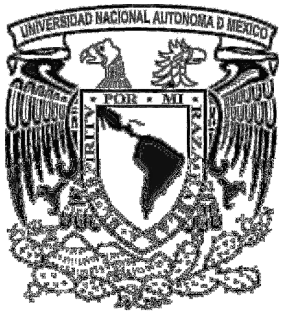

Universidad Nacional Autónoma de México

Facultad de Ingeniería

Guía para la elaboración de políticas de seguridad informática

Importancia de las políticas de seguridad en una organización

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

El éxito de todo programa de seguridad se basa en que el documento donde se encuentran dichas políticas tiene como base 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.

El hecho de que las políticas existentes en una organización sean 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 valiosos 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.

El que se subcontrate a 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.

El que las organizaciones busquen capacitar y mantener 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.

Correcta redacción de las políticas de seguridad

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

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

1. Escoger una filosofía prohibitiva o permisiva

Existen dos filosofías que se pueden utilizar al redactar las políticas de seguridad, 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.

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

El 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.

El 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

El 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.

- ¿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."[1] 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 demasiado complejo y complicado, que requiere invertir demasiado tiempo

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

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, sin embargo, debe ser a la vez no demasiado formal usando lenguaje que sólo los expertos en la materia puedan entender ya que tendría el mismo efecto y lo ignorarían.

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

7. Formato unificado

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

El 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.

El 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

El 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 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.

El 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

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

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

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

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

Puntos importantes a considerar en las políticas de seguridad

Existen puntos a considerar al hablar de políticas de seguridad, los cuales darán mayor cohesión y mejorarán los resultados, teniendo en mente estos puntos ayudarán a entender de una mejor manera el funcionamiento y será de gran apoyo para las revisiones, cambios, sugerencias así como a la implementación de las mismas.

a) Ventajas asociadas a un buen documento

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

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

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

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

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

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

En ocasiones, 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, sin embargo, cuando se necesite el uso de alguna tecnología nueva que después de analizarla cuidadosamente sea indispensable que se implemente, es importante considerar cómo se llevará a cabo y si es viable que se haga tal implementación.

c) Factores involucrados en la implementación

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

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

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

Por lo anterior es necesario 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.

El 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.