Equipo 9:

- Stefany Salamanca
- Lara Converso
- Andres Felipe Monterrosa
- Santiago Duran
- Jorge Andres Jimenez
- Maria Eugenia Gadea

Actividad 1:

La empresa que se les haya asignado los contrata como asesores de seguridad, ya que creen que es una parte fundamental para resguardar sus activos. En base a lo visto en clase y clases anteriores deben hacer:
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.

Escenario:

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.

Solución:

Análisis: Trata de una empresa la cual no maneja buenas prácticas a la hora de manipular información confidencial, tienen vacíos de integridad en la información ya que no realizan copias de información periódicamente, falta recurso humano experto en informática.

Plan de seguridad:

- **Seguridad lógica:** Crear directorios activos que restrinjan el uso no autorizado de la información, cifrar los datos personales de los clientes que hacen compras, instalar antivirus en los equipos de los colaboradores e implementar firewall para monitorear el tráfico en la red.
- **Seguridad física:** La realización de copias de seguridad de los datos en más de un dispositivo o en distintas ubicaciones físicas.
  Realizar una copia de los datos de mayor importancia por si alguno de los sistemas fallan.
- **Seguridad pasiva:** Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.
  Crear particiones en el disco duro para almacenar archivos y backups (copias de seguridad) en una unidad distinta a donde tenemos nuestro sistema operativo.
  Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.
  Es importante que cuando haya una infección por un virus, se compruebe que el antivirus funcione correctamente.
- **Seguridad activa:** Capacitar en el uso recomendado y diferentes técnicas al crear passwords, instalar servidores que permiten almacenar información relevante de la empresa, encriptar comunicaciones entre los servidores.
  Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.
- **Controles de medida de seguridad:** Sensibilizar y capacitar a los colaboradores (Preventiva y Correctiva). Realizar copias de seguridad periódicas (Preventiva), instalar directorios activos con políticas de seguridad y navegación (Directivas), Implementación de diferentes servidores con su respectiva seguridad (Preventiva y Disuasiva), instalar antivirus (Detectivas y Correctivas).
- **Vulnerabilidades:** Mal manejo de la información delicada ya que todo el mundo puede acceder a ciertos datos, y va en contra de las políticas de la empresa.