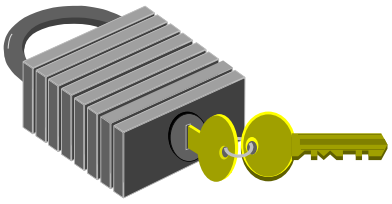
POLITICAS Y SEGURIDAD DE LA INFORMACION

Walter Vega Velasco

Docente Ingeniería de Sistemas



INTRODUCCION.

El gran desarrollo de las tecnologías de las Telecomunicaciones y de la Informática en las últimas décadas ha permitido el crecimiento exponencial del servicio de Internet. Al presente todos pueden acceder a este servicio. La información ha sido globalizada.

Habiendo comenzado en los años 80 con algunos miles de usuarios hoy se benefician de este servicio miles de millones. Tanto es así que según las últimas estadísticas el número de direcciones IP actualmente en uso en Internet alcanza los 3/4 de la capacidad total que permite el rango de direcciones IPv4.

Hoy en día es mejor tener una página WEB que no tenerla. El servicio de Internet permite a las Empresas y a cualquier Institución realizar publicidad de sus productos y servicios, simplificar las transacciones, ganar tiempo, ahorrar recursos y compartir y acceder a la información. El E-commerce y el E-business permiten conducir los negocios por Internet. Para una Organización tradicional esto significa ampliar la distribución de su catálogo de ofertas prácticamente sin fronteras, lo cual abre su mercado de una manera nunca imaginada con un costo muy bajo.

Una página WEB constituye una herramienta incansable y económica de publicidad y mercadeo. Las unidades de producción de las Empresas llevan a cabo acciones orientadas por los siguientes factores determinantes: Ventajas competitivas, innovación tecnológica y acceso a los mercados

Particularmente, las nuevas tendencias revelan un creciente consenso en torno al impacto que tiene la innovación tecnológica para el desarrollo económico y mejorar el nivel de vida de los ciudadanos. La innovación tecnológica es el resultado de quienes la crean y difunden (Universidades y Centros de Enseñanza, Centros de investigación), quienes la incentivan (Sector gubernamental) y quienes la utilizan económicamente (las empresas).

El E-businness permite mejorar el servicio al cliente, reducir los costos, y dar apoyo a la expansión de la Empresa sin necesidad de personal adicional. Quien tiene la

información tiene el poder se afirma muchas veces, la información es un recurso de la Empresa. Las organizaciones necesitan estar conectados en una red por obtener: imagen comercial, rentabilidad, flujo de fondos.

SEGURIDAD DE LA INFORMACION

Las facilidades para conectarse a las redes hay aumentado; además, las aplicaciones y el software son cada vez más amigables y accesibles, de esto modo todos tienden a conectarse en una red para compartir los recursos, pero esa facilidad de conexión también representa un aumento en los riesgos de que la información y los recursos de una organización puedan ser vulnerados.

Es por eso que se deben implementar medidas de seguridad para proteger la información y los activos de la Empresa.

Seguridad significa disponer de medios que permitan reducir lo más que se pueda, la vulnerabilidad de la información y de los recursos; aunque no se puede alcanzar el 100% de seguridad, la tendencia debe ser llegar a ese valor extremo.

Los hackers, crackers están vigilando permanentemente las redes con el fin de encontrar las vulnerabilidades o debilidades de un sistema de información, el desarrollo del software ha permitido hacer cada vez más fácil la configuración y su utilización, Internet también permite la conectividad de todo tipo de usuario, de esta forma las amenazas a la seguridad de la Información están latentes y en cualquier momento un servidor o dispositivo de red puede ser atacado con fines negativos a la imagen de la Empresa o Institución, a su funcionalidad y otros aspectos

La información constituye uno de los recursos principales de una organización, por lo tanto se la debe proteger, mediante un conjunto de actividades, controles y políticas de seguridad que se deben implementar en base a recursos humanos, hardware y software.

La seguridad de la información depende de la gestión y los procedimientos adecuados, de los empleados de la organización, proveedores, clientes, accionistas y del nivel de seguridad de los medios técnicos.

LOS ACTIVOS DE UNA ORGANIZACION

Los activos asociados a los sistemas de información de una organización, se pueden clasificar de acuerdo a lo siguiente:

Recursos de información: Se consideran así a las bases de datos, manuales de usuario, procedimiento operativos o de soporte, planes de continuidad, información archivada, disposiciones de emergencia para la recuperación de información.

Software: Software de aplicaciones, Sistemas operativos, herramientas de desarrollo y utilitarios.

Equipos: Servidores, Computadoras, Routers, Switches, Hubs, PABX, equipos de energía, aire acondicionado, equipos de comunicaciones, etc.

Servicios: Servicios de comunicaciones, de procesamiento informático, energía eléctrica, iluminación, aire acondicionado.

La seguridad debe permitir proteger las siguientes características de la información:

Confidencialidad, es decir, que la información sea conocida únicamente por personas autorizadas.

Integridad, osea que su contenido no sea alterado a menos que sea modificado por personal autorizado

Disponibilidad, es decir, la capacidad de estar siempre disponible para ser procesado por personas autorizadas.

Control, ya que sólo las personas autorizadas pueden decidir cuando y cómo acceder a la información.

Autenticidad: La información es válida y utilizable y también que la fuente de la información es válida.

Protección al replay: la transacción sólo se realiza una vez, a menos que se especifique lo contrario.

No repudio: Para evitar que una entidad que recibió o envió información alegue que no lo hizo.

Las Intranet o redes internas deben ser protegidas, puesto que existen diversas amenazas. Se debe realizar una valoración de los activos y determinar su importancia así como el riesgo a la que están sometidos. Esta valoración deberá responder a los siguientes cuestionamientos:

¿Qué activos se deben proteger? ¿De qué amenazas debemos proteger? y ¿de qué manera lo protegeremos?

AMENAZAS A LA SEGURIDAD DE LA INFORMACIÓN

Entre las amenazas mas frecuentes se encuentran:

Catástrofes naturales: Este tipo de amenazas generalmente provocan la interrupción de los servicios, afectando principalmente a la disponibilidad de la información, ejemplos de este tipo de amenazas son los provocados por la naturaleza: las inundaciones, terremotos, tornados, etc.

Amenazas físicas: Relativo al acceso físico a los recursos, pueden resultar en robos, daños físicos a los equipos, sabotajes. El acceso no autorizado pero que se logra mediante la ingeniería social, explotando la confianza de los empleados de una organización.

Fraude Informático: Representados por el engaño a los clientes en la venta de productos y servicios a través de promociones y agencias que no existen.

Intrusiones: Osea el acceso no autorizado a los sistemas de comunicaciones, a los servidores de una organización, con el fin de dañar la imagen u obtener beneficios económicos indebidos.

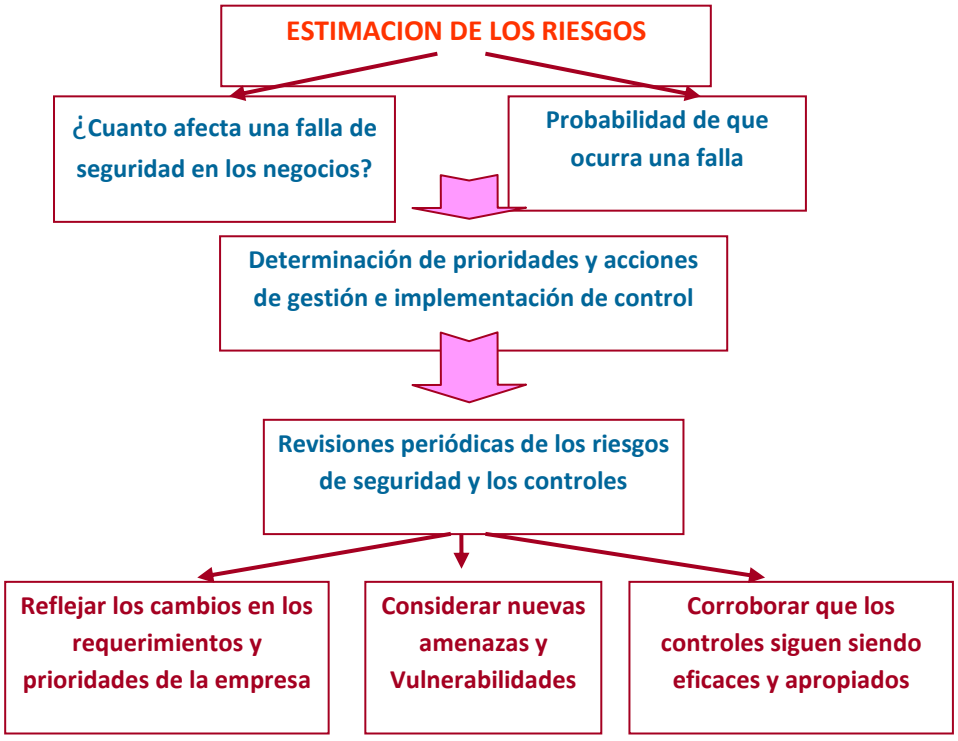
Errores humanos: Como su nombre lo indica resultan de la acción humana, como ser: passwords fácilmente vulnerables, backup de los sistemas mal hechos, interrupción de los servicios, configuraciones incompletas de los dispositivos.

Software ilegal: Las consecuencias de copiar software ilegal conducen a vulnerabilidades de los sistemas informáticos, ya que no se cuenta con las actualizaciones que los desarrolladores proporcionan, dentro del software ilegal se tienen también otras amenazas como los códigos maliciosos.

Código maliciosos: Es todo programa o parte de programa (software) que ocasiona problemas en los sistemas informáticos, como ser los virus, troyanos, gusanos, puertas traseras, cuando se activan en los sistemas finales. Este tipo de amenaza ha evolucionado por la conectividad cada vez mayor de Internet y por los recursos de engaño de los que se valen los atacantes.

Hemos indicado líneas arriba que es necesario estimar los riesgos a los que están sujetos la red, los servidores, los dispositivos de redes. Si bien, es difícil realizar una evaluación exacta de la información, se podría intentar evaluarla suponiendo su pérdida o alteración.

Una metodología de implementar un sistema de seguridad está expuesto en la figura siguiente:



POLITICAS DE SEGURIDAD.

La implementación de un sistema de seguridad debe estar complementado con las políticas de seguridad.

La política de seguridad requiere no solamente conocer las amenazas a las que están expuestas la información y los recursos de una organización, sino también establecer el origen de las mismas, que pueden ser internas o externas a la organización.

De nada valdría proteger la empresa de los usuarios del exterior si también existen amenazas internas. Por ejemplo, si un usuario utiliza un disquete que contiene un virus podría expandirlo a toda la intranet.

Una política de seguridad es "la declaración de las reglas que se deben respetar para acceder a la información y a los recursos". Los documentos de una política de

seguridad deben ser dinámicos es decir, ajustarse y mejorarse continuamente según los cambios que se presentan en los ambientes donde se crearon.

Las políticas de seguridad se desarrollan con el fin de preservar la información y los sistemas de una Empresa, y garantizando la integridad, confidencialidad y disponibilidad de la información. Los documentos relativos a las políticas de seguridad deben contemplar los procedimientos para hacer cumplir las reglas, las responsabilidades en todos los niveles. Todos ellos deben tener el apoyo gerencial de la organización.

Las políticas de seguridad deben ser conocidos por todo el personal de una organización.

En el contenido de los documentos deben estar claramente establecidos: El objetivo, los responsables del cumplimiento, las medidas que se aplicarán en caso de incumplimiento.

Entre los documentos pueden citarse los siguientes:

Administración de usuarios que reglamentará el acceso a los recursos por el personal de la organización.

Copias de respaldo: Describirá los pasos a seguir para asegurar una adecuada recuperación de la información, a través de las copias de respaldo.

Tratamiento de la información: Definirá claramente los tipos de información que es manejada por las personas autorizadas dentro de la organización.

Software legal: Definirá claramente el uso de software en la Empresa con licencias de uso legal.

Uso del servicio de Internet y del correo electrónico: Describirá la protección de la información mediante el uso de correo electrónico y del servicio de Internet.

Ambientes de Procesamiento: Define el uso de los ambientes de procesamiento de información.

Seguridad en las comunicaciones: Describirá la protección de la información durante los procesos de transmisión y recepción de datos en las redes internas y externas.

Auditorías de los sistemas: Que permitirá hacer un control de los eventos de seguridad de los sistemas.

Continuidad del procesamiento: Se definirán y reglamentarán las actividades relativas a la recuperación de la información en casos críticos mediante una metodología adecuada.

Protección física: Definirá la protección física de los equipos, de procesamiento, almacenamiento y transmisión de la información.

Sanciones por incumplimientos: Este documento contemplará las medidas que se aplicarán por incumplimiento de las reglas definidas.

CONCLUSION.

La información es un recurso de suma importancia para la Empresa u organización y se la debe proteger a través de la implementación de las medidas de seguridad basadas en hardware, software y recursos humanos, pero también complementadas con adecuadas políticas de seguridad que sean conocidas por el personal de la organización en todos sus niveles. El personal de la organización debe identificarse plenamente con los objetivos de seguridad y protección que busca la Empresa.

La seguridad de la información es tarea de todos: del personal de la Empresa, de los Socios, de los accionistas, de los clientes.