**Seguridad Informática**

**SEGURIDAD ACTIVA**

Esta protege y evita daños en los sistemas informáticos

Elementos activos: dentro de estos elementos podemos encontrar servidores, dispositivos móviles, bases de datos, entre otros. Estos contienen información que alguien quiere vulnerar, obtener, destruir, etcétera.

**SEGURIDAD PASIVA**

Este es el conjunto de acciones o técnicas de seguridad que entran en acción para minimizar los daños a los sistemas informáticos. Se activan cuando se ha introducido un malware o cualquier otra amenaza en los sistemas

**MEDIOS DE PROTECCIÓN**

La seguridad informática sea integral sobre los equipos y software informáticos se deben implementar también algunos controles de tipo administrativo y físicos.

**AUDITORÍAS**

Esta es la acción de analizar de manera exhaustiva y profunda las distintas características y áreas de una organización. El auditor es el encargado de analizar y determinar que toda la informática de la organización trabaje de manera eficiente.

**SEGURIDAD FÍSICA**

Este es el establecimiento de técnicas que permiten resguardar de cualquier tipo de daños a los equipos en los cuales se almacena los activos de una organización, sus datos.

**SEGURIDAD LÓGICA**

Esta está conformada por un conjunto de procesos que se encargan de garantizar la seguridad de los datos y sistemas, además controlan el acceso a los mismos.

**HACKER**

Esta persona que hackea cualquier tipo de sistema para descubrir sus vulnerabilidades con el objetivo de poder encontrar alguna herramienta que la minimice o suprima —en el caso de un white hat— o utilizar esta vulnerabilidad a su favor —en el caso de un black hat— y esto lo logra en base a su conocimiento.