MÓDULO 10 SEGURIDAD DE LA INFORMACIÓN	
01.- *Módulo Seguridad de la Información*	**02.- FECHA:** 23-septiembre-2022

03.- INTRODUCCIÓN:

El oficial de protección de hoy debe trabajar en un ambiente de desarrollo tecnológico, cuando se trata de protección informática, actualmente las personas responsables de protección se enfrentan a un trabajo adicional de asesoramiento en prevención de potenciales amenazas, donde las recomendaciones son esenciales.

Seguridad de la información

La seguridad de la información es el conjunto de medidas y técnicas utilizadas para controlar y salvaguardar todos los datos que **se manejan dentro de la organización y asegurar que los datos no salgan del sistema** que ha establecido la organización.

04.- DESARROLLO:

Encontramos estos objetivos de la seguridad de la información en la norma ISO 27001. La norma establece un modelo para la **implementación de sistemas de gestión de seguridad de la información**. El principal fin que persigue la norma ISO 27001 es la protección de los activos de información, es decir, equipos, usuarios e información.
Se establece este sistema ISO de seguridad de la información hay que tener en cuenta tres aspectos fundamentales:

- Integridad
- Confidencialidad
- Disponibilidad

Seguridad en Informática (Confidencialidad, Integridad y Disponibilidad)
https://www.youtube.com/watch?v=-WsO5BLAxSI

Integridad

Los sistemas que gestionan la información tendrán que garantizar la integridad de la misma, es decir, que la información se muestra tal y como fue concebida, sin alteraciones o manipulaciones que no hayan sido autorizadas de forma expresa. El objetivo principal es garantizar la transmisión de los datos en un entorno seguro, utilizando protocolos seguros y técnicas para evitar posibles riesgos.

Confidencialidad
La confidencialidad garantiza que solo las personas o entidades autorizadas tendrán acceso a la información y datos recopilados y que estos no se divulgarán sin el permiso de forma correspondiente. Los sistemas de seguridad de la información tendrán que garantizar que la confidencialidad de la misma no se ve comprometida en ningún momento.

Disponibilidad
En este aspecto se garantiza la información que se encuentra disponible en todo momento para todas las personas o entidades autorizadas para su manejo y conocimiento. Para esto deberán existir medidas de soporte y seguridad que se puedan acceder a la información cuando resulte necesario y que evite que se establezcan interrupciones en los servicios.

Vulnerabilidad, Amenazas y Contramedidas.

Hay tres conceptos que entran en discusión cuando hablamos de la amenaza a un sistema informático: peligro (threat), vulnerabilidad o factor de riesgo (vulnerability) y contramedidas (countermeasures).
Vulnerabilidad. - Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la protección del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.
Amenaza. - Posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya) o un suceso natural o de otra índole (fuego, inundación, entre otros). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.
Contramedida. - Técnicas de protección del sistema contra las amenazas.

Tipo de vulnerabilidad

La defensa es realmente la capacidad de estar a salvo de algún riesgo o amenaza. Desde este punto de vista, la protección integral es difícil de lograr porque significa describir todos los riesgos y amenazas a los que se puede enfrentar el sistema. No podemos hablar de un sistema informático completamente seguro, sino de uno en el que no se conocen tipos de ataque que puedan dañarlo, porque se han tomado medidas contra ellos.

Algunos tipos de vulnerabilidades del sistema incluyen:

vulnerabilidad física.
Está al nivel del entorno físico de un edificio o sistema. Implica la capacidad de penetrar o acceder físicamente a

un sistema para robarlo, modificarlo o destruirlo.

Naturalmente frágil.
Se refiere al grado en que un sistema se ve afectado por peligros naturales o ambientales que pueden dañar el sistema, como incendios, inundaciones, rayos, terremotos o, más comúnmente, una falla de energía o una sobrecarga de energía.

Vulnerabilidades de hardware y software.
Desde una perspectiva de hardware, algunos tipos de dispositivos pueden ser más vulnerables que otros. Por lo tanto, algunos sistemas requieren una herramienta o tarjeta para acceder a ellos.

Vulnerabilidad de medios o equipos.

Esto se refiere a la posibilidad de robo o daño de discos, cintas, tiras de impresora, etc.

Vulnerabilidad de la comunicación.
La conexión de computadoras a redes es, sin duda, un aumento importante en la vulnerabilidad del sistema. Al aumentar el número de personas que pueden estar expuestas o intentar contactarlo, aumenta mucho el riesgo al que está expuesto.
También existe el riesgo de interceptación de las comunicaciones:

- Se puede penetrar al sistema a través de la red.
- Interceptar información que es transmitida desde o hacia el sistema.

Tipo de amenaza

Las amenazas a los sistemas informáticos también se pueden clasificar desde diferentes perspectivas.

Según el origen de la amenaza, se puede dividir en: natural, forzada e intencional.

Peligros naturales o físicos.
Comprometen los componentes físicos del sistema. Entre ellos, por un lado, se pueden distinguir los desastres naturales (por ejemplo, inundaciones, rayos o terremotos) y las condiciones ambientales (por ejemplo, temperatura, humedad, presencia de polvo).

Una de las amenazas más comunes es el usuario sentado frente a la computadora con una lata de refresco en la mano y un sándwich cerca del teclado o la unidad central.

Amenazas no planificadas.
Estos se deben al uso descuidado del equipo debido a la falta de capacitación o conciencia de protección. Entre los más comunes podemos mencionar:
• Parte de la información se eliminó accidentalmente.
• Deje ciertos archivos críticos del sistema vulnerables.
• Dejar un post-it con nuestra contraseña pegado en la pantalla u olvidarse de cerrar la sesión.

Amenazas intencionales.
Estos son de personas que deliberadamente acceden al sistema para borrar, cambiar o robar información, bloquearla o simplemente por diversión.
Las causas del daño pueden ser de dos tipos: internas y externas.
El exterior puede ingresar al sistema de varias maneras:
• Entrar a un edificio o acceder físicamente a una computadora.
• Explotación de vulnerabilidades de software para obtener acceso a sistemas en una red.

• Acceso por parte de quien lo posea de forma autorizada.

Hay tres tipos de personas con información privilegiada: empleados despedidos o descontentos, empleados coaccionados y empleados que se benefician personalmente.

TIPOS DE MEDIDAS DE PROTECCIÓN O CONTRAMEDIDAS

Los sistemas informáticos pueden diseñarse de acuerdo con criterios de economía, de eficiencia y de eficacia, entre otros, porque son claramente medibles y se asocian a parámetros que, maximizando unos y minimizando otros se puede tender hacia diseños óptimos.

Las medidas de protección que pueden establecerse en un sistema informático son de cuatro tipos fundamentales: lógicas, físicas, administrativas y legales. Vamos a verlas con más detalle.

Medidas físicas

Aplican mecanismos para impedir el acceso directo o físico no autorizado al sistema. También lo protegen de desastres naturales o condiciones medioambientales adversas. Se trata fundamentalmente de establecer un perímetro de protección en nuestro sistema.

Existen tres factores fundamentales a considerar:

- El acceso físico al sistema por parte de personas no autorizadas.
- Los daños físicos por parte de agentes nocivos o contingencias.
- Las medidas de recuperación en caso de fallo.

Medidas lógicas

Incluye las medidas de acceso a los recursos, a la información y al uso correcto de los mismos, así como a la distribución de las responsabilidades entre los usuarios. Se refiere más a la protección de la información almacenada.

Dentro de las medidas lógicas se incluyen también aquellas relativas a las personas y que podríamos denominar medidas humanas. Se trata de definir las funciones, relaciones y responsabilidades de distintos usuarios potenciales del sistema. Se trataría entonces de responder a preguntas tales como:

- ¿A quién se le permite el acceso y uso de los recursos?
- ¿Qué recursos puede acceder cada usuario y qué uso puede hacer de ellos?
- ¿Cuáles son las funciones del administrador del sistema y del administrador de la protección?
- ¿Cuáles son los derechos y responsabilidades de cada usuario?

A la hora de responder a las preguntas anteriores hemos de diferenciar cuatro tipos fundamentales de usuarios. A cada tipo se le aplicará una política de control de accesos distinta y se le imputaran distinto grado de responsabilidades sobre el sistema:

- El administrador del sistema y en su caso el administrador de la protección.
- Los usuarios del sistema.
- Las personas relacionadas con el sistema, pero sin necesidad de usarlo.
- Las personas ajenas al sistema.

GRUNSEG CIA.LTDA