-

**SGSI**

**Nombre: Santiago Andres del valle pinilla**

**ID: 000427744**

*Sistema de gestión de la seguridad de la información*

*(en inglés: information security management system, ISMS)*

*Identificación de amenazas, vulnerabilidades y activos afectados por parte del oficial de seguridad informática.*

Perfil del oficial de seguridad informática:

<http://www.cudi.edu.mx/rfc/drafts/draft4.pdf>

<http://recpr.org/support/assets/funciones-y-responsabilidades-del-oficial-de-privacidad.pdf>

## **Vulnerabilidad**

Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

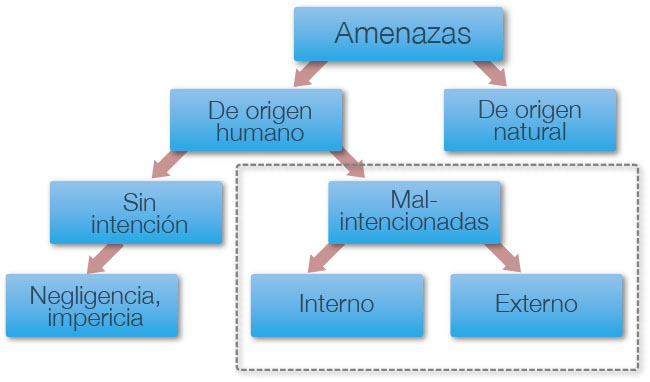
Como ejemplo de vulnerabilidad podemos comentar el siguiente. En su casa hay una computadora conectada a Internet, dónde además tiene configurada una cuenta de correo electrónico a través de la que recibe mensajes diariamente. También tiene instalado un antivirus que es capaz de chequear los mensajes electrónicos, incluidos los archivos que están adjuntos. Pero el antivirus lo instalo cuándo compró el equipo hace más de un año y no lo ha vuelto a actualizar. En este caso su equipo es vulnerable a los virus más recientes que puedan llegar mediante su correo electrónico, ya que el antivirus no está actualizado y no sabe que éstos nuevos virus existen.

Pero una cosa sí que es cierta, que exista una vulnerabilidad no significa que se produzca un daño en el equipo de forma automática. Es decir, la computadora tiene un punto flaco, pero no por eso va a fallar, lo único que ocurre es que es posible que alguien ataque el equipo aprovechando ese punto débil.

## **Amenaza**

Una amenaza a un sistema informático es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

Como ejemplos de amenaza están las personas que cometen ataques, al igual que los desastres naturales que puedan afectar a las computadoras y al sistema informático en general. También se pueden considerar amenazas los fallos cometidos por los usuarios al utilizar el sistema, o los fallos internos tanto del hardware o cómo del software.

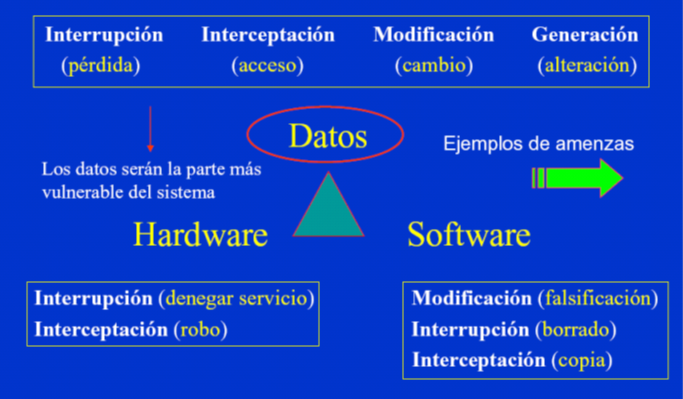


Disponible en <http://www.magazcitum.com.mx/?p=2193#.V7TT5ph9600>

## **Tipos de amenazas en los Sistemas Informáticos**

Podemos agrupar en cuatro tipos generales las amenazas a los sistemas informáticos:

1. **De interrupción**: Este se considera un ataque a la **disponibilidad**. Un recurso del sistema es destruido o deja de estar disponible.
2. **De intercepción**: Este es un ataque contra la **confidencialidad**. Una entidad no autorizada consigue acceso a un recurso, un ejemplo es la escucha de una línea para interceptar la información privada que fluye por la misma.
3. **De modificación**: Es un ataque contra la **integridad**. Una entidad no autorizada no solo consigue acceder a un recurso, sino que es capaz de modificarlo.
4. **De fabricación/generación**: Se produce cuando una entidad no autorizada inserta objetos falsificados en el sistema. Se considera un ataque contra el ‘**no repudio**‘



Completa el siguiente cuadro y comparte con los compañeros:

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerabilidad | Amenaza | Amenaza se debe a: interrupción, modificación, interceptación, generación | Activo que se ve afectado de materializarse la amenaza |
| Banda de ancha pobre / Saturación de la red | Lentitud en la transmisión de información a través de la red de datos de la empresa | Interrupción | Red de datos en la empresa |
| No actualizar los drivers ni revisar los procesos “zombies” | Continuos fallos en el del sistema operativo que obligan a reiniciar la máquina. | Interrupción | Sistema operativo y aplicaciones (A grandes rasgos el computador/servidor) |
| Falta de seguridad / cifrado en la red de la empresa. | Extracción de información a través de escucha no autorizada de la red inalámbrica de la organización. | Intercepción | Información confidencial comprometida |
| Pobre/inexistente designación de roles de acceso | Borrado intencional de datos de la base de datos de la empresa. | Interrupción | Información de la empresa |
| Falta de control/restricción respecto a los puertos “usb” de la entidad | Copia ilícita de un programa de contabilidad comprado a un tercero. | Fabricación | Imagen de la empresa además de problemas legales |
| la falta de controles de acceso físico adecuados. | Sustracción y cambio de elementos del hw de la empresa por unos de menor calidad. | Modificación | Integridad de los datos |
| Pobre/inexistente designación de roles de acceso.  Falta de política de manejo de “IPS” por parte de la entidad.  Problemas con la lógica del programa (SQL injection) | Añadir registros a la base de datos de clientes y proveedores sin permiso del DBA. | Fabricación | Integridad de los datos |
| la falta de controles de acceso físico adecuados. | Empleado que trae archivos infectados de su casa y los pasa al PC de la oficina. | Fabricación | Información confidencial de la entidad además del riesgo de acceso por terceros. |
| Falta de seguridad / cifrado en la red de la empresa.  Políticas nulas de acceso virtual (Roles) | Interceptación de documentos sensibles respecto a los empleados. | Intercepción | Buen nombre |
| Falta de políticas de privacidad / acceso remoto y físico | Un empleado de Tesorería no cierra sesión cada vez que se levanta de su puesto de trabajo, permanece logueado en el sw de gestión de la empresa. | Interrupción | Software de gestión de la empresa |
| No hay extintores en ninguna de las dependencias de la organización. | Riesgo de incendio el cual no se pueda parar a tiempo | Interrupción | Elementos físicos de la entidad |
| No hay ningún control de acceso al cuarto de servidores | Modificación / Inserción / eliminación / extracción de datos de la entidad. | Interrupción  Intercepción  Fabricación  Modificación | Integridad, confidencialidad, acceso de los datos |
| Los backups de la base de datos del sistema de gestión y control de la empresa no están actualizados. | Perdida de la información mas actual en relación al restablecimiento de la base de datos. | Interrupción | Falta de la información más actual. |
| Las cintas y discos con el backup diferencial de la organización se almacenan en la oficina del ingeniero de sistemas, contigua al cuarto de servidores. | Perdida de información total en caso de un fallo natural. | Interrupción | Perdida total de la información. |
| Existe un wi fi de exteriores de acceso público para visitantes y empleados de la empresa. | Robo de información personal de los empleados el cual podría comprometer a la empresa. | Interceptación | Robo de credenciales e información sensible. |