Práctica de auditoría y búsqueda de vulnerabilidades- Equipo 4

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:
Chequear control de acceso, cifrado de datos, actualización de antivirus y firewalls para asegurar que se aplique de manera correcta la seguridad lógica a través de su intranet.

2-SEGURIDAD FÍSICA:
Recomendamos la instalación de pararrayos y alarmas contra intrusos
Además recomendamos la revisión periódica de extintores de incendio y detectores de humo para cumplir la reglamentación.

Instalación de UPS en servidores importantes, para evitar pérdidas de información ante cortes de suministro.

Recomendamos un sistema de respaldo de datos periodico y la utilización de sistemas redundantes para información más valiosa para la empresa.

3-SEGURIDAD PASIVA
Recomendamos tener un procedimiento actualizado de realización de copias de seguridad, actualización de antivirus
Adicionalmente un plan de acción y simulacro de emergencia ante ataque de malware.

4-SEGURIDAD ACTIVA
Comenzar a capacitar de inmediato a los colaboradores acerca de las buenas prácticas en seguridad para evitar ataques.
Instalación de sotfware de seguridad informática

5-CONTROLES DE MEDIDAS DE SEGURIDAD Y DE VULNERABILIDADES.
Realizar simulacros de ataques de malware (por ejemplo a través de phishing) para generar conciencia de la gravedad e importancia de la ciberseguridad.