Seguridad activa y pasiva:

**Seguridad activa:** Protege y evita daños en los sistemas informáticos, tales como servidores, dispositivos móviles, bases de datos, etc.

Buenas prácticas:

-Uso adecuado de contraseñas.

-Uso de software de seguridad informática.

-Encriptación de datos importantes.

**Seguridad pasiva:** Es un conjunto de acciones que minimizan los daños a los sistemas informáticos. Éstas actúan cuando ya se ha introducido un malware u otra amenaza en el sistema.

Buenas prácticas:

-Realizar copias de seguridad.

-Escanear y limpiar continuamente los dispositivos.

-Crear particiones en el disco duro y backups en una unidad distinta de nuestro sistema operativo.

-Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.

-Comprobar el que el antivirus funciones correctamente.

Medidas de protección

Se clasifican en dos grupos:

ACTIVAS:

-Directivas: Nos dicen qué podemos hacer y qué no. Intentan que las actividades de los sistemas se realicen de una manera específica con el fin de que se produzcan ciertos resultados esperados.

-Disuasivas: Desvían la atención del atacante. A diferencia de la anterior, ésta no impide la acción dañina sino que nos da una advertencia del riesgo que podría causar la misma.

-Preventivas: Buscan que no se produzca un accidente o cualquier tipo de acción indebida en los sistemas. La diferencia con las disuasivas es que estas buscan informar y prevenir una acción indebida.

PASIVAS:

-Detectivas: Se basan en buscar potenciales ataques en sistemas informáticos.

-Correctivas: Se activan una vez que el sistema ya corre riesgo, o cuando los datos o información se encuentran en peligro. Su objetivo es solucionar esta situación.

Seguridad física y seguridad lógica

**Seguridad física:**

-Dispositivos físicos de protección: Pararrayos, extintores, detectores de humo, alarma contra intrusos, entre otros.

-UPS (Uninterruptable Power Supply): Es un dispositivo electrónico que almacena energía por medio de una batería interna. Esto le permite a los dispositivos que están conectados al mismo, frente a un apagón eléctrico, seguir almacenando la información por un determinado tiempo.

-Respaldo de datos: Es importante saber que los datos son los activos más importantes dentro de una organización, por tal motivo, es de suma importancia el manejo y cuidado de los mismos ya que pueden estar expuestos a muchos factores como hurto, alteración, virus, entre otros. Por tal motivo, se deben realizar copias de seguridad o backups de los datos completos e incrementales. El backup es un proceso por el cual se realiza la copia de los datos originales con el fin de prevenir cualquier tipo de pérdida de los mismos.

-Sistemas redundantes: Son la copia de datos de mayor importancia. Cuando uno de los sistemas falla, no se pierde la información, sino que se recupera del otro lugar donde se encuentra.

**Seguridad lógica:**

-Control de acceso: Impide el acceso a personas no autorizadas mediante el uso de usuarios y contraseñas.

-Cifrado de datos: El cifrado es la acción de transformar un mensaje de tal forma que no pueda ser comprendido por otra persona distinta al receptor. Por lo tanto, el cifrado de datos consiste en la aplicación de un algoritmo de cifrado acompañado de una clave, con el objetivo de transformar el mensaje, para q únicamente pueda ser leído por el destinatario

-Antivirus: Permite escanear, detectar y eliminar malware en un sistema informático.

-Firewalls: Impide que malwares o hackers puedan ingresar a nuestra computadora a través de internet o de una red.

Seguridad en Internet

**ATAQUES DE DENEGACIÓN DE SERVICIOS**

DoS: Sucede cuando se produce una gran cantidad de peticiones desde **una** **sola** máquina o dirección IP a un servicio, saturando los puertos hasta colapsar el servidor, haciendo que no pueda responder a todas las peticiones. Otra forma de que ocurra puede ser el incremento de uso de recursos de manera forzada, saturando los recursos del dispositivo provocando el mismo efecto.

DDoS: Se produce una gran cantidad de peticiones al servicio, pero esta vez es desde **varios puntos o direcciones IP**. Provoca el mismo efecto que el ataque anterior.

**HACKING Y CRACKING**

Un hacker es una persona con un conocimiento elevado de informática y seguridad. Una persona que hackea un sistema es porque descubre sus vulnerabilidades con el objetivo de encontrar una herramienta que la minimice o suprima, o bien utilizar esta vulnerabilidad a su favor (dependiendo el tipo de hacker que sea)

TIPOS DE HACKER:

-White hats: utilizan los conocimientos de informática y seguridad con el fin de defender los sistemas de información.

-Gray hats: Tienen conocimientos tanto de la parte defensiva como ofensiva y pueden trabajar en cualquiera de los ámbitos.

Black hats: Utilizan los conocimientos para hacer actividades maliciosas o ilegales. También se los conoce como crackers.

**Diferencias entre hacker y cracker**

El hacker es un experto en varias ramas técnicas relacionadas con las tecnologías de información de las comunicaciones, como son: programación, redes, sistemas operativos e ingeniería de software.

El cracker es también un experto, pero además es quien viola la seguridad de un sistema informático con fines ilícitos o con un objetivo deshonesto y no ético.