POLITICAS DE SEGURIDAD.

INTRODUCCIÓN Y ANTECEDENTES:

La seguridad informática consiste en asegurar que el sistema de información se mantenga de una manera correcta y se utilice de la manera que se decidió y controlar el acceso a la información restringiéndose a todo aquello que carezca de autorización.

Seguridad informática se fundamenta en tres principios.

- Integridad: que la información no se altere de forma no autorizada.
- Confidencialidad: requiere que la información sea accesible únicamente por las entidades autorizadas.
- Control de acceso: información únicamente accesible a personas autorizadas.
- Amenaza: la posibilidad de un intento deliberado y no autorizado de:
    a) Acceder a información.
    b) Manipular información.
    c) Convertir un sistema en no-confiable o inutilizable.

Debido a que el uso de Internet se encuentra en aumento, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información. Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información.

Riesgo: Exposición accidental e impredecible de información, o violación de la integridad de operaciones debido al malfuncionamiento de hardware o diseño incorrecto o incompleto de software.

Vulnerabilidad: una falla conocida o su sospecha tanto en hardware como en el diseño de software, o la operación de un sistema que se expone a la penetración de su información con exposición accidental.

Ataque: Una formulación especifica o ejecución de un plan para levar a cabo una amenaza.

Penetración: Un ataque exitoso; la habilidad de obtener acceso no-autorizado (indetectable) a archivos y programas o el control de un sistema computarizado."

OBJETIVOS.

Generalmente, los sistemas de información incluyen todos los datos de una compañía y también en el material y los recursos de software que permiten a una compañía almacenar y hacer circular estos datos. Los sistemas de información son fundamentales para las compañías y deben ser protegidos.

Generalmente, la seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

La seguridad informática se resume, por lo general, en cinco objetivos principales:

Integridad, que garantiza que los datos sean los que se supone que son;

Confidencialidad, que asegura que solo los individuos autorizados tengan acceso a los recursos que se intercambian; Disponibilidad, que garantiza el correcto funcionamiento de los sistemas de información; Evitar el rechazo, que garantiza de que no pueda negar una operación realizada; Autenticación, que asegura que solo los individuos autorizados tengan acceso a los recursos.

La seguridad informática tiene técnicas o herramientas llamados mecanismos para fortalecer la:

- Confidencialidad.
- Integridad.
- disponibilidad de un sistema informático.

CHECKLIST.

Directrices de la Dirección en seguridad de la información.

La seguridad de la información es el conjunto de medidas que ayudan a prevenir que la información no está expuesta al peligro, además es el valor más importante de las organizaciones, los sistemas tecnológicos permiten resguardar y proteger la información buscando mantener la seguridad de los datos ya que la información generada por una empresa pueden tener un alto valor económico para alcanzar el éxito de la organización.

- Política de seguridad
- Aspectos organizativos de la seguridad de la información
- Gestión de activos
- Seguridad ligada a los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Gestión de incidentes de seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

Aspectos negativos que ponen en riesgo a la información.

- Divulgación de la información.
- Mal uso.
- Robo de la información.
- Robar la información.

1. Conjunto de políticas para la seguridad de la información.

Política integral de seguridad.

La información que se gestiona mediante sistemas o redes, en el ámbito de la administración electrónica, básicamente se encuentra en tres estados:

- Transmisión.
- Almacenamiento.
- Proceso.

La política de seguridad debe garantizar las siguientes características fundamentales de la información:

- **Confidencialidad.** Seguridad de prevención frente a la disposición, la comunicación y la divulgación de información a terceros no autorizados
- **Integridad.** Seguridad de prevención ante la transformación o la modificación no autorizada durante su tratamiento o el almacenamiento de la información, con la exigencia de una rápida observación de alteraciones
- **Disponibilidad.** Seguridad de facilitar el acceso a la información por parte de quien esté autorizado y seguridad de prevención contra denegaciones a accesos autorizados
- **Autenticidad.** Seguridad frente a la identidad del productor o emisor de la información
- **Conservación.** Seguridad frente al deterioro de la información, mediante medidas preventivas y de preservación durante todo el ciclo de vida de los documentos
- **Trazabilidad.** Seguridad frente al conocimiento de operaciones, consultas o modificaciones de la información.

2. Revisión de las políticas para la seguridad de la información.

Principios relativos a la seguridad se podían resumir en nueve apartados, que son los siguientes:

1. **Concienciación.** Hay que adquirir conciencia de la necesidad de disponer de sistemas y redes de información seguros, al tiempo que conocer los medios para ampliar la seguridad.
2. **Responsabilidad.** Todos los actores implicados en la gestión de los documentos electrónicos son responsables de la seguridad de la información.
3. **Respuesta.** Hay que desarrollar actuaciones conjuntas y pertinentes para prevenir, detectar y responder a los incidentes que afecten a la seguridad.

4. **Ética.** Hay que contemplar los intereses legítimos de terceros.
5. **Democracia.** Hay que compatibilizar la seguridad y los valores esenciales de una sociedad democrática.
6. **Evaluación del riesgo.** Hay que llevar a cabo evaluaciones de riesgo.
7. Diseño y realización de la seguridad. Hay que incorporar la seguridad como un elemento esencial de los sistemas y redes de la información.
8. **Gestión de la seguridad.** Hay que adoptar una visión integral de la seguridad en la administración electrónica.
9. **Reevaluación.** Hay que revisar y reevaluar la seguridad de la información y realizar aquellas modificaciones pertinentes sobre políticas, prácticas, medidas y procedimientos relativos a la seguridad.

PUNTOS DE APLICACIÓN.

Necesidad de un enfoque global

Frecuentemente, la seguridad de los sistemas de información es objeto de metáforas. A menudo, se la compara con una cadena, afirmándose que el nivel de seguridad de un sistema es efectivo únicamente si el nivel de seguridad del eslabón más débil también lo es. De la misma forma, una puerta blindada no sirve para proteger un edificio si se dejan las ventanas completamente abiertas.

Esto significa que el tema de la seguridad debe ser abordado a nivel global y debe tomar en cuenta los siguientes aspectos:

- La sensibilización de los usuarios a los problemas de seguridad.
- La seguridad lógica, es decir, la seguridad a nivel de los datos, en especial los datos de la empresa, las aplicaciones e incluso los sistemas operativos de las compañías.
- La seguridad en las telecomunicaciones: tecnologías de red, servidores de compañías, redes de acceso, etc.
- La seguridad física, o la seguridad de infraestructuras materiales: asegurar las instalaciones, los lugares abiertos al público, las áreas comunes de la compañía, las estaciones de trabajo de los empleados, etc.

Cómo implementar una política de seguridad.

Generalmente, la seguridad de los sistemas informáticos se concentra en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autentificación y control que aseguran que los usuarios de estos recursos solo posean los derechos que se les han otorgado. Los mecanismos de seguridad pueden sin embargo causar inconvenientes a los usuarios.

Las causas de inseguridad.

Generalmente, la inseguridad se puede dividir en dos categorías: un estado de inseguridad activo, es decir, la falta de conocimiento del usuario sobre las funciones del sistema, algunas de las cuales pueden resultar perjudiciales para el sistema (por ejemplo, no desactivar los servicios de red que el usuario no necesita); un estado de inseguridad pasivo, es decir, la falta de conocimiento de las medidas de seguridad disponibles.

INFORMACIÓN Y ELEMENTOS ADICIONAL.

- ESPAÑA. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Boletín Oficial de Estado [en línea], 29 de enero de 2010, 25. [Consulta: 15 diciembre 2014].
- INTERNATIONAL ORGANIZATION FOR STANDARIZATION (ISO). 2013. ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. Ginebra: ISO.
- INTERNATIONAL ORGANIZATION FOR STANDARIZATION (ISO). 2013. ISO/IEC 27002:2013. Information technology - Security techniques - Code of practice for information security controls. Ginebra: ISO.