

Introducción a la Informática - Clase 25

Grupo 8

Escenario

- 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.

Plan de seguridad

Seguridad lógica

Si bien la empresa ya cuenta con buena seguridad lógica, se recomienda para tener una intranet más segura:

- Cifrado de datos
- Control de acceso

Seguridad física

Se debe reforzar la seguridad física:

- Agregar UPS
- Instalación de dispositivos físicos de protección: extintores, detectores de humo, alarma contra intrusos, etc.
- Respaldo de datos en tres servidores ubicados en distintos sitios.
- Sistemas redundantes para evitar perder datos.

Seguridad pasiva

- Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware
- Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.
- Revisar diariamente que el Antivirus esté en funcionamiento y operando con normalidad.

Seguridad activa

- Encriptación de datos importantes.
- Cambiar las contraseñas cada 3 meses y exigir que sea una combinación de letras, números, mayúsculas y otros caracteres.
- Capacitación al personal en temas de seguridad informática.

Controles de medida de seguridad

- Implementación de medidas de seguridad Detectivas basadas en la búsqueda de potenciales ataques o peligros.

Controles de vulnerabilidades

- Establecer Controles de acceso en la Intranet para que sólo accedan personas autorizadas.
- Encriptación de datos importantes.
- Delimitar quién puede y debe acceder a la información confidencial.