EQUIPO 8

Damelio Agustín, Díaz Salvador, Gattás Martina, Ravina Rodrigo, Sánchez Antonella, Vitelli Daniela

Escenario para grupos 2, 4, 6, 8, 10 , 12

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.

ANÁLISIS SITUACIÓN ACTUAL

La empresa cuenta con una Intranet, parte de su personal trabaja localmente y otros en forma remota. Presenta cierta seguridad lógica, pero vulnerabilidades en la seguridad física. Su personal es resistente al cambio.

PLAN DE SEGURIDAD

El plan de seguridad es aplicable a la intranet de la empresa.

- **Seguridad Lógica:** Autenticación de dos factores, restringiríamos el acceso por VPN, por protocolo L2TP con IPSec
- **Seguridad Física:** Establecer un sistema periódico de respaldo de datos con retrospectiva para poder hacer backup incremental de los archivos sensibles, duplicación cruzada de máquinas virtuales, instalación de UPS en todos los servidores.
- **Seguridad Pasiva:** Actualización de contraseñas una vez por mes, usar el principio del mínimo permiso, tener un sistema de dominio para poder manejar permisos por grupos de usuarios. Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.
- **Seguridad Activa:** Buenas políticas de contraseñas, encriptar los datos importantes.
- **Controles de medida de seguridad y vulnerabilidades:** Contratar servicios externos para auditoría de servicio (ej. de base de datos, de sistemas operativos no

sólo de los servidores sino también de las computadoras para evitar los exploits a través de rootkit).