**Auditoria:**

Práctica de auditoría y búsqueda de vulnerabilidades- Equipo 8

Empresa ya consolidada que se dedica a brindar servicios informáticos. La mayoría de sus empleados trabajan de forma remota, pero hay algunos que lo hacen on site. Necesitan una intranet más segura. La información confidencial de la empresa tiene buena seguridad lógica, pero muy poca física, aunque igualmente desean tener asesoramiento en seguridad lógica. No tienen problemas en invertir dinero, pero sus empleados se resisten al cambio de nuevas restricciones. Poseen una página web donde brindan sus servicios y los clientes pueden contactarse a través de la misma.

Este plan debe ser de 6 pasos e incluir: seguridad lógica, física, pasiva, activa y controles de medida de seguridad y de vulnerabilidades que podrían explotar los atacantes.

1. SEGURIDAD LÓGICA:

Verificar que en los últimos días sólo la gente con acceso accedió a la información que correspondía. Pedir que nos muestren una porción de la información para verificar si está correctamente encriptada. Verificar que los antivirus estén actualizados.

2-SEGURIDAD FÍSICA:

Una forma sería generar un apagón de la corriente eléctrica para simular un corte de luz y verificar que las UPS están funcionando.

Verificar cuándo se realizaron los últimos backups.

3-SEGURIDAD PASIVA:

Hacer seguimiento de un archivo aleatorio, para ver en dónde se encuentra el backup y en cuántos dispositivos.

Ver el historial de los análisis de antivirus realizados en el último período y sus resultados.

4-SEGURIDAD ACTIVA:

Pedir que le generen un perfil para verificar qué contraseñas nos pide y a qué datos podemos acceder, y qué información está encriptada.

5-CONTROLES DE MEDIDAS DE SEGURIDAD Y DE VULNERABILIDADES:

Solicitar un informe con los últimos ataques informáticos y ver qué medidas preventivas había hasta el momento, qué fue lo que no funcionó para poder corregirlo en el futuro y qué acciones se implementaron a partir de ello.