**SEGURIDAD INFORMÁTICA**

Es la 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.

**Ciberseguridad**

Esta se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma,como la información que se transmite a través de las redes de computadoras. Para minimizar todos los riesgos a la infraestructura y a la información se han creado múltiples métodos, como estándares, protocolos, reglas, herramientas y leyes informáticas.

Debemos tener en cuenta que la seguridad informática únicamente se va a centrar en el medio de comunicación por el cual va a viajar la información.

**Amenazas**

Malware: Software maligno que tiene como objetivo infiltrarse o dañar un sistema de información sin el consentimiento del usuario. Necesita estar oculto para que el usuario no lo elimine. Existen distintos tipos de malware:

* Virus: este busca permanecer en el sistema copiando a sí mismo en varios lugares desde el momento en que se ejecuta en el sistema, así cuando se elimine un archivo el virus seguirá existiendo en otras partes del sistema. Son de poca infección, no tienen la capacidad por sí mismos de afectar otros dispositivos a menos que se pasen por hardware (pendrive).
* Gusano: se copia a sí mismo en sistema y utiliza la red para copiarse a otras máquinas a través de vulnerabilidades o agujeros en la seguridad. Por lo que posee mayor capacidad de infección. Su objetivo es saturar el funcionamiento del sistema.
* Troyanos:su estructura es usada para cargar malwares ocultos. Usualmente programas sin licencia y cracks. Requiere de la ejecución del usuario porque no puede multiplicarse solo.

**Principios de la seguridad de la información**

Información: 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.

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

**Fallas Vs 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.