Plan de seguridad -Mesa 2:

1. Un análisis de la situación actual de cada empresa que se les haya asignado.

Detectamos las siguientes oportunidades de mejora en la empresa:

- Necesitan una intranet más segura.

- Identificamos que la empresa cuenta con empleados trabajando de forma remota.

- La empresa cuenta con poca seguridad física.

- Requieren obtener asesoramiento en seguridad lógica.

2 y 3. Para cada escenario planteado, crear un plan de seguridad:

- **Necesitan una intranet más segura:**
  - Se deben generar métodos de autenticación de cifrado mediante OTP para generar el ingreso de los escritorios remotos de la compañía y para la red de la empresa.

  - Proxy para tener un control en el tráfico de la red corporativa, para restringir la visita a páginas que no son acordes a las políticas de la empresa.

- **Seguridad física:**
  - La empresa debe contar con Pararrayos, extintores, detectores de humo, alarma contra intrusos, entre otros.
  - UPS
  - Respaldo de datos
  - Sistemas redundantes

- **Seguridad lógica:**
  - Contratar una empresa que realice auditoría
  - Aplicativo web que audite
  - Cifrado de datos

- **Seguridad Proactiva-Preventiva:**
  - Fomentar una cultura de seguridad: Capacitar a los empleados para que se concienticen para que entre todas y todos cuiden la seguridad de la organización.

- **Seguridad Pasiva:**
  - Invitar a los empleados a que realicen copias de seguridad en más de un dispositivo cada semana para proteger la información de posibles ataques.

-Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.

-Crear particiones en el disco duro para almacenar archivos y backups (copias de seguridad) en una unidad distinta a donde tenemos nuestro sistema operativo.

-Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar. Es importante que cuando haya una infección por un virus, se compruebe que el antivirus funcione correctamente.

- **Buenas prácticas para la Seguridad Activa:**

- Uso y empleo adecuado de contraseñas. Una de las técnicas para que una contraseña sea segura consiste en la combinación entre letras, números, mayúsculas y otros caracteres. No se debe usar nombre de mascotas o fechas de nacimiento, entre otros datos que pueden ser de conocimiento público.

- Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos. Encriptar los datos importantes. La encriptación consiste en cifrar los datos o la información mediante un algoritmo de cifrado con una clave para que el dato/información sólo pueda ser leído si se conoce la clave de cifrado.