Arquitectura de seguridad informática y políticas para el aseguramiento de la información

Autor: Claudia Rita Medina Ortiz

Tesina presentada para obtener el título de:
Lic. En Sistemas Computarizados [sic]

Nombre del asesor:
Sergio Francisco Barraza Ibarra

UNIVERSIDAD VASCO DE QUIROGA
ESCUELA DE SISTEMAS COMPUTARIZADOS

N° DE ACUERDO 952006 CLAVE 16PSU0014Q

"ARQUITECTURA DE SEGURIDAD INFORMATICA Y POLITICAS PARA EL ASEGURAMIENTO DE LA INFORMACIÓN "

T E S I N A

PARA OBTENER EL TÍTULO DE:

Licenciado en Sistemas Computarizados

PRESENTA:

Claudia Rita Medina Ortiz

ASESOR:
ING. Y M.A. SERGIO FCO. BARRAZA I.

MORELIA, MICHOACÁN, NOVIEMBRE DE 2004

Agradecimientos

A mis padres y hermanos por todo su apoyo y confianza que siempre han depositado en mi.

Y Agradecimientos Especiales:

A mi asesor el Ing. Sergio Barraza y el Act. Javier Altuzar Arenas por toda su ayuda y motivación para que pudiera logra mi titilación.

INDICE

I. INTRODUCCION

La continua evolución de las tecnologías de la información y de las comunicaciones hace que los sistemas tecnológicos adquieran un papel cada vez mas critico en el funcionamiento de las empresas y en la obtención de resultados de negocios.

Pero esta mayor interconexión de las redes y esta grande dependencia de los sistemas informáticos hacen que las empresas, si no toman las medidas adecuadas, se vuelvan mucho más vulnerables a los ataques a través de estos sistemas.

Intrusiones externas o internas, virus, sabotajes y robos de información son problemas que van en constante aumento. Sin embargo, existen todavía muchas ideas erróneas en el ámbito de la seguridad de los sistemas de información y esto constituye un serio riesgo para la empresa, muchas veces infravalorado.

Las soluciones para evitar este tipo de problemas requieren no solo la utilización de sofisticadas herramientas técnicas, tanto de hardware como de software, si no la definición, gestión y continuo control de arquitecturas, políticas, procedimientos y normativas orientadas a evitar cualquier tipo de vulnerabilidad, y de detectar los problemas y minimizar los daños si estos ya se han producido.

Conseguir sistemas seguros requiere, en consecuencia, no solo soluciones tecnológicas, si no también organizativas.

Un enfoque adecuado para la seguridad informática de una empresa debe ser global, involucrar a todo el personal de la organización y proteger todos los elementos del sistema, no solo los perimetrales.

No debe confundirse la Seguridad Informática con otras áreas de la Seguridad en la empresa como son las relativas a la seguridad de las personas o de las cosas. La Seguridad Informática también se ocupa de aspectos físicos pero sólo en lo relativo a zonas en las que haya Recursos Informáticos y de los accesos a estas zonas, y de aspectos relativos a las personas pero sólo en lo relacionado con la protección de los Activos de Información y sus accesos a ellos.

En todo sitio en el que se usen computadoras, el establecimiento de políticas de seguridad es imperativo y de gran valor. Una política de seguridad informática permite un uso más seguro, organizado, eficiente y productivo de los recursos informáticos; previene y reduce el impacto de pérdidas humanas y materiales derivadas de diversos incidentes; define reglas y principios de acción a tomar en caso de cualquier incidente de violación de seguridad.

Las políticas de seguridad informática representan un tipo especial de reglas de negocios documentadas. Su auge ha sido estimulado por la explosión de tecnologías de manejo de información, incluyendo a los teléfonos celulares, los buscapersonas y los computadores. Los que trabajan en el ambiente empresarial deben recibir instrucciones claras y definitivas que los ayuden a garantizar la seguridad de la información generada en el complejo mundo de los negocios. Definitivamente, es imprescindible mantener reglas claras que enmarquen el desarrollo de las actividades en cualquier actividad comercial, los sistemas de información no escapan a este tipo de documentación.

En general, la seguridad informática depende de la articulación eficiente de varios factores, uno de los cuales es ese conjunto de políticas de seguridad informática, las cuales representan el marco normativo para el establecimiento de cualquier solución de seguridad para las organizaciones.

2. ANTECEDENTES

Las sociedades avanzadas de fin de este siglo son denominadas frecuentemente sociedades de la información, pues el volumen de datos que es procesado, almacenado y transmitido es inconmensurablemente mayor.

Además, no sólo el volumen, sino la importancia de esta información para el desarrollo económico y social, no tienen ninguna comparación con la que tuvo en el pasado. De hecho, en la actualidad, las organizaciones consideran que la información es un bien más de su activo y, en muchos casos, prioritario sobre los restantes.

Pero gran parte de esos datos que nosotros, o las entidades de nuestra sociedad, manejamos, han sido tratados, sea durante su proceso, o almacenamiento, o transmisión, mediante las llamadas tecnologías de la información, entre las que ocupa un lugar focal la informática. Consiguientemente, la seguridad de las tecnologías de información, y por ende las informática, se convierte en un tema de crucial importancia para el continuo y espectacular progreso de nuestra sociedad, e incluso para su propia supervivencia.

Por otro lado, la explosión en los últimos años de las redes informáticas y fundamentalmente de Internet, ha sido el factor fundamental que ha hecho que la Seguridad Informática cobrase una importancia vital en el uso de sistemas informáticos conectados. Desde el momento en que nuestra computadora se conecta a Internet, se abren ante nosotros toda una nueva serie de posibilidades, sin embargo éstas traen consigo toda una serie de nuevos y en ocasiones complejos tipos de ataques. Más aún, mientras en una computadora aislada el posible origen de los ataques es bastante restringido, al conectarnos a Internet, cualquier usuario de cualquier parte del mundo puede considerar nuestro sistema un objetivo apetecible.

Existe un acuerdo y conciencia general sobre la importancia de la Seguridad de los Sistemas de Información. Los Sistemas de Información están relacionados con la disponibilidad, confidencialidad e integridad de la información tratada por las computadoras y las redes de comunicación. Se usan comúnmente otros términos que en esencia tienen el mismo significado, tales como seguridad de la información, seguridad de las computadoras, seguridad de datos o protección de la información, pero se orientan a la Seguridad de los Sistemas de Información.

3. OBJETIVO GENERAL

Analizar la importancia de la arquitectura y seguridad informática, como apoyo a las empresas, para optimizar el manejo y procesamiento de la información; así como identificar, y eliminar o controlar las fuentes de riesgos en los sistemas de información.

4 OBJETIVOS ESPECIFICOS

- Analizar los principales objetivos de las políticas para el aseguramiento de la información.

- Determinar cómo se plantean, organizan y controlan las políticas de información.

- Conocer la relevancia que tienen los sistemas de información dentro de las empresas.

- Impulsar y fomentar una cultura de Seguridad Informática.

- Preparar recursos humanos capacitados en la práctica de las distintas herramientas de seguridad Informática.

- Crear conciencia de la importancia y los alcances que las políticas de información tienen actualmente las empresas.

5. SEGURIDAD INFORMATICA

Cuando se habla de la función informática generalmente tendemos a hablar de tecnología nueva, de nuevas aplicaciones, nuevos dispositivos hardware, nuevas formas de elaborar información más consistente, etc.

Sin embargo se suele pasar por alto o se tiene muy implícita la base que hace posible la existencia de los anteriores elementos. Esta base es la información.

Es muy importante conocer su significado dentro la función informática, de forma esencial cuando su manejo esta basado en tecnología moderna, para esto se debe conocer que la información:

- Esta almacenada y procesada en computadoras
- Puede ser confidencial para algunas personas o a escala institucional
- Puede ser mal utilizada o divulgada
- Puede estar sujeta a robos, sabotaje o fraudes

Los primeros puntos nos muestran que la información esta centralizada y que puede tener un alto valor y los últimos puntos nos muestran que se puede provocar la destrucción total o parcial de la información, que incurre directamente en su disponibilidad que puede causar retrasos de alto costo.

Pensemos por un momento que hoy se sufre un accidente en el centro de cómputo o el lugar donde se almacena la información. Ahora preguntémonos: ¿Cuánto tiempo pasaría para que la organización este nuevamente en operación?

Es necesario tener presente que el lugar donde se centraliza la información con frecuencia el centro de cómputo puede ser el activo más valioso y al mismo tiempo el más vulnerable.

Para continuar es muy importante conocer el significado de dos palabras, que son riesgo y seguridad.

Riesgo

Proximidad o posibilidad de un daño, peligro, etc.

Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.

Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.

Seguridad

Cualidad o estado de seguro

Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo.

Una política de seguridad informática es aquella que fija los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen.

Podemos definir política de seguridad de la información como el conjunto de normas, reglas, procesos, prácticas que regulan la protección de la información contra la pérdida de la confidencialidad, integridad o disponibilidad.

La política de seguridad nos indica:

- Qué hay que proteger
- Qué principios hemos de tener en cuenta
- Cuáles son los objetivos de Seguridad a conseguir
- La asignación de cometidos y responsabilidades

La política de Seguridad se expresa mediante principios y objetivos. Un principio es una norma o idea fundamental y que se acepta en esencia. Un objetivo es la declaración expresa de la información a conseguir para contribuir a la seguridad de la información.

Una buena política de seguridad corporativa debe recoger, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos. Esta visión general resulta vital para asegurar un nivel homogéneo en el grado de seguridad que quiera alcanzarse, y evitar la aparición de "agujeros" en determinados puntos del sistema. En definitiva, de nada sirve un excelente cortafuegos si no se encuentra instalado un buen antivirus, o tener un avanzado software de detección de intrusos si se carece de una adecuada política de contraseñas para los usuarios.

Las áreas que contemple la política de seguridad variarán en función de cada empresa y sistema. Como mínimo deberán abordar apartados tales como: evaluación de riesgos, protección perimétrica, control de acceso a los recursos, directrices de uso de Internet y correo electrónico, antivirus, y copias de seguridad.

Otra característica importante que no debe olvidarse en las políticas de seguridad es su mantenimiento y revisión periódica. En la práctica, el crecimiento y la modificación de los sistemas de la empresa, así como la continua aparición de nuevas vulnerabilidades y amenazas, exigen que la política de seguridad corporativa sea un elemento vivo que se vaya adaptando a las necesidades que vayan surgiendo.

Se dice que la seguridad informática de una organización, será tan fuerte como el punto más débil que esta posea. Si bien una organización puede iniciar una estrategia de seguridad informática, podría pasar que no se tenga lo bastante claro de los diferentes elementos que deba considerar para cubrir todos los puntos necesarios de vulnerabilidad en su propia infraestructura.

El planear de manera superficial la incorporación de seguridad en una organización que basa su productividad en la información electrónica, no es suficiente si antes no hace un análisis más a profundidad de aquellos puntos débiles (y no tan débiles) que en materia de seguridad informática pudiesen existir.

Para iniciar con una planeación adecuada de la seguridad informática, se debe entender (conceptualmente hablando) el significado de la seguridad informática. Puesto que este tema abarca múltiples y muy diversas áreas relacionadas con los sistemas, existen elementos que van desde la protección física de un equipo de cómputo como componentes hardware, de su entorno, hasta la protección de la información que contiene o de las redes que lo comunican con exterior. Tampoco es único el objetivo de la seguridad ya que son muy diversos los tipos de amenazas contra los que una organización debería protegerse, desde amenazas físicas, como los cortes eléctricos, hasta errores no intencionados de los usuarios, pasando por los virus informáticos o el robo, destrucción o modificación de la información, por eso mismo no existe una definición exacta que se pueda localizar en libros del tema, sin embargo el "concepto" podría ser fácilmente entendible. Se dice que un sistema se encuentra en optimas condiciones para operar cuando se cumplen los siguientes tres puntos fundamentales: Confidencialidad - Integridad - Disponibilidad.

5.1 Confidencialidad.

Es un servicio de seguridad que tiene como meta asegurar que la información esté solamente disponible para personas y procesos autorizados. La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él. En áreas de seguridad gubernamentales el secreto asegura que los usuarios pueden acceder a la información que les está permitida en base a su grado o nivel de autoridad, normalmente impuestas por

disposiciones legales o administrativas. En entornos de negocios, la confidencialidad asegura la protección en base a disposiciones legales o criterios estratégicos de información privada, tal como datos de las nóminas de los empleados, documentos internos sobre estrategias, nuevos productos o campañas, etc. Este aspecto de la seguridad es particularmente importante cuando hablamos de organismos públicos, y más concretamente aquellos relacionados con la defensa o inclusive bancos en estos días, los cuales éstos deben asegurar y comprometer la información que manejan. En estos entornos los otros dos aspectos de la seguridad son menos críticos. Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son:

Por ejemplo: El uso de técnicas de control de acceso a los sistemas. El cifrado de la información confidencial o de las comunicaciones.

5.2 Integridad.

Es otro servicio de seguridad que garantiza que la información pueda ser modificada, creada y eliminada solo por personal autorizado, teniendo por objetivo asegurar que la información almacenada o circulante no pueda ser corrompida ni falseada ya sea intencional o accidentalmente. Suelen integrarse varios conceptos análogas en este segundo aspecto de la seguridad: precisión, integridad autenticidad.

El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado. De hecho el problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales o no intencionados. En el

ámbito de las redes y las comunicaciones, un aspecto o variante de la integridad es la autenticidad.

Se trata de proporcionar los medios para verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos. En el entorno financiero o bancario, este aspecto de la seguridad es el más importante. En los bancos, cuando se realizan transferencias de fondos u otros tipos de transacciones, normalmente es más importante mantener la integridad y precisión de los datos que evitar que sean interceptados o conocidos (mantener la confidencialidad).En el campo de la criptografía hay diversos métodos para mantener/asegurarla autenticidad de los mensajes y la precisión de los datos recibidos. Se usan para ello códigos/firmas añadidos a los mensajes en origen y recalculadas /comprobadas en el destino. Este método puede asegurar no sólo a integridad de los datos (lo enviado es igual a lo recibido), sino la autenticidad de la misma (quién lo envía es quien dice que es).

5.3 Disponibilidad.

Un sistema seguro debe mantener todos sus datos y recursos disponibles para sus usuarios; entendiéndose en el lugar, momento y forma en que es requerido por el personal autorizado. La situación que se produce cuando se puede acceder a un sistema informático en un periodo de tiempo considerado aceptable. Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo. Lo opuesto a disponibilidad, y uno de los posibles métodos de ataque a un sistema informático, se denomina "negación de servicio". Por ej: Una de negación de servicio significa que los usuarios no puede obtener del sistema los recursos deseados?: El ordenador puede estar estropeado o haber una caída del sistema operativo? No hay suficiente memoria para ejecutar los

programas? Los discos, cintas o impresoras no están disponibles o están llenos? No se puede acceder a la información. De hecho, muchos ataques, como el caso del gusano de 1988, no buscaban borrar, robar, o modificar la información, sino bloquear el sistema creando nuevos procesos que saturaban recursos.

Existen otros aspectos o características de la seguridad que pueden en su mayor parte incluirse o asimilarse a uno de los tres aspectos fundamentales, pero que es importante concretar en sí mismos. Autenticidad. Esta propiedad permite asegurar el origen de la información.

La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser. De este modo se evita que un usuario envíe una información haciéndose pasar por otro. Imposibilidad de rechazo (no repudio). Esta propiedad permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió. Esta propiedad y la anterior son especialmente importantes en el entorno bancario y en el uso del comercio digital.

6. AMENAZAS Y CONTRAMEDIDAS

Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadoras, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad. La confidencialidad nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades; la integridad significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada, y la disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; Es el contrario de la negación de servicio.

Algunos estudios integran la seguridad dentro de una propiedad más general de los sistemas, la confiabilidad, entendida como el nivel de calidad del servicio ofrecido.

Dependiendo del entorno en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad. Por ejemplo, en un sistema militar se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad: seguramente, es preferible que alguien borre información confidencial (que se podría recuperar después desde una cinta de backup) a que ese mismo atacante pueda leerla, o a que esa información esté disponible en un instante dado para los usuarios autoriza

Un sistema Operativo que reúna estos tres aspectos mencionados, debe ser capaz de proteger los tres elementos principales en cualquier sistema informático que son: el software, el hardware y los datos. Por hardware entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, diskettes, etc.) o tarjetas de red. Por software entendemos el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones, y por datos el conjunto de información lógica que manejan el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos. Aunque generalmente en las auditorias de seguridad se habla de un cuarto elemento a proteger, los fungibles (elementos que se gastan o desgastan con el uso continuo, como papel de impresora, tónners, cintas magnéticas, diskettes.), aquí no consideraremos la seguridad de estos elementos por ser externos al sistema.

Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar: con toda seguridad una máquina está ubicada en un lugar de acceso físico restringido, o al menos controlado, y además en caso de pérdida de una aplicación (o un programa de sistema, o el propio núcleo de este software se puede restaurar sin problemas desde su medio original (por ejemplo, el CD-ROM con el sistema operativo que se utilizó para su instalación). Sin embargo, en caso de pérdida de una base de datos o de un proyecto de un usuario, no tenemos un medio "original" desde el que restaurar: hemos de pasar obligatoriamente por un sistema de copias de seguridad, y a menos que la política de copias sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la pérdida.

6.1 Tipos de Amenazas

Generalmente, la taxonomía más elemental de estas amenazas las divide en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación. Un

ataque se clasifica como interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no disponible. Se tratará de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y de una modificación si además de conseguir el acceso consigue modificar el objeto; algunos autores consideran un caso especial de la modificación: la destrucción, entendiéndola como una modificación que inutiliza al objeto afectado. Por ultimo, se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el "fabricado".

En seguridad informática en general, y especialmente en las relativas a seguridad se intenta clasificar en grupos a los posibles elementos que pueden atacar nuestro sistema. A continuación se presenta una relación de los elementos que potencialmente pueden amenazar a nuestro sistema:

Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas. Generalmente se dividen en dos grandes grupos: los atacantes pasivos, aquellos que fisgonean por el sistema pero no lo modifican -o destruyen-, y los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor.

6.1.1 PERSONAL

Las amenazas a la seguridad de un sistema proveniente del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento, etc.) puede comprometer la seguridad de los equipos. Aunque los ataques pueden ser intencionados lo normal es que más que de ataques se trate de accidentes causados por un error o por desconocimiento de las normas básicas de seguridad.

Ex-empleados

Otro gran grupo de personas potencialmente interesadas en atacar nuestro sistema son los antiguos empleados del mismo, especialmente los que no abandonaron el entorno por voluntad propia (y en el caso de redes de empresas, los que pasaron a la competencia). Personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo como venganza por algún hecho que no consideran justo

Curiosos

Junto con los crackers, los curiosos son los atacantes más habituales de sistemas. Aunque en la mayoría de situaciones se trata de ataques no destructivos, parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema.

Crackers

Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Las redes son generalmente abiertas, y la seguridad no es un factor tenido muy en cuenta en ellas; por otro lado, el gran número y variedad de sistemas conectados a estas redes provoca, que al menos algunos de sus equipos sean vulnerables a problemas conocidos de antemano. De esta forma un atacante sólo ha de utilizar un escáner de seguridad contra el dominio completo y luego atacar mediante un simple exploit los equipos que presentan vulnerabilidades.

Terroristas

Por "terroristas" no debemos entender simplemente a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él.

Intrusos remunerados

Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados para robar secretos (el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espía.) o simplemente para dañar la imagen de la entidad afectada.

6.1.2 Amenazas lógicas

Bajo la etiqueta de "amenazas lógicas' encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros). Algunas de las amenazas con que nos podemos encontrar son:

6.1.3 Software incorrecto

Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones.

A estos errores de programación se les denomina bugs, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema.

6.1.4 Herramientas de seguridad

Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

Puertas traseras

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar "atajos" en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se los denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos.

Virus

Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

Gusanos

Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande.

Un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema, pero en un tiempo muchísimo menor. De ahí su enorme peligro y sus devastadores efectos.

Caballos de Troya

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas, es decir que ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

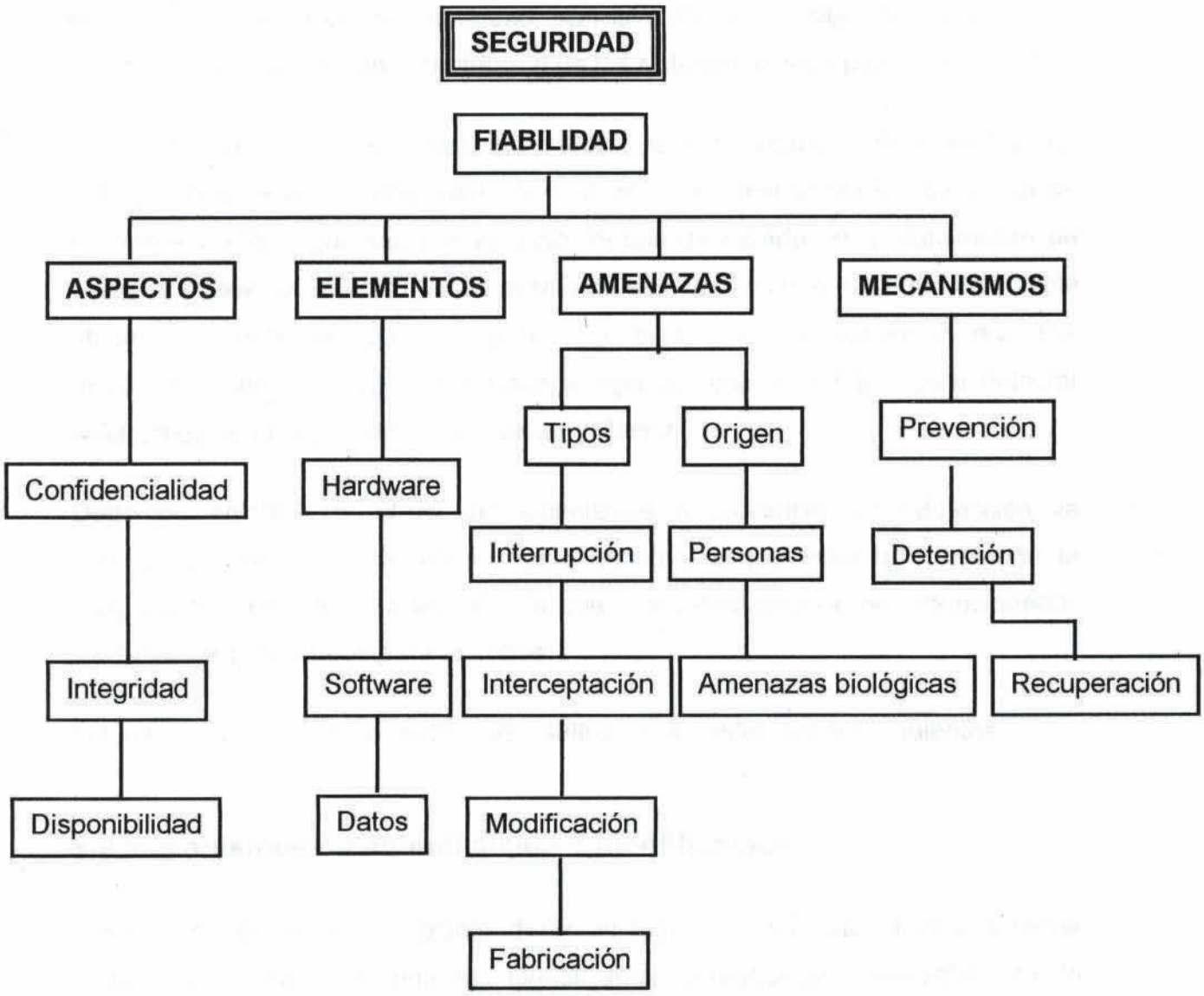
Programas conejo o bacterias

Son los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco, etc.), produciendo una negación de servicio.

Catástrofes

Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: Como ejemplos de catástrofes hablaremos de terremotos, inundaciones, incendios, humo o atentados de baja magnitud (más comunes de lo que podamos pensar).

Hasta ahora se han mencionado los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del origen de tales amenazas; para completar nuestra visión global de la seguridad, queda hablar de las formas de protección de los sistemas.



Para proteger cualquier sistema se deben realizar análisis de las amenazas potenciales que puede sufrir el sistema, las pérdidas que podrían generar, y la probabilidad de su ocurrencia; a partir de este análisis se debe diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan.

A los mecanismos utilizados para implementar esta política de seguridad se las denomina mecanismos de seguridad; son la parte más visible del sistema de seguridad, que garantizan la protección de los sistemas o de la propia red.

Los mecanismos de prevención son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema en la red. Por mecanismos de detección se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación.

Debemos enfatizar en el uso de mecanismos de prevención y de detección, ya que es mucho más productivo para el sistema, a que tener que restaurar la máquina tras una penetración. Por lo que estos dos mecanismos mencionados serán los de más interés para nosotros.

Los mecanismos de prevención más habituales en redes son los siguientes:

6.2 Mecanismos de autenticación e identificación

Estos mecanismos hacen posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quién dice ser). Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto.

6.2.1 Mecanismos de control de acceso

Cualquier objeto del sistema ha de estar protegido mediante mecanismos de control de acceso, que controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema.

6.2.2 Mecanismos de separación

Cualquier sistema con diferentes niveles de seguridad ha de implementar mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles siempre que no exista una autorización expresa del mecanismo de control de acceso.

Los mecanismos de separación se dividen en cinco grandes grupos, en función de como separan a los objetos: separación física, temporal, lógica, criptográfica y fragmentación Mecanismos de seguridad en las comunicaciones

Es especialmente importante para la seguridad del sistema proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. Para garantizar esta seguridad en las comunicaciones, debemos utilizar ciertos mecanismos, la mayoría de los cuales se basan en la Criptografía: cifrado de clave pública, de clave privada, firmas digitales, etc.

Se tiene claro que la palabra seguridad implica muchas cosas y que si hablamos de seguridad en sistemas informáticos, en especial en sistemas que es el que nos lleva a desarrollar este tema, debemos entender que son varios los aspectos que considerar si queremos encontrarnos con un sistema medianamente seguro o mejor dicho "más fiable".

SEGURIDAD DEL ENTORNO DE OPERACIONES

La seguridad del entorno de operaciones comprende dos aspectos que generalizan este entorno:

Seguridad física de sistemas

Administradores, usuarios y personal

SEGURIDAD FÍSICA DE SISTEMAS

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial.

La seguridad física abarca la protección del hardware (del acceso físico y de desastres naturales o climatológicos) y la protección de los datos.

ADMINISTRADORES, USUARIOS Y PERSONAL

El punto más débil de cualquier sistema informático son las personas relacionadas en mayor o menor medida con él; desde un administrador sin una preparación adecuada o sin la suficiente experiencia, hasta un guardia de seguridad que ni siquiera tiene acceso lógico al sistema, pasando por supuesto por la gran mayoría de usuarios, que no suelen ser conscientes de que la seguridad también les concierne a ellos.

Existen otras amenazas a la seguridad provenientes de ese personal que no son necesariamente ataques en un sentido estricto de la palabra; en muchos casos no son intencionados, sino accidentales, lo cual también implica que se deben prevenir.

Entre algunos de los ataques potenciales que pueden ser causados por estas personas, encontramos:

Ingeniería social: consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.

Shoulder Surfing: consiste en "espiar" físicamente a los usuarios para obtener generalmente claves de acceso al sistema.

Masquerading: consiste simplemente en suplantar la identidad de cierto usuario autorizado de un sistema informático o su entorno.

Garbage: consiste en obtener información dejada en o alrededor de un sistema informático tras la ejecución de un trabajo.

Actos delictivos: bajo este nombre se engloba actos tipificados claramente como delitos por las leyes, como el chantaje, el soborno o la amenaza.

Atacante interno: Principalmente que la mayor amenaza a nuestros equipos viene de parte de personas que han trabajado o trabajan con los mismos. Para minimizar el daño que un atacante interno puede causar se suelen seguir principios fundamentales sobre el personal de la empresa, por ej: mínimo privilegio, conocimiento parcial, rotación de funciones y separación de funciones, entre otras.

7. ANÁLISIS DE RIESGOS

La Seguridad Informática tiene como objetivo el mantenimiento de la Confidencialidad, Integridad y Disponibilidad de los Sistemas de Información. Es necesario identificar y controlar cualquier evento que pueda afectar negativamente a cualquiera de estos tres aspectos, así como definir e implantar las defensas necesarias para eliminar o reducir sus posibles consecuencias.

Para ello, deben utilizarse métodos formales de análisis de riesgos que lo garanticen.

7.1 Sus Componentes

En un proceso de Análisis de riesgos se pueden establecer los siguientes componentes:

Sistema de Información. Son los Recursos Informáticos y Activos de Información de que dispone la empresa para su correcto funcionamiento y la consecución de los objetivos propuestos por la Dirección.

Amenaza. Cualquier evento que, pueda provocar daños en los Sistemas de Información, produciendo a la empresa pérdidas materiales o financieras.

Vulnerabilidad. Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas para causarles daño y producir pérdidas a la empresa.

Impacto. Es la medición (y valoración) del daño que podría producir a la empresa la materialización de una amenaza sobre los Sistemas de Información. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, que siempre será subjetiva, de los daños intangibles.

Riesgo. Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema de Información, causando un impacto en la empresa.

Defensa. Cualquier medio, físico o lógico, empleado para eliminar o reducir un riesgo. Debe realizarse una valoración cuantitativa de su coste.

7.2 La Realización de Análisis

En el proceso de Análisis de riesgos se pueden diferenciar:

1. La Evaluación de Riesgos, esta orientada a determinar los Sistemas de Información que, en su conjunto o en cualquiera de sus partes, puedan verse afectados directa o indirectamente por amenazas, valorándose todos los riesgos y estableciendo sus distintos niveles a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la empresa.

2. La Gestión de Riesgos, que implica la identificación, selección, aprobación y manejo de las defensas (contra medidas) para eliminar, o reducir a niveles aceptables, los riesgos evaluados, con actuaciones tendentes a: reducir la posibilidad de que una amenaza ocurra; limitar el impacto de una amenaza, si ésta se manifiesta; reducir o eliminar una vulnerabilidad existente; permitir la recuperación del impacto o su transferencia a terceros (contratación de seguros).

Un primer análisis de riesgos será mucho más costoso que los sucesivos.

Puede requerir mucho tiempo y la participación de personal cualificado y especializado. El tiempo empleado estará en proporción a los objetivos fijados y a su ámbito de cobertura.

Para resaltar la necesidad de sucesivos análisis de riesgos se deben tener en cuenta las siguientes consideraciones:

Los elementos que componen los Sistemas de Información de una empresa están sometidos a constantes variaciones: nuevo personal informático, nuevas instalaciones, nuevos productos, nuevas aplicaciones, etc.

Pueden aparecer nuevas amenazas o variar la probabilidad de que ocurra alguna de las existentes, afectando al posible impacto.

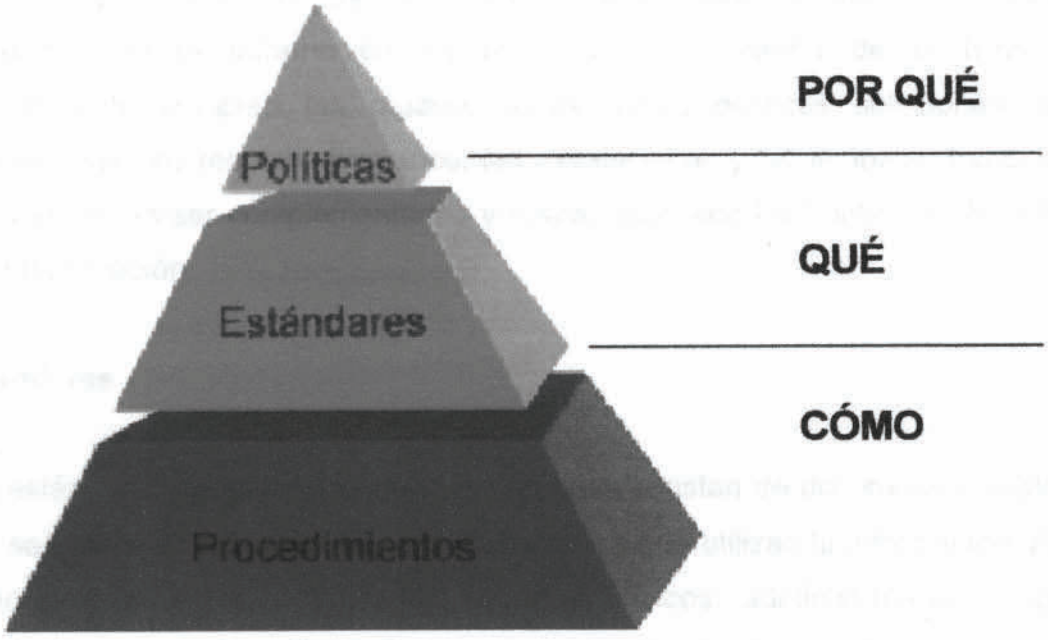
Pueden aparecer nuevas vulnerabilidades o variar (o desaparecer) alguna de las existentes, creando o eliminando posibles amenazas.

En consecuencia, es necesario actualizar periódicamente el análisis de riesgos tomando como base de partida el último realizado y las defensas implantadas hasta la fecha, por lo que los factores tiempo y medios necesarios para su realización serán menores.

El análisis de riesgos, además de centrarse en los Sistemas de Información existentes, es recomendable aplicarlo en el desarrollo de nuevos Sistemas, asegurándolos desde su creación.

8. POLITICAS, ESTANDARES, GUIAS Y SU CLASIFICACION

Las políticas, estándares y procedimientos para la seguridad de la Información son una serie de múltiples documentos interrelacionados que utiliza una organización para administrar y proteger la información de la que depende para sus operaciones actuales y futuras. Desafortunadamente, las discusiones acerca de las "políticas", "estándares" y "procedimientos" para la seguridad de la información son con frecuencia confusas; están llenas de malos entendidos, información errada y definiciones contradictorias.



Una política de seguridad explica con documentación el por qué una organización protege su información.

Los estándares de la organización explican con documentación lo qué la organización quiere hacer para implementar y administrar la seguridad de su información.

Los procedimientos explican con documentación exactamente cómo la organización obtendrá los requerimientos ordenados por estándares y políticas de nivel superior.

Documento de la política de seguridad.

Es importante anotar que la política de seguridad de la información de una organización es un simple documento que articula la filosofía, los requerimientos reglamentarios y las creencias que la organización tiene en relación con la protección a los recursos de la información. Esta política explica con documentación el enfoque del medio ambiente, del personal y de los procesos en donde la aplica, así como las consecuencias de su incumplimiento. La Política de Seguridad de la Información es parte de un conjunto de políticas que generalmente cumplen las organizaciones. Otras políticas solucionan áreas críticas como los recursos humanos, las instalaciones y las finanzas. Estas otras políticas deben ser complementadas y respaldadas con La Política de Seguridad de la Información.

Estándares

Los estándares de seguridad de la información constan de documentos múltiples que se aplican a todas las áreas de la empresa que utilizan la información. Estos estándares abarcan controles de seguridad físicos, administrativos y lógicos (técnicos) que están diseñados para proteger la información. Uno de los documentos de estándares define el contenido y presentación de toda la documentación de seguridad de la compañía de manera que muchas organizaciones contarán con docenas de documentos de los estándares para la seguridad de la información.

Procedimientos

Los procedimientos de seguridad de la información establecen de manera detallada las operaciones que necesitan realizarse para satisfacer los requerimientos especificados en el Estándar que se aplica a una actividad determinada, proceso de seguridad o protección a un recurso de la información.

A fin de proteger adecuadamente los recursos de información de la organización, es importante entender las clases de recursos de información y sus valores respectivos. A continuación se presentan otras dos definiciones cortas:

Recurso de la información: Todo equipo, proceso o información que se asocia con la información y se considera debe ser protegida por la compañía.

Valor de la información: El valor o costo relacionado con lo siguiente:

El valor intrínseco de la información
La creación de la información
El almacenaje de la información
La retención y administración de la información
La protección de la información requiere una inversión inicial y progresiva bien se trate del hardware, software, almacenaje o personal.

A continuación se presentan algunos parámetros básicos que se deben tener en cuenta cuando evalúe el nivel de protección que necesita la información:

Si la información no tiene valor, no la proteja.

Si la pérdida (temporal o permanente), divulgación o modificación de la información no afecta el funcionamiento de la empresa, entonces ¿para qué almacenarla o protegerla? Bórrela. Le ahorrará dinero.

No toda la información es igual -- ¿por qué proteger toda la información al mismo nivel?

En todos los casos, se debe realizar una evaluación de riesgos y análisis del impacto en la empresa por la pérdida (temporal o permanente), divulgación o modificación de su información para determinar el nivel de protección necesario. Si no se realiza un análisis del impacto en la empresa, nunca se sabrá si la información está subprotegida, sobreprotegida o adecuadamente protegida.

La protección a la información no es trivial y requiere de mucho esfuerzo y compromiso administrativos para que sea exitosa.

9. DESARROLLO DE LA POLITICA DE SEGURIDAD

Para nadie es un secreto la importancia de que la empresa implemente un programa completo de seguridad de la información. Sin embargo, crear un programa de seguridad con componentes "bloqueadores de cookies" rara vez produce resultados efectivos. Lo más efectivo es utilizar una metodología comprobada que diseñe el programa de seguridad con base en las necesidades de la empresa.

La clave para desarrollar con éxito documentos para un programa efectivo de seguridad de la información consiste en recordar que las políticas, estándares y procedimientos de seguridad de la información son un grupo de documentos interrelacionados. La relación de los documentos es lo que dificulta su desarrollo, aunque es muy poderosa cuando se pone en práctica. Muchas organizaciones ignoran esta interrelación en un esfuerzo por simplificar el proceso de desarrollo. Sin embargo, estas mismas relaciones son las que permiten que las organizaciones exijan y cumplan los requerimientos de seguridad.

9.1 Metodología para el Desarrollo de Políticas y Procedimientos en Seguridad de Información

Antes de embarcarse en un esfuerzo de elaborar las políticas de seguridad, es aconsejable aclarar quién es responsable de promulgarlas y aplicarlas. Solamente cuando exista claramente la asignación clara de responsabilidades. Si se ignora este paso importante, se corre el riesgo de posteriores objeciones, críticas y malentendidos, que pueden significar problemas y grandes retrasos.

Otro requisito previo necesario para tener éxito involucra la perspectiva de la Junta Directiva y la alta gerencia. Sólo después de que sus miembros tomen conciencia de que los activos de información son un factor vital para el éxito de la organización, es que la seguridad informática es apreciada como un asunto serio

que merece atención. En caso contrario probablemente no apoyen la idea de establecer políticas de seguridad.

La alta gerencia debe darse cuenta que hay problemas serios de seguridad y que se requiere de políticas para afrontarlos. Si bien esto puede parecer obvio, muchos intentos de desarrollar e implantar las políticas no ha llegado a ninguna parte porque no se habían echado las bases. El trabajo previo incluye a menudo una breve presentación a la alta gerencia para sensibilizarla sobre la necesidad de la seguridad informática.

Idealmente, el desarrollo de políticas de seguridad debe comenzarse después de una evaluación a fondo de las vulnerabilidades, amenazas y riesgos. Esta evaluación debería indicar, quizás sólo a grandes rasgos, el valor de la información en cuestión, los riesgos a los cuales esa información se sujeta, y las vulnerabilidades asociadas a la manera actual de manejar la información. También pueden ser incluidos en la declaración de las políticas, los tipos generales de riesgos enfrentados por la organización, así como cualquier otra información útil obtenida a partir del análisis de riesgos.

Un buen momento para desarrollar un conjunto de políticas de seguridad es cuando se está preparando el manual de seguridad para los activos de información. Debido a que ese manual va a ser distribuido a lo largo de toda la organización, representa un medio excelente para incluir también las políticas de seguridad. También pueden publicitarse las políticas en material tal como video, carteles o artículos en un periódico interno.

Otro bueno momento es después de que haya ocurrido una falla grave en seguridad, por ejemplo una intrusión de hackers, un fraude informático, un accidente sin poder recuperar los datos, un incendio y en general algún tipo de daño o perjuicio que haya recibido la atención de la alta gerencia. En este caso habrá un alto interés en que se apliquen las políticas de seguridad y que se

implanten medidas más efectivas. Hay que actuar rápidamente para desarrollar las políticas, ya que el nivel de preocupación de los gerentes y de los empleados tiende a decrecer luego que ha pasado el incidente.

Un buen objetivo a tener presente cuando se redactan las políticas, es que ellas deberían durante varios años, por ejemplo cinco años. En realidad, se harán modificaciones más a menudo, pero para evitar que se vuelvan obsoletas rápidamente, debe elaborarse para que sean independientes de productos comerciales específicos, estructuras organizativas específicas, así como las leyes específicas y las regulaciones.

Las cosas mueven muy rápidamente en el campo de tecnología, incluyendo la seguridad informática. Por ejemplo, hace apenas algunos años la mayoría de las organizaciones no creían que era necesaria una política de seguridad para Internet, pero hoy día es muy importante.

Las políticas deben revisarse en forma periódica, preferiblemente cada año, para asegurarse de que todavía son pertinentes y efectivas. Es importante eliminar aquellas políticas que ya no son útiles o que ya no son aplicables. Este esfuerzo también ayudará a mejorar la credibilidad de las actividades de seguridad informática dentro de la organización. Los empleados apreciarán que el personal de seguridad informática no está allí para crear más burocracia, sino para realmente ocuparse de las medidas de seguridad requeridas para proteger los recursos.

¿Cómo deben elaborarse las políticas?

a) recopilar material de apoyo

Para elaborar eficazmente un conjunto de políticas de seguridad informática, debe haberse efectuado previamente un análisis de riesgo que indique claramente las

necesidades de seguridad actuales de la organización. Antecedentes de fallas en la seguridad, fraudes, demandas judiciales y otros casos pueden proporcionar una orientación sobre las áreas que necesitan particular atención.

Para afinar aun más el proceso, se debe tener copia de todas las otras políticas de organización (o de otras organizaciones similares) relativas a compra de equipos informáticos, recursos humanos y seguridad física.

b) Definir un marco de referencia

Después de recopilar el material de apoyo, debe elaborarse una lista de todos los tópicos a ser cubiertos dentro de un conjunto de políticas de seguridad. La lista debe incluir políticas que se piensa aplicar de inmediato así como aquellas que se piensa aplicar en el futuro.

c) Redactar la documentación

Después de preparar una lista de las áreas que necesitan la atención y después de estar familiarizados con la manera en que la organización expresa y usa las políticas, se estará ahora listos redactar las políticas, para lo cual pueden servir de ayuda el ejemplo que se encuentra más adelante.

Las políticas van dirigidas a audiencias significativamente distintas, en cuyo caso es aconsejable redactar documentos diferentes de acuerdo al tipo de audiencia. Por ejemplo, los empleados podrían recibir un pequeño folleto que contiene las políticas de seguridad más importantes que ellos necesitan tener presente. En cambio, el personal que trabaja en informática y en telecomunicaciones podría recibir un documento considerablemente más largo que proporciona mucho más detalles.

Una vez que se hayan elaborado los documentos sobre las políticas, deben ser revisados por un comité de seguridad informática antes de ser sometido a consideración de la Presidencia y Junta Directiva para su aprobación. Este comité debería tener representantes de los distintos departamentos de la organización y una de sus funciones más importantes es evaluar las políticas en la luz de su viabilidad, análisis costo/beneficio y sus implicaciones. Las preguntas que debe contestar son, por ejemplo: ¿Son estas políticas prácticas y fácilmente aplicables? ¿Son estas políticas claras e inequívocas?

Es muy importante que la Junta Directiva apruebe las políticas en el caso frecuente que ciertos empleados objeten o piensen que ellos no necesitan obedecer.

Además es fundamental de que luego de la entrada en vigor, las políticas se apliquen estrictamente, ya que de otra forma se puede fomentar la hipocresía entre los empleados y la tolerancia por conductas inapropiadas. El tener políticas que no se aplican puede ser peor que no tener políticas en absoluto.

La aplicación de nuevas políticas es a menudo más eficaz si los empleados han sido informados de exactamente qué actividades representan trasgresiones de la seguridad y qué penalización recibirían si fueran encontrados culpables.

Un curso o taller de sensibilización es una forma muy efectiva para dar a conocer las nuevas políticas. Allí, por ejemplo, se explicaría que la información interna es la propiedad de organización, y que no puede ser copiada, modificada, anulada o usada para otros propósitos sin la aprobación de la gerencia.

La longitud del documento sobre las políticas debe diseñarse de acuerdo a las necesidades específicas e una organización. Algunas organizaciones tienen muchas políticas, mientras otros tienen sólo unas cuantas. Como ejemplo, el manual sobre las políticas de seguridad de British Telecom (una compañía

telefónica británica) es de más de 150 páginas, mientras que el de Lockheed (una compañía aerospacial) es de 75 páginas.

El personal de seguridad puede opinar que es necesario que todo esté absolutamente claro y explícito sobre los asuntos de seguridad informática. En estos casos puede que se requiere un conjunto de políticas.

Otros serán renuentes a tener tantas políticas, prefiriendo enfatizar la confianza en buen juicio y buen comportamiento de los empleados.

Aunque un documento conciso será leído y asimilado con más probabilidad, hay mucho a favor de un conjunto completo y extenso de políticas de seguridad. Un principio general es que se deben promulgar sólo aquellas políticas que sean absolutamente necesarias. Esto es debido a que las personas son inherentemente muy diferentes entre sí, como también son diferentes los grupos a que pertenecen. El imponer un único conjunto de reglas para todos puede llevar a resistencia y a pobres resultados. En cambio, al tener sólo aquellas políticas que son estrictamente necesarias, se favorece la iniciativa personal y la creatividad. Además tantas políticas de seguridad van a impedir que el trabajo se haga a tiempo.

En todo caso, en vez de emprender un trabajo a fondo, es mejor empezar primero ocupándose de los aspectos esenciales, para luego ir ampliando con políticas adicionales. Este procedimiento toma a menudo la forma de declaraciones separadas que se tratan las áreas problemáticas, por ejemplo PCs, LANs e Internet. De esta manera es también más fácil conseguir la aprobación de la alta gerencia así como de los propios empleados.

Por otro lado las políticas nunca pueden tomar en cuenta todas las circunstancias y un conjunto extenso y minucioso de políticas puede generar críticas, disgusto y rechazo.

La extensión y el grado de detalle de las políticas es una función de tipo de audiencia y puede haber distintos documentos según el caso. Por ejemplo, podría haber documentos para los usuarios, la gerencia y el personal de informática. Muchas de las políticas en cada uno de estos documentos serían iguales, aunque el grado de detalle, las palabras técnicas utilizadas, y el número de ejemplos puede variar de un documento a otro. Para los usuarios finales, el documento debe limitarse a unas cuantas páginas. Para la gerencia habrá consideraciones adicionales, tal como los aspectos legales, y es probable que esto extienda el documento. Para el personal técnico será todavía más largo y más detallado. Otro factor que afecta es el grado de seguridad requerido en la organización. En general, cuánto mayor es el uso de la información para las actividades de una organización, mayor es la necesidad de seguridad. Por ejemplo, un banco tendrá muchas y extensas políticas, mientras que una cadena de tiendas por departamentos tendrá menos políticas. Por supuesto que actividades especialmente delicadas, tal como salud y defensa, requieren de políticas muy detalladas.

Adicionalmente al número de políticas, hay que plantearse cuán larga debe ser la definición de cada política. Las definiciones concisas, de unas cuantas frases, son más aceptadas por los empleados ya que son más fácilmente leídas y entendidas. En todo caso deben ser suficientemente específicas para ser entendidas e interpretadas sin ambigüedad, pero no deben ser tan específicas que impidan adaptarlas a las condiciones particulares de un sitio o departamento. Por ejemplo, se puede promulgar una política la cual especifica que todos los usuarios deben usar contraseñas difíciles de adivinar. Esta política da la flexibilidad a un gerente local para determinar su longitud mínima o un sistema automático que chequee si realmente una dada contraseña es difícil de adivinar.

Para ayudar a aclarar qué son las políticas, se pueden incluir ejemplos específicos. Como ilustración, una política que prohíbe el uso de los recursos

computacionales para fines personales podría incluir ejemplos sobre Internet Chat Relay (IRC) o juegos por computadora.

Si se opta por elaborar un conjunto muy completo de políticas de seguridad, se aconseja hacerlo en dos etapas. El primer paso involucra el obtener la aprobación de la Junta Directiva para un conjunto genérico de políticas, mientras que el segundo paso involucra la aprobación para un conjunto más específico de políticas. El conjunto genérico podría incluir de 10 a 20 políticas, y el juego específico podría incluir otras 50-100.

De hecho, si el conjunto inicial de políticas es demasiado largo o severo, la Junta Directiva puede rechazarlo. Como resultado, la ventana de tempo para conseguir la aprobación puede cerrarse por un cierto periodo de tiempo (a menudo un año o más). Así que se aconseja elaborar un primero conjunto de políticas corto y relativamente fácil de cumplir por parte del personal. Después, cuando haya sido implantado y asimilado a lo largo de la organización, se puede preparar una lista más completa y más estricta. Es mucho mejor proceder de forma relativamente lenta, con una serie pasos en el desarrollo de políticas, y así lograr credibilidad y apoyo, que preparar de una vez un solo documento extenso con todas las políticas, el cual se rechaza porque fue percibido como engorroso o excesivamente severo.

9.2 Políticas de Seguridad Justificación

Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra Compañía. Sin ellos nos quedaríamos rápidamente fuera del negocio y por tal razón la Presidencia y la Junta Directiva tienen el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales

como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La información perteneciente a la Compañía debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se procesa (PCs, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Las distintas gerencias de la Compañía están en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos. En todo caso cada año el Comité de Seguridad Informática llevará a cabo un análisis de riesgos y se revisarán las políticas de seguridad. Así mismo, se preparará cada año un informe para la Junta Directiva que muestre el estado actual de la Compañía en cuanto a seguridad informática y los progresos que se han logrado.

A todos los empleados, consultores y contratistas debe proporcionárseles adiestramiento, información, y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la Compañía. Debe hacerse hincapié en que la seguridad informática es una actividad tan vital para la Compañía como lo son la contabilidad y la nómina.

La finalidad de las políticas de seguridad que se describen más adelante es proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los computadores de la Compañía (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

9.3 RESPONSABILIDADES

Los siguientes entes son responsables, en distintos grados, de la seguridad en la Compañía:

El Comité de Seguridad Informática está compuesto por los representantes de los distintos departamentos de la Compañía, así como por el Gerente de Informática, el Gerente de Telecomunicaciones (cuando exista), y el abogado o representante legal de la Compañía. Este Comité está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad en informática y telecomunicaciones. También es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones trimestrales o ad hoc, el Comité efectuará la evaluación y revisión de la situación de la Compañía en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad.

La Gerencia de Informática es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Junta Directiva y la Gerencia de Telecomunicaciones (cuando exista). También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

El Jefe de Seguridad es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

El Administrador de Sistemas es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como por ejemplo, aplicar inmediatamente los parches correctivos cuando le llegue la notificación del fabricante del producto o de un ente como el CERT (Computer Emergency Response Team). El Administrador de Sistemas también es responsable de informar al Jefe de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un Jefe de Seguridad, el Administrador de Sistemas realizará sus funciones.

Los usuarios son responsables de cumplir con todas las políticas de la Compañía relativas a la seguridad informática y en particular:

Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.

No divulgar información confidencial de la Compañía a personas no autorizadas.

No permitir y no facilitar el uso de los sistemas informáticos de la Compañía a personas no autorizadas.

No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Compañía.

Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.

Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.

Reportar inmediatamente a su jefe inmediato a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la Compañía y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

9.4. Políticas de seguridad para computadores.

Los computadores de la Compañía sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

Los equipos de la Compañía sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática

No se permite fumar, comer o beber mientras se está usando un PC.
Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS).

Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.

Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Compañía se requiere una autorización escrita.

La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.

Si un PCs tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente.

Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Compañía.

A menos que se indique lo contrario, los usuarios deben asumir que todo el software la Compañía está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

Los usuarios no deben copiar a un medio removible (como un diskette), el software o los datos residentes en las computadoras de la Compañía, sin la aprobación previa de la gerencia.

No pueden extraerse datos fuera de la sede de la Compañía sin la aprobación previa de la gerencia. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.

Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.

Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la Compañía.

No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.

Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el Departamento de Informática.

Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la Compañía a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

Periódicamente debe hacerse el respaldo de los datos guardados en PCs y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de Compañía debe guardarse en otra sede, lejos del edificio.

Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los gerentes de los distintos departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).

La información de la Compañía clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por la Gerencia de Informática.

No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.

El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

Siempre que sea posible, deba eliminarse información confidencial de de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de una representante de la Compañía.

No deben salirse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la Compañía.

El personal que utiliza un computador portátil que contenga información confidencial de la Compañía, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información debe estar cifrada.

9.5. Políticas de seguridad para las comunicaciones Propiedad de la informacion.

Con el fin de mejorar la productividad, la Compañía promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de

voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la Compañía y no propiedad de los usuarios de los servicios de comunicación.

Uso de los sistemas de comunicación.

Los sistemas de comunicación de la Compañía generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la Compañía.

Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Compañía y en tal sentido deben usarse las horas no laborables.

Confidencialidad y privacidad

Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que estén cifrada. Para tal fin debe utilizarse PGP (Pretty Good Privacy), Outolook, Outlook Express u otros productos previamente aprobados por la Gerencia de Informática.

Los empleados y funcionarios de la Compañía no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La Compañía se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.

Es política de la Compañía no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoria. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.

De manera consistente con prácticas generalmente aceptadas, la Compañía procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica (PABX) contienen detalles sobre el número llamado, la duración de la llamada, y la hora en que se efectuó la llamada.

Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la Compañía, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de la Compañía sin la debida aprobación.

Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

9.6 Políticas de seguridad para redes

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la Compañía al estar conectada a redes de computadoras.

Alcance

Esta política se aplica a todos los empleados, contratistas, consultores y personal temporal de la Compañía.

Aspectos generales

Es política de la Compañía prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

Modificaciones

Todos los cambios en la central telefónica (PABX) y en los servidores y equipos de red de la Compañía, incluyendo la instalación de el nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

Cuentas de los usuarios

Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.

No debe concederse una cuenta a personas que no sean empleados de la Compañía a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

Privilegios especiales, tal como la posibilidad de modificar o barrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Gerente de Informática determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad.

Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

Cuando un empleado es despedido o renuncia a la Compañía, debe desactivarse su cuenta antes de que deje el cargo.

Contraseñas y el control de acceso

El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

Para el acceso remoto a los recursos informáticos de la Compañía, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña (o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad).

Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Compañía, pudiendo ser causal de despido.

Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

Los archivos de bitácora (logs) y los registros de auditoria (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoria. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

Los servidores de red y los equipos de comunicación (PABX, routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo, tarjetas de proximidad).

10. ASPECTOS DE IMPLEMENTACION EN LAS POLITICAS DE SEGURIDAD.

Como se muestra en la figura 1, el diseñar una Política de Seguridad para su posterior implementación no puede ser un acto caprichoso, de momento, de moda; es un proyecto completo que debe ser asumido con la mayor responsabilidad si se quiere lograr el efecto buscado. Cada una de estas etapas cumple papel importante en el exitoso final del proyecto.

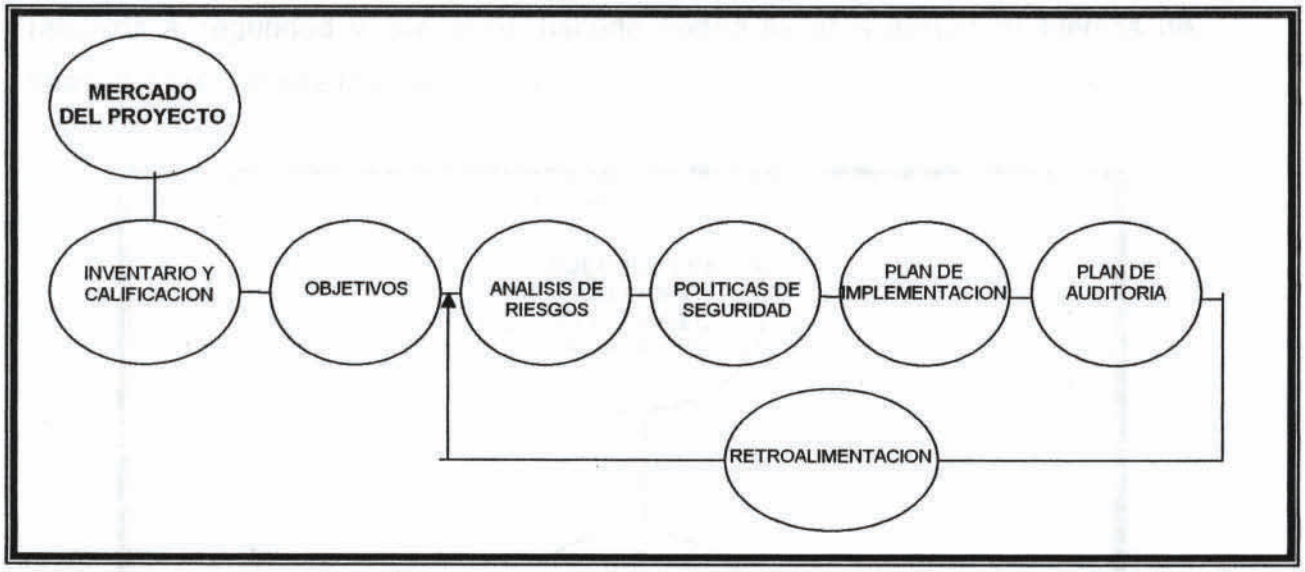


Fig. 1. ETAPAS EN EL DISEÑO E IMPLEMENTACION DE UNA POLITICA DE SEGURIDAD

Mercadeo del Proyecto

Vender un nuevo proyecto nunca es fácil y mas si se trata de asuntos relacionados con la seguridad en sistemas, donde muchos consideran que no tienen riesgos o no son de su interés y piensan que las Políticas de Seguridad basta con copiarlas de otras instalaciones o usar el sentido común para expedir un recetario de normas. Como se aprecia en la figura 2, se pueden usar diferentes estrategias para involucrar a la alta gerencia en el proyecto, sin la participación de la cual

jamás se logrará llevarlo al punto que se requiere. Esta etapa enfrenta el poco interés de las altas directivas de la empresa, el desconocimiento de la importancia de la seguridad informática y el exceso de tecnicismo de los expertos en seguridad. Para facilitar el trabajo de concientización es bueno apoyarse en casos de fallos de seguridad ocurridos en negocios similares y los efectos generados; hacer notar la responsabilidad que cabe a las empresas que no han realizado los esfuerzos necesarios para minimizar los riesgos y que debido a ello pueden infringir normas legales o afectar a otros; para finalizar se puede evaluar la razón costo/beneficio de las medidas tendientes a enfrentar con seriedad los aspectos relativos a seguridad y que el no hacerlo podría llevar a graves problemas de imagen y prestigio de la organización

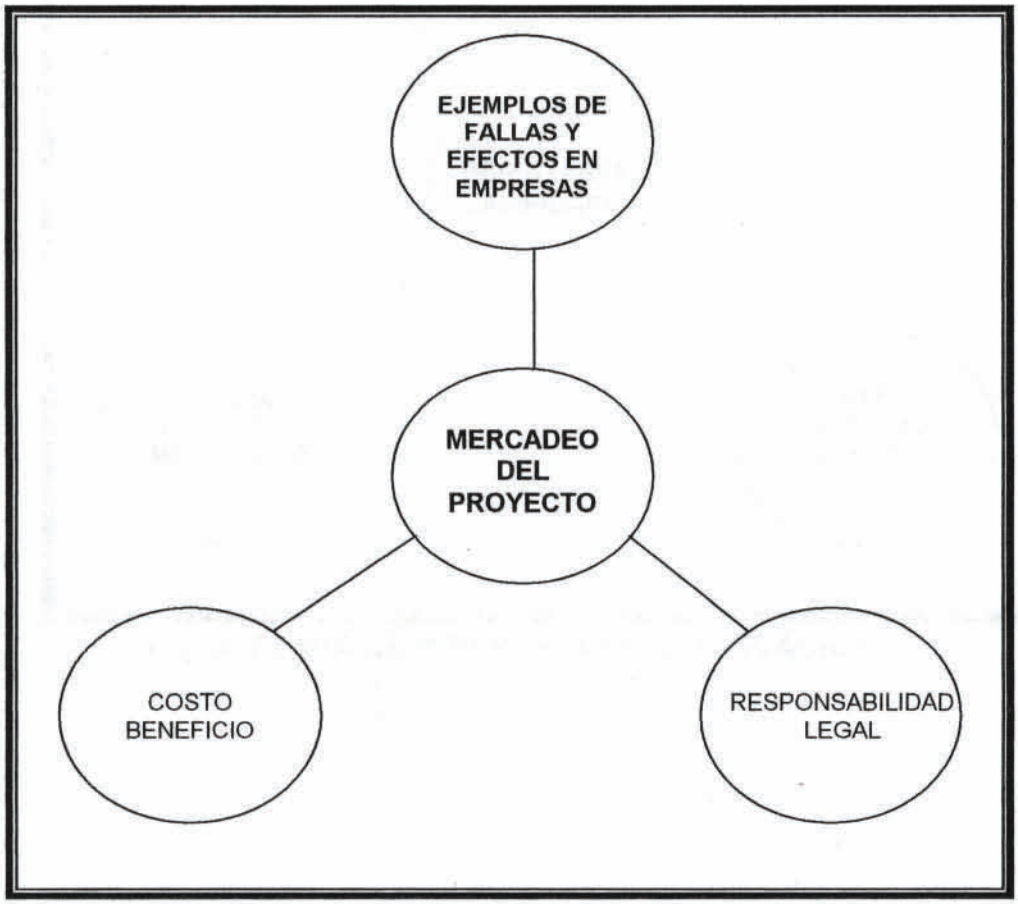


Fig. 2. ETAPA DE MERCADEO DEL PROYECTO

Inventario y Calificación

Para saber que hay que proteger es necesario hacer un juicioso inventario de recursos informáticos (hardware, software), y de los servicios ofrecidos, donde se determine la importancia para la organización y el grado de criticidad de cada uno. En la figura 3 se aprecian estos elementos.

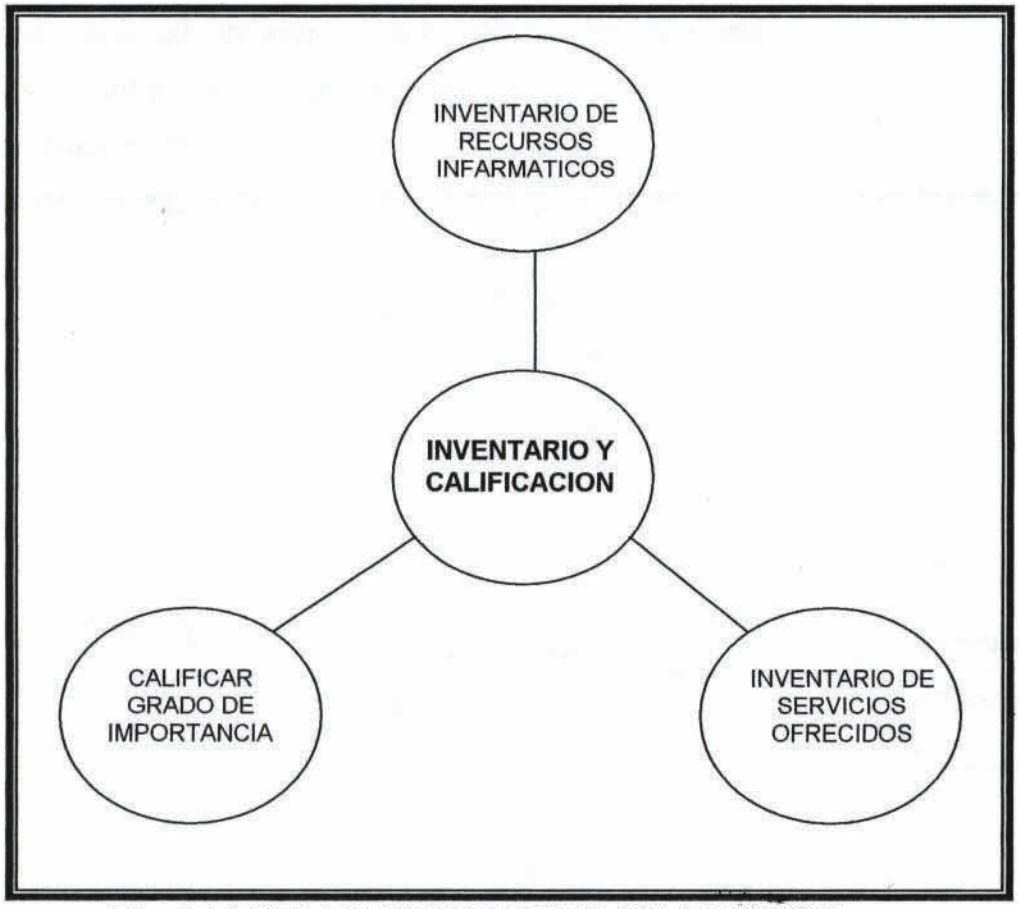


Fig. 3. ETAPA DE INVENTARIO Y CALIFICACION

Determinar los Objetivos

Están asociados, como se aprecia en la figura 4, a los objetivos de la Seguridad Informática, orientados a proteger la organización contra amenazas que atenten contra:

1. La continuidad de las operaciones.
2.-La confidencialidad y privacidad de la información manejada.
3. La confiabilidad y exactitud del sistema.
4. La seguridad física.

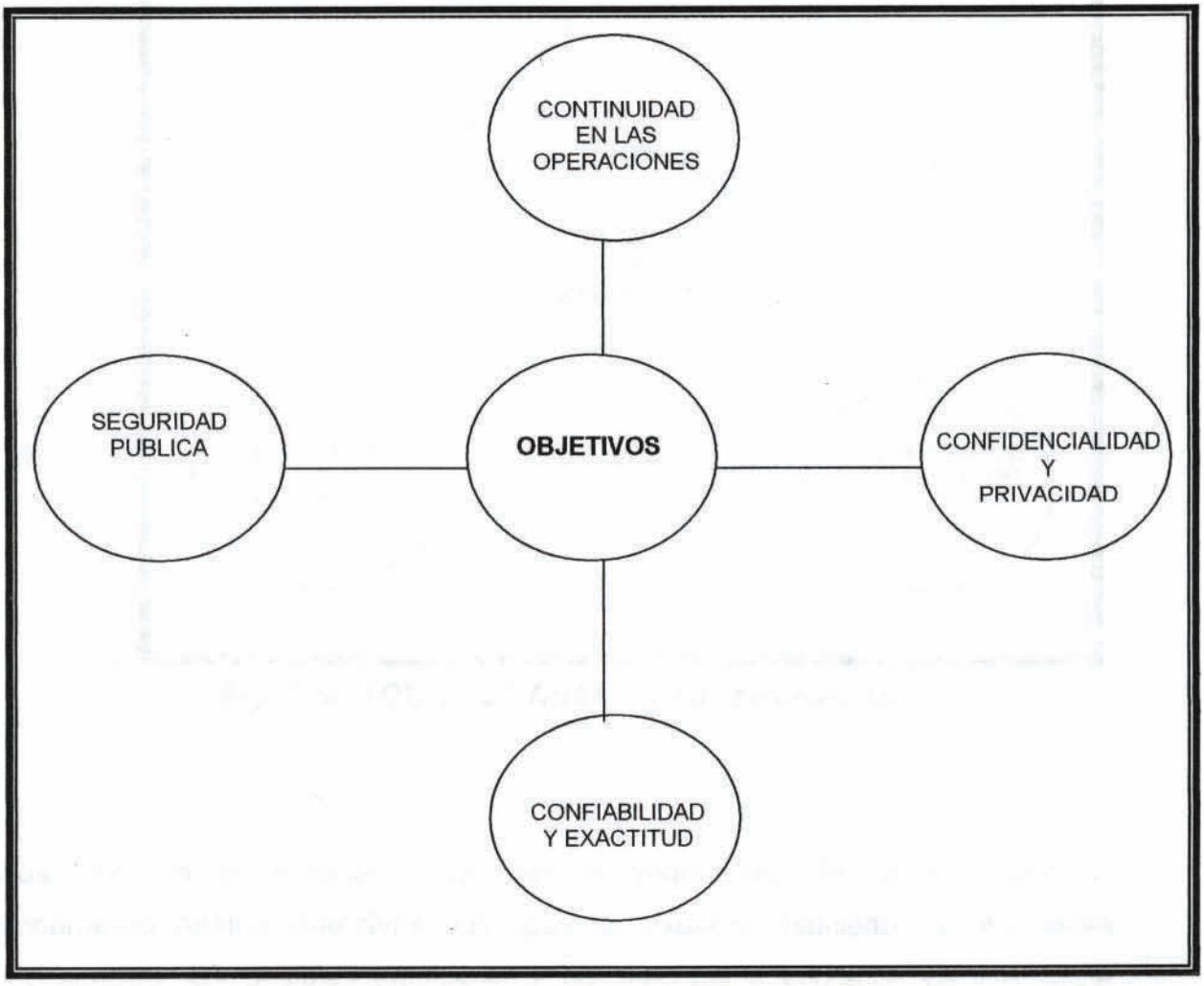


Fig. 4. OBJETIVOS DE LA SEGURIDAD

Análisis de Amenazas

En la figura 5 se aprecian algunas de las posibilidades que se tienen de conocer los riesgos que se presentan para los diferentes recursos de la organización.

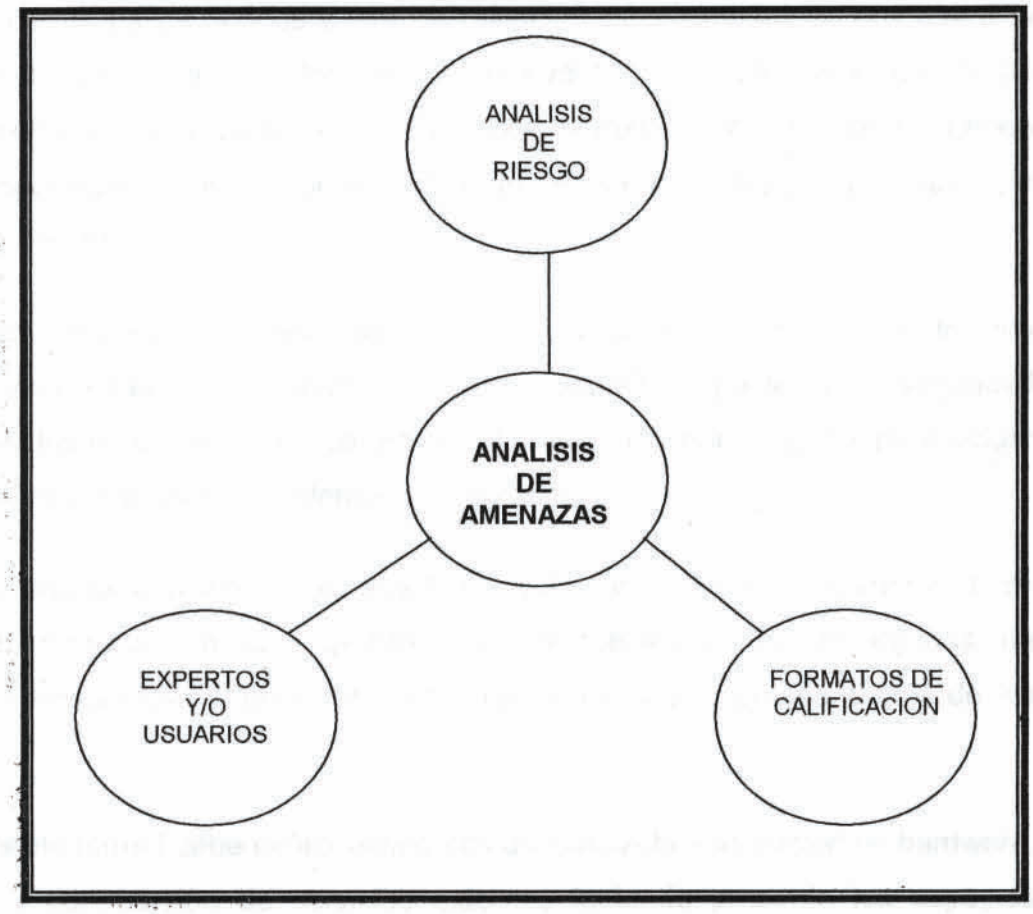


Fig. 5. METODOS DE ANALISIS DE AMENAZAS

Los formatos de calificación recogen la información de cada recurso, la importancia relativa que tiene, los tipos de usuarios asociados a situaciones indeseables, las posibles amenazas y las medidas a implantar para proteger suficientemente los activos contra esos riesgos.

Como otra forma, pero casi siempre acompañando algunos de los métodos anteriores se recurre a la opinión de expertos y a las vivencias de los usuarios del sistema, para recolectar información de los probables riesgos y los efectos a que están expuestos los procesos o corrientes de información.

Políticas de Seguridad Informática

Después de los pasos previos y con los conocimientos ganados se procede a la construcción del documento formal que incluirá los diversos elementos. Debe entenderse esta etapa como la del diseño de la Política de Seguridad y deben quedar especificados los diferentes componentes que cubrirá y la forma como se aplicará la misma.

La Política de Seguridad tiene dos propósitos centrales: Informar a todos los usuarios sobre las obligaciones que deben asumir respecto a la seguridad asociada a los recursos de tecnología de Información y dar las guías para actuar ante posibles amenazas y problemas presentados.

Para que pueda convertirse en esa línea guía, es necesario involucrar a los diferentes sectores en la organización: Alta gerencia, los encargados de seguridad, los auditores, gerentes de las dependencias y representantes de los usuarios.

El documento formal debe definir elementos asociados la adquisición de hardware, software y contratación de servicios externos teniendo presente los aspectos referentes a seguridad (outsourcing, mantenimiento a hardware y/o software, desarrollo de aplicaciones, administración de proyectos, etc.); las disposiciones sobre privacidad y control de acceso incluidas las políticas de autenticación; las responsabilidades asociadas a las métodos de actuación y el manejo de incidentes. Un aspecto importante es la declaración de disponibilidad, entendida como el compromiso que hace el área de sistemas informáticos sobre el mínimo nivel la prestación de servicios en términos de tiempo y cobertura que se garantizará.

Un reto importante es lograr todo lo anterior emitiendo un documento sencillo y claro, apoyado por la alta dirección, que permita la normal actuación, haciendo de las políticas procedimientos inmersos en los tareas cotidianas, enfocados a los problemas relevantes, fácil de ajustar a los cambios permanentes, que garanticen su cumplimiento apoyándose en herramientas de seguridad antes que orientado a castigar a los infractores, lo cual no se descarta. Pero hay que resaltar algunas características que hacen de ella una buena Política de Seguridad: La constante actualización y el hacerla pública y respaldada por los usuarios en la vida práctica.

Plan de Implementación

Terminado el diseño, se procede a la fase de construcción.

Plan de Auditoria

En un medio cambiante y en especial en las nuevas tecnologías informáticas y de comunicación, no ha pasado mucho tiempo sin que las condiciones varíen, esto puede llevar a nuevos riesgos y debe actuarse pro activamente para lograr los sistemas auto controlado que tanto se pregonan. La labor de auditoria entendida como la evaluación y análisis de esa realidad, en forma critica, objetiva e independiente, con el objeto de evaluar el grado de protección que presenta una instalación ante las amenazas a que está expuesta; es parte importante del diseño e implantación de Políticas de Seguridad. No basta con diseñar buenas políticas es necesario llevarlas a la práctica en forma correcta y garantizar que se adecuan a nuevas condiciones

Retroalimentación

La implementación de Políticas de Seguridad, genera diferentes situaciones en los negocios lo que obliga al manformacintenimiento constante. Los cambios deben iniciarse con un nuevo análisis de riesgos detectados en la labor de auditoria.

CONCLUSIONES

Un negocio depende de la calidad y disponibilidad de la información. El almacenamiento apropiado de esta información es esencial para las operaciones de cualquier negocio.

Una política de seguridad informática fija los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen.

Si bien existen algunos modelos o estructuras tipo, tiene que diseñarse "a medida" para así recoger las características propias de cada compañía.

Una buena política de seguridad corporativa debe recoger, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos.

Esta visión general resulta vital para asegurar un nivel homogéneo en el grado de seguridad que quiera alcanzarse, y evitar la aparición de "agujeros" en determinados puntos del sistema.

En definitiva, de nada sirve un excelente cortafuegos si no se encuentra instalado un buen antivirus, o tener un avanzado software de detección de intrusos si se carece de una adecuada política de contraseñas para los usuarios.

Las áreas que contemplen las políticas de seguridad variarán en función de cada empresa y sistema. Como mínimo deberán abordar apartados tales como: evaluación de riesgos, protección perimétrica, control de acceso a los recursos, directrices de uso de Internet y correo electrónico, antivirus, y copias de seguridad.

Otra característica importante que no debe olvidarse en las políticas de seguridad es su mantenimiento y revisión periódica. En la práctica, el crecimiento y la modificación de los sistemas de la empresa, así como la continua aparición de nuevas vulnerabilidades y amenazas, exigen que la política de seguridad corporativa sea un elemento vivo que se vaya adaptando a las necesidades que vayan surgiendo.

Como conclusión me gustaría que quedara claro que la Seguridad Informática es un aspecto muchas veces descuidado en nuestros sistemas, pero de vital importancia para el correcto funcionamiento de todos ellos.

Sería importante hacer hincapié en los siguientes conceptos:

- Todo sistema es susceptible de ser atacado, por lo que conviene prevenir esos ataques.
- Conocer las técnicas de ataque ayuda a defenderse más eficientemente.
- Elegir Sistemas Operativos con poco énfasis en la seguridad, puede suponer un auténtico infierno.
- La seguridad basada en la ocultación no existe.

Cabe preguntarse qué hacer, qué pasos dar. No hay soluciones únicas, sino que dependen de la entidad y del momento por lo que se indican los siguientes pasos generales.

- Debe permitirse una política corporativa sobre la seguridad.
- El paso siguiente debe ser la designación de personas concretas para funciones determinadas.

Y si no existe una idea clara de cuáles son los riesgos debe hacerse una evaluación de dichos riesgos, por personas objetivas.

Una vez conocidos los riesgos se deben tomar decisiones, tendentes a eliminarlos, que no siempre es posible, a reducirlos, a transferirlos, o bien aceptarlos, a un nivel suficientemente alto y corporativo.

Cabe mencionar que la seguridad informática ha de ser una preocupación constante de las empresas, a un nivel suficientemente alto, que no es un problema exclusivamente técnico y de los técnicos, y que se trata de un camino para el que puede haber indicaciones, pero que serán diferentes según la empresa y el momento.

BIBLIOGRAFIA

[1] Caballero Gil, Pino. "Seguridad informática. Técnicas criptográficas", 2001.

[2] NORMA ISO 7498-2: Sistemas de Procesamiento de la Información - Sistemas Interconectados Abiertos (OSI) – Modelo de Referencia Básica. Parte 2: Arquitectura de Seguridad.

[3] Reglamento de Ética de la UPR, 2001.

[4] REQUEST FOR COMMENTS (RFC) 2196. Network Working Group - Internet Engineering Task Force (IETF).

[5] Pagina de Seguridad Informática http://WWW.Virusprot.com

[6] Pagina de Seguridad Informática http://www.nextvision.com

[7] Internet Secure Comunication between Citizen and Public Administrator, Javier López, otros, Universidad de Málaga, España.

[7] Intranets. Usos y Aplicaciones, Randy J. Hinrichs, PRENTICE HALL, México, 1998.

TÉCNICAS CRIPTOGRÁFICAS DE PROTECCIÓN DE DATOS. 2ª EDICIÓN.

SABATER / DE LA GUÍA / HERNANDEZ / MONTOYA / MUÑOZ. EDIT ALFA OMEGA – RAMA, MÉXICO, 2001