**II\_15\_AMENAZAS\_INFORMÁTICAS**

La **seguridad informática, o ciberseguridad**, es una **disciplina** que se encarga de proteger la integridad y la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático. La idea principal es que se pueda evaluar la seguridad de los sistemas de cómputo y redes para, posteriormente, protegerlos de los ataque informáticos que se pueden llevar a cabo a los sistemas.

A lo largo de la historia, esta seguridad se ha ido transformando, gracias a los controles y auditorías sobre los sistemas, explotando las vulnerabilidades que se puedan encontrar en los mismos. Se han implementado medidas de seguridad física y lógicas en conjunto con la seguridad en Internet.

**TIPOS DE AMENAZAS INFORMÁTICAS**

**Software maligno: malware Malicious Software**. Tienen como objetivo dañar un sistema de información sin la autorización del usuario.

Malware: virus, troyanos,

**VIRUS:** componente de software copiándose a si mismo en distintos archivos. El objetivo puede variar, pero en esencia es destruir o inhabilitar archivos o programas que tena nuestro dispositivo. No pueden afectar a otros dispositivos a menos que los pasemos a través de un hardware. Se pegan a los archivos por lo general ejecutables.

**GUSANO:** se copia a sí mismo en el sistema y **utiliza la red** para copiarse a otras máquinas. Tiene mayor capacidad de infección. El objetivo es replicarse hasta saturar el funcionamiento del sistema.

**Para solucionarlo**: apagar toda la red y pasar el antivirus por cada pc.

**TROYANOS:** No causan daño en sí mismos, pero tienen una estructura para cargar dentro virus, gusanos y demás malwares. Por lo general vienen en los programas sin licencias y cracks. Requieren de la ejecución del usuario, ya que no pueden replicarse a si mismos.

También pueden crear backdoors que es como una puerta trasera para que el dispositivo pueda ser controlado de manera remota por otro usuario. También pueden utilizarlo como un servidor proxy para ocultar ataques. O lo más común, para introducir spam a nuestro equipo.

**ADWARES:** similar a los troyanos, cuyo objetivo es bombardear el dispositivo con publicidad pero mucho más frecuente. No son dañinos y por lo gral vienen dentro de troyanos.

Los MALWARE siempre buscan robar nuestros datos.

**SPYWARES**: O software espía, no daña el dispositivo pero roba información de contraseñas, información bancaria, puede acceder a la cámara del dispositivo, etc.

Por lo general los MALWARE atacan el SO y cuando este se reinstala desaparecen.

**ROOTKITS**: conjunto de softwares, van dirigidos al firmware del sistema o los programas de usuario y tienen acceso al dispositivo en modo sistema o kernel. Por lo que pueden realizar modificaciones en los procesos internos del SO, a los archivos del sistema e incluso a las cuentas de usuario. Estos logran esconderse de los antivirus.

Para solucionarlo: hay q resetear la BIOS a valores de fábrica. La info se puede guardar en otros discos duros.

**BOTNETS: BOT=ROBOT NET=RED** red de robots que es puesto por un atacante para controlar a todas las computadoras al mismo tiempo. Por lo gral se utilizan para cometer crímernes digitales = crimeware como robos de identidad, chantajes, entre otros. También vienen dentro de Troyanos.

Todos los anteriores suelen permanecer ocultos para el usuario.

**RANSOMWARE:** o software de secuestro, suelen utilizarse contra empresas para pedir rescate. Se pueden encontrar en archivos adjuntos de correos no deseados.

Hay q hacer acciones preventivas para no perderla info si nos entra un ransomware.

**PROTECCIÓN DE LA INFORMACIÓN**

La información es recurso clave para tomar decisiones, dimensionar cosas, y disminuir riesgos. La misma cuenta con tres dimensiones conocidas como: integridad, disponibilidad y confidencialidad, también llamadas CIA por sus siglas en inglés. Los atacantes de un sistema van a tratar de vulnerar algunas de esas dimensiones.

**Integridad**: Consiste en que la información se encuentre completa, entera y que los datos que están dentro del sistema sean los que deberían ser. Un ejemplo de esta dimensión sería el ataque a una base de datos y la modificación de los datos que hay en la misma, con lo cual podemos seguir viendo la información, pero la misma es errónea debido a que la original fue alterada.

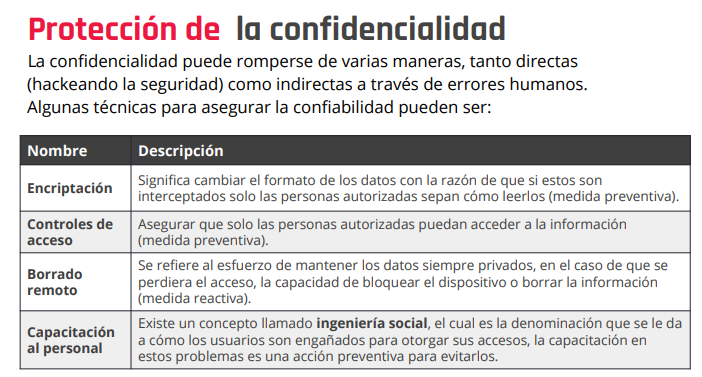
**Disponibilidad:** Significa que la información una persona/usuario debe poder tener acceso a la información en el momento que lo necesita, es decir, en tiempo y forma. Un típico ataque a este tipo de dimensión es el ataque de denegación de servicio.

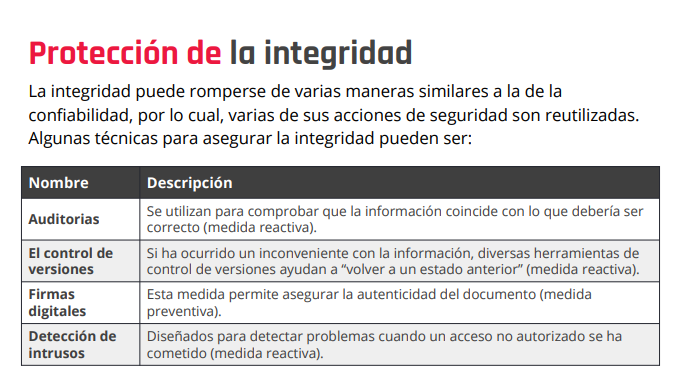
**Confidencialidad:** Refiere a que la información tiene que estar disponible únicamente para las personas que tienen acceso a esta información y bloqueada para el acceso a terceros. Por ejemplo, los datos personales e historiales médicos.

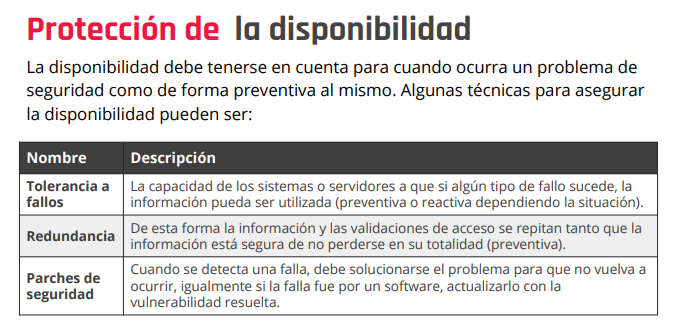
La protección de la información se basa en garantizar el completo y total funcionamiento de las 3 dimensiones, para ello, debemos implementar medidas preventivas y reactivas.

Medidas preventivas se refiere a todas las acciones que pueden tomarse para evitar problemas no deseados. Por otro lado, las medidas reactivas son aquellas donde ya se ocasionó un problema de seguridad y hay que solventarlo.

**Protección de la confidencialidad** La confidencialidad puede romperse de varias maneras, tanto directas (hackeando la seguridad) como indirectas a través de errores humanos. Algunas técnicas para asegurar la confiabilidad pueden ser:





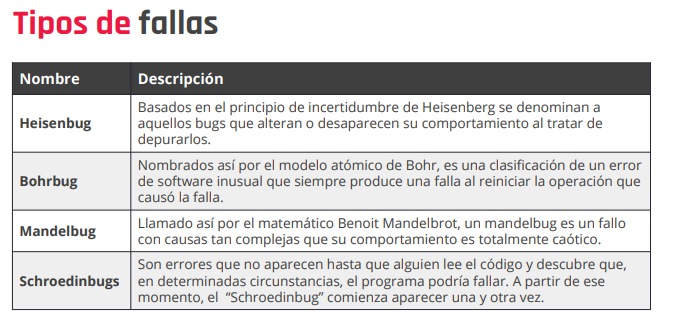


**FALLAS Y VULNERABILIDADES**

Una **falla**, también conocida como bug, es un **error en un programa o sistema operativo que desencadena un resultado indeseado**.

El término bug viene desde 1947 cuando Grace Hopper, mientras estaba programando el Mark II, descubrió que un insecto (bug) había provocado un error en uno de sus relés electromagnéticos.

En el desarrollo del software existen muchos tipos de fallas, pero en general se pudieron establecer unos tipos generales de bugs según su comportamiento.



Una **vulnerabilidad** es una **debilidad o fallo de un sistema informático** que **puede poner en riesgo la integridad, confidencialidad o disponibilidad de la información**.

La evaluación o detección de vulnerabilidades permite reconocer, clasificar y caracterizar los agujeros de seguridad.

**Pasos para detectar una vulnerabilidad**

Si bien no existe un método único para detectar vulnerabilidades, es posible armar una serie de ítems a tener en cuenta para considerar nuestra información segura.

● Evaluar cómo está constituida la red e infraestructura de la empresa.

● Delimitar quién puede y debe acceder a la información confidencial.

● Probar que las copias de seguridad realizadas funcionen.

● Identificar las partes más sensibles y esenciales del sistema.

● Realizar auditorías del estado de la seguridad informática.

Quiz

[1](https://playground.digitalhouse.com/)

**[Un software maligno también se lo conoce como \_\_\_\_\_](https://playground.digitalhouse.com/)**

Malware

**Corrección**  ¡Muy bien! El malware, también conocido como malicious software, tiene por objetivo infiltrarse o dañar un sistema de información.

[2](https://playground.digitalhouse.com/)

**[¿Cuál es la diferencia entre virus y troyano?](https://playground.digitalhouse.com/)**

El virus es un componente de software que se copia a sí mismo en varios lugares, mientras que el troyano es un programa sin licencia que necesita de la ejecución del usuario.

**Corrección**  ¡Muy bien!

[3](https://playground.digitalhouse.com/)

**[Los spywares dañan los dispositivos.](https://playground.digitalhouse.com/)**

Falso.

**Corrección**  ¡Muy bien! Los spywares permanecen ocultos para robar información.

[4](https://playground.digitalhouse.com/)

**[¿En qué se diferencian los rootkits de las demás amenazas?](https://playground.digitalhouse.com/)**

Los rootkits logran esconderse de los softwares antimalware o antivirus.

**Corrección**  ¡Muy bien!

[5](https://playground.digitalhouse.com/)

**[¿Cuáles son los aspectos de la información que se deben proteger para evitar ataques?](https://playground.digitalhouse.com/)**

Confidencialidad, integridad y disponibilidad.