EQUIPO 6:

Julia Faraudello, Edith Suarez, Daniel Delgado, Constanza Sauan

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:** Establecer políticas de seguridad de acceso remoto y local. Crear controles de acceso. Uso de contraseñas, encriptación de la información, antivirus, firewall, etc .
- **Seguridad Física:** Establecer un sistema periódico de respaldo de datos (backups); sistemas redundantes (copia de los datos de mayor importancia); instalación de UPS (para resguardo ante apagones de electricidad).

- **Seguridad Pasiva:** Implementación de buenas prácticas en la empresa como la realización de copias de seguridad de los datos en más de un dispositivo o en distintas ubicaciones físicas y el escaneo y limpieza continua de los equipos para controlar y evitar ataques de malware.
- **Seguridad Activa:** Los elementos activos contienen información, ya sea en forma de servidores, dispositivos móviles, bases de datos, etc. Estos elementos contienen información que puede ser destruida, vulnerada, o robada por malware, por lo tanto hay que establecer un uso y empleo adecuado de contraseñas, con combinaciones entre letras, números, y caracteres especiales. Prohibir el uso de nombres, fechas de nacimiento y otros datos de conocimiento público.

  También utilizar software de seguridad informática, como antivirus y antiespias. Por último encriptar los datos importantes mediante un algoritmo de cifrado con una clave para que la información pueda ser leída sólo por las personas que tienen acceso.

- **Controles de medida de seguridad y vulnerabilidades:** En primer lugar, implementar medidas de control preventivas para buscar que no se produzca un accidente o cualquier tipo de acción indebida en los sistemas (medida proactiva). Establecer medidas detectivas para buscar potenciales ataques o peligros a los que puede estar expuesto un sistema informático (medida reactiva).