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.

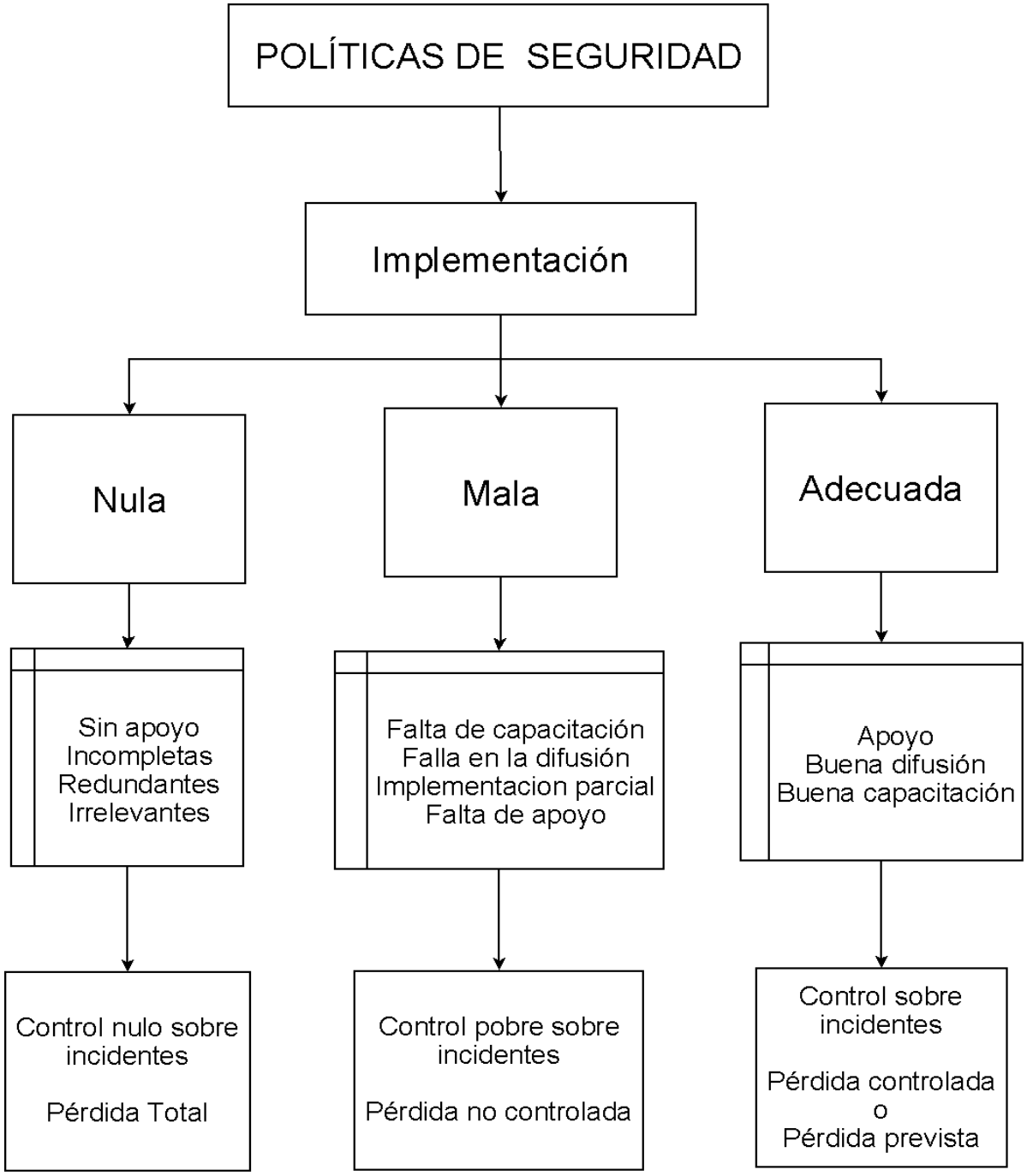

Figura 3.1 Fallas en la implementación de las políticas de seguridad

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[4], un experto en la rama de políticas de seguridad, él aclara que el tiempo para la

[4] 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.[5]

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.

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

- ¿Quién es el que implementa la política?
- ¿Quién es el encargado del mantenimiento, monitoreo, 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."[6] 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

[6] 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 al pendiente de él.

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

11. El factor error humano

Las políticas de seguridad no son reglas que buscan castigar al usuario en caso de cometer algún error, el hecho de que el usuario cometerá errores está contemplado, es decir, las políticas buscan que el usuario no cometa errores por medio de la capacitación y la experiencia, sin embargo, 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 cuenten, el acceso a las distintas áreas dentro de la organización, el prestigio de la organización, así como proteger a los usuarios y su información personal.

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

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

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

- Caso 1

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

- Caso 2

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

- Caso 3

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

No sólo es importante 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."[7]

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.

[7] 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.