Jhonathan Antonio, Mateo Chauchet, Linda Jessenia Ramirez Giraldo, Mar Opradolce.

1. Hacer un análisis de la situación actual de cada empresa que nos toque.

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 medidas de seguridad, y de vulnerabilidades que podrían explotar los atacantes.

Empresa emergente dedicada a la venta de productos fertilizantes para campos, con una capacidad financiera acotada, todos sus empleados trabajan on site y están dispuesto 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. Seguridad lógica y activa: poner contraseñas a los usuarios que pueden ingresar, cifrar los datos de los compradores y la información sensible que manejan los empleados. Instalar antivirus y firewalls en los equipos de los empleados.
2. Seguridad física: hacer backups de toda la información de la organización y un respaldo extra de la información sensible. Instalar un UPS.
3. Seguridad pasiva: realizar escaneos con el antivirus de forma frecuente y capacitar al personal para desconectar los equipos de la red en caso de accesos no autorizados.
4. Implementar políticas que deban cumplir los empleados en cuanto a la seguridad de la información.
5. Vulnerabilidades: cualquier usuario puede ver la información sensible, se puede acceder a los datos de compra y facturación a los clientes porque no están cifrados, pueden perder todos sus datos al no tener respaldos, la empresa no cuenta con políticas de seguridad de la información.