Grupo 11 Escenario 1

Empresa emergente dedicada a la venta de productos fertilizantes para campos con una capacidad financiera acotada. Todos sus empleados trabajan on site 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.

Análisis:

La empresa no tiene una política clara sobre permisos de usuarios que pueda establecer el acceso a la información y su modificación. Además, la empresa actualmente no emplea un sistema de respaldo para su información por lo cual está en riesgo de perderla ante ataques dirigidos y/o causas externas como fallas eléctricas, rayos, incendios, derrames de líquidos, etc. También se nota que los empleados actuales encargados del sistema informático no tienen los conocimientos técnicos necesarios para la gestión del sistema pero están dispuestos a que los formen adecuadamente. Finalmente, con respecto a las transacciones que pueden realizar los usuarios en esta plataforma web, existe un riesgo grande de exposición de datos sensibles no sólo de la empresa sino de información bancaria (tarjetas de crédito, cheques, etc.)

Seguridad Lógica

- Establecer un esquema de permisos para los usuarios del sistema de modo que la información sólo pueda ser modificada por personas autorizadas.
- Cifrado de datos (ej: páginas con certificado https)

Seguridad Física

- Instalar un sistema de respaldo para la información.
- Asegurarse de tener un abanico de sistemas físicos de protección como un extintor, una alarma contra intrusos, pararrayos.

Seguridad Pasiva

- Calendarización de copias de seguridad en varias computadoras.

Seguridad Activa

- Crear credenciales con altos niveles de seguridad empleando caracteres especiales, números y letras en minúscula y mayúscula.
- Actualizar los software antimalware frecuentemente y realizar escaneos periódicos del sistema.

Controles de Medidas de Seguridad

- Disuasivas: sistema de alertas a través de mensajes que indican una brecha en la seguridad y que puede acarrear acciones legales.
- Directivas: crear una serie de instructivos sobre el uso del sistema para los distintos usuarios (base de conocimiento).
- Correctivas: cuando se detecte una falla en la integridad de la información, se emprenderá un proceso de corrección interno por parte de los gestores.

Cómo evitar las vulnerabilidades

- Capacitar al personal a cargo del sistema en temas de seguridad informática y prevención de riesgos.
- Usar software propietario con licencia para incrementar la confiabilidad de la protección y para poder usar el soporte técnico de estas herramientas.