**Resolución clase 25 – Plan de seguridad.**

**Aplicar seguridad física:**

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

-UPS.

-Respaldo de Datos local y remoto.

-Servidores redundantes.

**Seguridad lógica:**

 -Cifrado de datos -Antivirus –Firewalls.

**Aplicar seguridad activa:**

-Uso y empleo adecuado de contraseñas.

-Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.

-Encriptar los datos importantes.

**Seguridad pasiva**

-Comprobar si el antivirus funciona correctamente cuando hay una infección por un virus.

-Escanear el sistema al completo y, si se encuentra algún malware, limpiarlo.

-Realizar copias de seguridad de los datos y del sistema operativo en distintos soportes y ubicaciones físicas.

-Crear particiones del disco duro para almacenar archivos y backups en una unidad distinta a la del sistema operativo.

-Desconectar la máquina de la red hasta que se encuentre una solución. Comprobacion de antivirus

**Vulnerabilidades detectadas:**

-La intranet de la empresa es insegura, ya que las credenciales de acceso al sistema no tienen un alto nivel de seguridad.

-Parte del personal podría tener dificultades para adaptarse a los nuevos servicios de seguridad informática.

-Un posible ataque DDoS ante la falta de seguridad física en los servidores.