Grupo 7.

Escenario:

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.

Situación Actual:

- Empresa emergente de pocos recursos que no implementa ningún tipo de plan de seguridad para proteger sus datos, el acceso a la información no es restringido y cualquiera puede acceder a ella.
- Este sistema es vulnerable a daños físicos como avería de una computadora, lo cual generaría pérdida total de la información al no contar con copias de seguridad.
- Es vulnerables a virus y ataques como DoS o DDos, generando un colapso total de su sistema, impidiendo a los clientes la realización de las compras.
- Las personas encargadas de manejar el sistema no se preocupan por la seguridad e integridad de la información.

Plan de Seguridad:

Seguridad Activa:

- Implementar el uso de contraseñas seguras (Caracteres alfanuméricos y especiales) para el acceso a la red.
- Uso de antivirus licenciados y actualizados.
- Capacitación al personal sobre la manera de prevenir problemas de seguridad informática.

Seguridad Pasiva:

- Realización de copias de seguridad periódicamente de la información sensible de la empresa.
- Crear particiones en el disco duro para almacenar las copias de seguridad en una partición diferente al sistema operativo.

Controles de medidas de seguridad:

*** Proactivas:**

- Usar Inteligencia de amenazas:
  - Conocer quién está atacando
  - Cuales son sus motivaciones
  - Conocer como mitigar esas amenazas

***Reactivas:**

- Detectivas:
  - Recopilar información para determinar amenazas Internas o externas.
  - Monitorear las actividades de los usuarios en el sistema y el uso de los recursos
- Correctivas:
  - Contar con un manual detallado de los pasos a seguir en caso de un ataque informático o un fallo en un equipo del sistema.

Seguridad Física:

- Alarmas contra intrusos que quieran acceder a la información del sistema
- Instalar UPS para evitar pérdida de información al tener problemas en el fluido eléctrico.
- Implementar sistemas redundantes para evitar pérdida de información.

Seguridad Lógica:

- Implementación y actualización de Antivirus
- Control de Acceso y establecimiento de privilegios para usuarios.