Seguridad informática

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 seguridad informática únicamente se va a centrar en el medio de comunicación por el cual va a viajar la información. Va a identificar, eliminar vulnerabilidades y proteger de ataques maliciosos a los equipos de cómputo, servidores, redes informáticas y todo aquel medio informático por el cual se transmita información.

Malwares

Ataques informáticos que tienen como objetivo infiltrarse y dañar un sistema de información y sin el consentimiento del usuario, debe estar oculto.

Tipos de malwares:

- **VIRUS**: Componente de software cuyo objetivo es permanecer en un sistema, copiándose a sí mismo en varios lugares desde el momento que se ejecuta en el sistema.
- **GUSANO**: Se copia a sí mismo en el dispositivo y se copia en otros a través de la red, aprovechando las vulnerabilidades de la red y agujeros de seguridad.
- **TROYANO**: No causan daño en sí mismo, son estructuras que se usan para ocultar otros malwares.
- **SPYWARES**: Software espía. No daña el dispositivo pero roba toda la información del sistema.
- **ROOTKITS**: Conjunto de softwares. A diferencia de los demás malwares, que atacan el sistema operativo (y si se reinstala el SO se elimina el malware), los rootkits van directo al firewall del sistema o a los programas de usuario y tienen acceso al dispositivo en modo sistema o kernel.
- **BOTNETS**: Es una mezcla entre Bot (robot) y Net (red). Es una red de robots que es puesto por un atacante en una red de computadoras para ser controladas todas al mismo tiempo.
- **RANSOMEWARE**: A diferencia de los malwares anteriores que permanecen ocultos al usuario, el Software de Secuestro suele ser usado en contra se empresas para acceder a productos y servicios y luego pedir rescate.

Principios de la seguridad de la información

INFORMACION: Es recurso clave para tomar decisiones, dimensionar cosas, y disminuir riesgos.

Tiene tres dimensiones (CIA por sus siglas en inglés):

- **Integridad**: que la información se encuentre completa, entera y que los datos que están dentro del sistema sean los que deberían ser. Ejemplo: Ataque a una base de datos y modificación de datos (sigo viendo la info pero es incorrecta)

- **Disponibilidad**: una persona/usuario debe poder tener acceso a la información en el momento que lo necesita. Ejemplo: denegación del servicio

- **Confidencialidad**: la info debe estar disponible para quienes tienen acceso y bloqueada para terceros. Ejemplo: datos personales e historiales médicos

Los atacantes de un sistema van a tratar de vulnerar algunas de esas dimensiones.

Fallas y vulnerabilidades

FALLA: también conocida como bug, es un error en un programa o sistema operativo que desencadena un resultado indeseado.

VULNERABILIDAD: Es una debilidad o fallo de un sistema informático que puede poner en riesgo la integridad, confidencialidad o disponibilidad de la información.