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 el 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 reditúa, 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

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

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 la 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 qué 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 esta 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 cuenten, 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.