Grupo 5

Tomás Correa
Juan Castore
Lourdes Martinez
Sofia Lancuba
Santiago Hernandez

1.Un análisis de la situación actual de cada empresa que se les haya asignado.
2. Para cada escenario planteado, crear un plan de seguridad
3. 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.

Esta serie de pasos y sugerencias debe ser presentada en un documento que pueda ser compartido con otras personas, especificando el grupo que son y el escenario que les tocó.

Empresa emergente dedicada a la venta de productos fertilizantes para campos con una capacidad financiera acotada. Todos sus empleados trabajan onsite y están dispuestos a recibir capacitación. Poseen actualmente dos personas encargadas de sistemas, las cuales manejan información sensible, pero que todos los usuarios pueden ver (no es política de la empresa). No realizan copias de información porque no las creen convenientes. Poseen una página web donde hay catálogos y los clientes pueden hacer compras a través de la misma.

1)

La situación de seguridad de la empresa en cuestión, a priori, es extremadamente vulnerable. Esto se debe a que hay solo dos personas que trabajan en sistemas con información sensible, pero todos los empleados tienen acceso a esta información y ninguno está capacitado en seguridad informática como para evitar problemas como el ingreso de algún malware que pueda robar o eliminar esa información.
Además, el hecho de que no cuentan con copias de seguridad de esta información, maximiza el riesgo al que está expuesta actualmente la información de la empresa, porque una vez afectada, no podría recuperarse en absoluto.

2 y 3)

Teniendo en cuenta la situación financiera acotada de la empresa, se pueden encontrar soluciones para los problemas antes mencionados sin realizar un plan demasiado costoso ni sofisticado, simplemente introduciendo algunos conceptos clave que ayudarían a prevenir problemas:

Seguridad lógica:

1. Acá lo recomendable sería comprar un servicio de antivirus con buena relación calidad precio, como el McAfee total protection.

Si la empresa cuenta con licencias oficiales de Windows, no haría falta ya que el sistema de antivirus y firewall de Windows es suficiente.

2. Recomendamos un software de control de acceso ya que permite llevar un registro de todas las operaciones realizadas sobre el sistema con fecha, horario, autorización, etc. lo que llevaría a tener mayor control sobre los datos que posee.

Seguridad física:

3. Colocar Pararrayos, extintores, detectores de humo, alarma contra intrusos, entre otros como también conectar los servidores de la empresa a un UPS(Uninterruptable Power Supply).
4. Agregar un sistema de respaldo de datos, de carácter urgente y usar sistemas redundantes para conservar los datos de mayor importancia.

Seguridad pasiva:

5. Garantizar el correcto funcionamiento y mantenimiento de los softwares que fortalezcan la seguridad lógica, como antivirus y firewalls.

Es fundamental crear backups offline y mantenerlos actualizados con frecuencia para que en caso de emergencia, de ciberataques, o que los datos estén comprometidos de alguna manera, podamos minimizar las pérdidas.

Seguridad activa:

6. Capacitar al personal en seguridad informática, que entiendan qué es el phishing y cómo suelen atacar los tipos de malware y cómo podrían entrar al sistema. Además, es importante que las contraseñas sean complejas y difíciles de descifrar, y que el mismo sistema obligue a complejizar la misma, requiriendo símbolos especiales, combinaciones de mayúsculas, minúsculas, números y que sean mínimo 8 caracteres.