MESA 4: ESCENARIO 2.

Integrantes:

Ana Paula Molina López, Andrea Bracco, Mauricio Perez, Federico Bustamante, Carlos Cepeda Danies.

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.

1. Un análisis de la situación actual de cada empresa que se les haya asignado.

Es una empresa consolidada, que no tiene problemas para invertir en mejorar su seguridad. Necesitan una Intranet más segura, con énfasis en una mayor seguridad física. El problema principal es la resistencia al cambio por parte de sus empleados.

2. Para cada escenario planteado, crear un plan de seguridad 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.

- Seguridad Lógica:

  Implementar control de acceso robusto a la intranet: contraseñas seguras y uso de doble factor de autenticación.

  Antivirus con base de datos actualizada para los usuarios on site.

  Firewall para prevenir la entrada de amenazas externas.

- Seguridad física: podrían emplear el uso de **UPS** para garantizar que no se pierda información en caso de cortes de energía. También sería útil, ya que la empresa cuenta con poca seguridad física, realizar copias de seguridad o **backups** de los datos completos e incrementales.

- Seguridad pasiva:
  1. Pueden hacer copias de seguridad de los datos en más de un dispositivo o en distintas ubicaciones físicas

2. Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.
3. Crear particiones en el disco duro para almacenar archivos y backups en una unidad distinta a donde tenemos nuestro sistema operativo.

- Seguridad activa
  - Contraseñas seguras, usando combinación de caracteres numéricos, alfanuméricos y especiales; con una política de no usar datos de posible conocimiento público.
  - Implementar antimalware, firewall y anti spywares profesionales
  - Encriptar datos más importantes.

- Controles de medida de seguridad

1. Proactivas.

- Directivas: Políticas de seguridad visibles para todos los empleados.
- Disuasivas: Mensajes de advertencia y alarmas conectadas a agentes de seguridad ante cualquier uso indebido.
- Preventivas: Mensajes de prevención y de información en puntos sensibles del sistema, para evitar errores.

2. Reactivas:

- Detectivas: Efectuar regularmente búsquedas de virus y otros malwares.
- Correctivas: Enviar a cuarentena activos comprometidos, buscar un reemplazo de los mismos.

- Vulnerabilidades que podrían explotar los atacantes: los empleados no están acostumbrados a usar contraseñas con buen nivel de seguridad. Conocen las contraseñas de otros empleados y las anotan en medios como papel, o notas dentro de la misma computadora.

  Al tener muy poca seguridad física, los atacantes podrían aprovechar la falta de firewalls para acceder a la intranet de la empresa y robar información.

ANOTACIONES MESA 3:

Recomendamos la implementación de una red privada virtual para las conexiones remotas de los empleados que trabajan desde su casa.

Para prevenir la pérdida de información importante es recomendable utilizar otras medidas de seguridad física, como extintores, detectores de humo, pararrayos y alarma contra intrusos.

La falta de capacitación en seguridad informática de los empleados es una vulnerabilidad importante, ya que el manejo descuidado de la información puede ser fuente de numerosas filtraciones. Al compartir las contraseñas, algún ex-empleado podría utilizar una de ellas para perjudicar a la empresa. Es recomendable utilizar un servicio de administración de contraseñas para eliminar la costumbre de anotarlas en papel.