**Equipo 1:**
Tania Lenis
Brenda Bueno
Rocio Torrez
Gina Rodríguez
Lucila Arjona
Victor Valencia

**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**

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:**

- Implementar control, que permita identificar a las personas encargadas de sistemas, con uso de biometría, contraseñas de autenticación.

**Seguridad Física:**

- Conformar un equipo (brigada), que reciba capacitaciones para el manejo de prevención ante cualquier factor ambiental (incendio, inundaciones, humedad, calor, frío).
- Dispositivos físicos de protección: como trabajan on site, es necesario implementar el uso de pararrayos, extintores, detectores de humo, alarma contra intrusos.
- UPS.

**Seguridad Activa:**

- Verificar el uso adecuado de contraseñas y la encriptación de datos importantes

- Uso de software adecuado al site para mantener la seguridad informática

**Seguridad Pasiva:**

- Considerar usar un hardware adecuado contra averías y accidentes.
- Realizar copias de seguridad de los datos y del sistema operativo en distintos soportes y ubicaciones físicas.
- Si se presentase algún error desconectar la máquina de la red hasta que se encuentre una solución.
- Crear particiones del disco duro para almacenar archivos y backups en una unidad distinta a la del sistema operativo.
- Implementar antivirus, con el fin de proteger los equipos.
- Realizar copias de seguridad.

**Controles de medida de seguridad:**

- Cifrado de la información.
- Restringir acceso a intranet a las personas que ya no laboran para la empresa.
- Copias de seguridad
- Sólo el personal autorizado puede tener acceso a la información.
- Trabajar en la nube.
- Utilizar contraseñas seguras.
- Proteger correo electrónico.

**Vulnerabilidades que podrían explotar los atacantes**:

- Suplantación de identidad.
- Amenazas de malware.
- Las malas prácticas o la falta de formación en ciberseguridad
- Errores que permiten el acceso a directorios.
- Errores en los sistemas de validación.
- Errores en la gestión y asignación de permisos
- Botnets conjunto de equipos infectados que ejecutan programas de manera automática y autónoma.