers/policyissues/overview-corporate-computer-user-policy_535), 2009

### **The social approaches to enforcing information security**

[http://www.sans.org/reading\\_room/whitepapers/policyissues/social-approaches-enforcing-information-security\\_1102](http://www.sans.org/reading_room/whitepapers/policyissues/social-approaches-enforcing-information-security_1102), 2009

### **Security Process for the implementation of a Company's extranet network**

[http://www.sans.org/reading\\_room/whitepapers/policyissues/security-process-implementation-companys-extranet-network\\_1115](http://www.sans.org/reading_room/whitepapers/policyissues/security-process-implementation-companys-extranet-network_1115), 2009

### **Acceptable Use Policy Document**

[http://www.sans.org/reading\\_room/whitepapers/policyissues/acceptable-policy-document\\_369](http://www.sans.org/reading_room/whitepapers/policyissues/acceptable-policy-document_369), 2009



**Guidelines for an Information Sharing Policy**

[http://www.sans.org/reading\\_room/whitepapers/policyissues/guidelines-information-sharing-policy\\_918](http://www.sans.org/reading_room/whitepapers/policyissues/guidelines-information-sharing-policy_918), 2009

**Developing a Security Policy - Overcoming Those Hurdles**

[http://www.sans.org/reading\\_room/whitepapers/policyissues/developing-security-policy-overcoming-hurdles\\_915](http://www.sans.org/reading_room/whitepapers/policyissues/developing-security-policy-overcoming-hurdles_915), 2009

**Security Policies: Where to Begin**

[http://www.sans.org/reading\\_room/whitepapers/policyissues/security-policies\\_919](http://www.sans.org/reading_room/whitepapers/policyissues/security-policies_919), 2009

**Development of an Effective Communications Use Policy**

[http://www.sans.org/reading\\_room/whitepapers/policyissues/development-effective-communications-policy\\_485](http://www.sans.org/reading_room/whitepapers/policyissues/development-effective-communications-policy_485), 2009

**Seguridad UNAM**

<http://www.seguridad.unam.mx/noticias/>

**Symantec**

<http://www.symantec.com/>

<http://www.symantec.com/podcasts/>

**ISO 27000**

<http://www.iso27000.es/>

<http://www.iso27001security.com/>

**O-ISM3 Services**

<http://www.ism3.com/>

**ISM3.es.1.0.pdf**

[http://hades.udg.edu/~xavier/downloads/White\\_Papers/ISM3.es.1.0.pdf](http://hades.udg.edu/~xavier/downloads/White_Papers/ISM3.es.1.0.pdf), 2010

**Information Security**

<http://www.infosecuritymag.com>

**National Security Agency NSA**

<http://www.nsa.gov/ia/index.shtml>

**Laboratorio de Redes y Seguridad**

<http://132.248.52.4/>

**Computerworld**

[http://www.computerworld.com/s/article/85583/10\\_steps\\_to\\_a\\_successful\\_security\\_policy](http://www.computerworld.com/s/article/85583/10_steps_to_a_successful_security_policy)

**CACFI Facultad de Ingeniería**

<http://www.ingenieria.unam.mx/cacfi/>

**Segu-info, Seguridad informática**

<http://www.segu-info.com.ar/politicas/>

**Universidad del Quindío**

[http://www.uniquindio.edu.co/uniquindio/meci/informacion/guia\\_para\\_elaborar\\_politicas\\_v1\\_0.pdf](http://www.uniquindio.edu.co/uniquindio/meci/informacion/guia_para_elaborar_politicas_v1_0.pdf), 2009

**Harvard Information Security & Privacy**

<http://www.security.harvard.edu/>, 2010

**Brown University Checklist for Protecting Information**

<http://www.brown.edu/cis/policy/protectinginfo.php>, 2010

**Information Security Policy - The University of Newcastle, Australia**

<http://www.newcastle.edu.au/policy/000813.html>

**Universidad Nacional de Luján**

<http://www.unlu.edu.ar/>

<http://www.unlu.edu.ar/v1-5-v2-0-v3-noved-seguridad.html>