Sección 1: Importancia de la Seguridad Informática

Identificar la importancia de la información en las organizaciones, puntos a tener en cuenta, como afecta la perdida de la información y sus posibles consecuencias.

Contenido:

La seguridad informática son todas aquellas medidas donde se busca salvaguardar, proteger o resguardar la integridad de la información ya sea mediante medidas preventivas o correctivas, que permitan minimizar al máximo o completamente la pérdida de algún tipo de información para una persona o compañía.

La seguridad informática busca mantener la confidencialidad, integridad y disponibilidad de la información, es el estado donde su almacenamiento, procesamiento y comunicación se encuentra segura. La seguridad de la información también abarca el identificar las partes que interactúan entre ellas (emisor –receptor), entre usuarios o entre usuarios y sistemas de información, registrar las actividades de ser necesario, modificaciones, reemplazos y todo tipo de movimiento que se genera alrededor de ella y que sea susceptible de mantener una credibilidad y confianza que allí se encuentra.

Se deben mantener sistemas que permitan la autenticación, verificación, aprobación, autorización de la información, la no alteración de los datos y evitar la indisponibilidad o comunicación de la información o de los servicios.

En el contexto jurídico, la seguridad informática hace referencia a las obligaciones legales de implementar, mantener y mejorar continuamente los sistemas que permitan proteger y promover la eficiencia en la información, su procesamiento de acuerdo a sus derechos y libertades de los individuos.

La seguridad de la información no debe ser contemplada únicamente como un elemento para salvaguardar o para tomar medidas de protección de la información, se debe contemplar como un conjunto de acciones y de buenas prácticas que permitan administrar la información de una manera eficiente, sencilla, confiable y amigable con todos los actores que involucran la interacción con ella.

En la seguridad de la información se debe establecer infraestructuras y arquitecturas que sean amigables con las necesidades, los derechos humanos y las libertades de los individuos.

Se debe garantizar y proteger el derecho a la información, comunicación y acceso a los sistemas de información de los individuos, garantizando su privacidad, disponibilidad, confidencialidad e integridad.

Sección 2: Elementos de la seguridad informática, estándares y seguridad en redes

Mostrar los aspectos y elementos necesarios para prevenir la perdida de la información, estándares a seguir y medidas necesarias

Contenido:

Los elementos de la seguridad informática constituyen todas aquellas acciones, equipos e infraestructura que permiten interactuar con los sistemas informáticos y los usuarios, salvaguardando la integridad de toda aquella información o acción entre estos, evitando la posibilidad de que sea manipulada, robada o alterada.

Se debe tener en cuenta que esto no implica la protección total, ya que no es posible en la práctica, teniendo en cuenta la evolución de la tecnología y cuyo entorno se encuentra en constante cambio e interacción con diferentes actores que consultan, manipulan, extraen e ingresan información y en constante comunicación.

Con el paso del tiempo, los grupos encargados de los accesos, el control y la planificación de la recuperación de desastres, se ha convertido en un grupo de seguridad informática en las empresas y son los encargados de la protección de la información.

Por otro lado, se tiene los estándares que son las normas que se disponen donde se establecen los principios normativos en el uso de metodologías y buenas prácticas, para un uso eficaz, eficiente y aceptable de las tecnologías de la información con el objetivo de proteger la información de las compañías y usuarios que disponen de ellas.

Para este caso dividiremos en 2 partes, elementos de seguridad y estándares de seguridad:

- Elementos de seguridad: se darán algunos ejemplos y una breve descripción

• Firewalls: Son elementos de hardware o software que su principal función es controlar, limitar, cifrar o impedir el acceso no autorizado a cierta información, cumpliendo unas reglas o criterios específicos diseñados para tal fin.

- Análisis de riesgo: Consta de realizar un estudió o análisis que le permita identificar o saber cuales son sus principales vulnerabilidades o riesgos, permitiendo tomar medidas o realizar acciones con el fin de mitigar los posibles acontecimientos que invoquen en la perdida de algún tipo de información.

- Análisis de impacto al negocio: Es la implementación de medidas que permita restaura en el menor tiempo posible los sistemas de información de una compañía, en caso de que se sufra un ataque o perdida de información y así evitar pérdidas económicas, fallas en la prestación de servicios o el posible cierre se una empresa.

- Control de Virus y equipo de respuesta a amenazas: Implementación de programas de seguridad, que permitan minimizar el ataque o la propagación de software maligno o códigos que permitan la perdida se información, equipo de técnicos capacitados para dar repuesta y soporte en caso de sufrir ataques cibernéticos.

- Equipo de Respuesta a Emergencias TI (Computer Emergency Response Team - CERT): Equipo de técnicos capacitados para recibir incidentes de seguridad, analizar situaciones y dar respuesta en caso de amenazas.

- Equipo de investigación forense: Es un equipo de técnicos capacitados para adquirir, preservar obtener y presentar datos almacenados en medios informáticos, capaces de recuperar información, realizar peritajes y analizar evidencias en delitos informáticos.

- La administración de registros (logs): Es el registro de eventos en una compañía al acceder o procesar información, se debe realizar una auditoría a estos registros con el fin de analizar la información resultante y generar

- Cifrado: Algoritmo que permite transformar la información mediante una clave, no se puede interpretar la información si no se cuenta con ella.

- Políticas para el uso de: E-mail, correo de voz, Internet, video-mail: Como lo indica su mismo nombre, generar reglas o lineamientos en el uso de estas herramientas y del envío de información a través de ellas.

- Controles de espionaje industrial: Este es un tema difícil de controlar, pero se deben tener varias herramientas que permita minimizar los riesgos como por ejemplo cifrado de conexiones, controles de acceso, seguridad en los documentos, evitar el robo de identidad y mantener en cuidad los documentos físicos con información sensible para las compañías.

- Acuerdos de confidencialidad: Son contratos o acuerdos que se firman cuando se va a tratar información sensible para una organización y se requiere de discreción en el manejo de esta.

- Aspectos legales: Los aspectos legales son normas que se deben cumplir en el tratamiento de un tema específico para las cuales fueron creadas, por lo general están reguladas por entes públicos y aplican para las relaciones con terceros.

- Monitoreo de Internet: Permite conocer el tráfico de una red, identificar cuellos de botella y tomar acciones u obtener soluciones frente a problemas que resulten por el uso correcto o indebido de las herramientas informáticas.

- Planificación de desastres: Es la preparación, organización y adopción de planes para la atención de desastres, permitiendo mitigar las consecuencias que puedan llegar a ocurrir en eventos que no podamos controlar o que estén fuera de nuestro alcance, se deben generar programas y capacitar al personal involucrado de las organizaciones para dar una respuesta oportuna a cada caso.

- Planificación de continuidad de negocio: Es un plan logístico en donde una organización establece como se debe recuperar y restaurar sus funciones críticas, parcialmente o totalmente, dentro de un tiempo determinado después de la ocurrencia del evento que afectó su normal operación.

- Firmas digital: Es un algoritmo o mecanismo criptográfico que permite al receptor de un mensaje o documento, verificar la autenticidad y origen, permitiendo certificar que no ha sido modificado desde la salida de un autor.

- Inicio de sesión seguro: Es la pantalla que garantiza se está iniciando sesión correctamente digitando credenciales y contraseñas, evitando así introducir información en programas que imitan el inició de sesión en un equipo.

- Clasificación de la información: Se debe separar o clasificar la información, para de esta manera evitar que personal que no está involucrado con un proceso tenga acceso a áreas restringidas o que no están acordes a sus necesidades y puedan por descuido o negligencia alterar información de otras áreas.

- Administración de redes de área local: Es la persona o grupo de personas encargadas de la administración, gestión y seguridad de los equipos conectados a una red y de toda la red en conjunto, que permite dar soporte a fallas y actualizaciones necesarias para mantener la disponibilidad y seguridad de los servicios que viajan a través de ella.

- Control del uso de módems: Por lo general un modem es el dispositivo puerta de enlace que permite la conexión a redes externas desde y hacia las organizaciones, en algunos casos administra los usuarios que permite conectarse a la red y en otros contienen firewall o bloqueo de puertos y vpn, se debe disponer de un monitoreo y administración de estos recursos ya que son un puente importante entre las conexiones.

- Control de accesos remotos: El control de acceso remoto debe ser igualmente administrado por el personal de tecnologías de las organizaciones, con unos parámetros establecidos, monitoreados para controlar la información que se gestiona fuera de las organizaciones.

• Programas de concientización seguridad: Los programas de concientización de seguridad como su nombre lo indica es generar una serie de capacitaciones al personal de las organizaciones de la importancia de los sistemas de seguridad, la seguridad en contraseñas y los riesgos al compartir información susceptible, el uso de redes y el acceso a ellas.

- Estándares de seguridad: estos son algunos de los estándares más destacados:

• ISO 27001-2005: es un estándar Internacional donde se busca establecer, implementar, monitorear, operar, mantener, revisar y mejorar los SGSI de una organización, evalúa su riesgo, permite implementar controles para preservar la confidencialidad, integridad y disponibilidad de la información.

• ISO 27002: Estándar de buenas prácticas para los SGSI en una organización donde contiene recomendaciones para tomar medidas en la aseguración de la información y describe los aspectos a analizar para garantizar la seguridad, especifica controles y medidas para la información de las organizaciones.

• ISO 27005-2008: Imparte directrices para la gestión del riesgo de la seguridad de la información, para lo cual se debe tener previo conocimiento de los estándares anteriores con el fin que se pueda implementar en las organizaciones la intención de gestionar el riesgo en la información.