**Situación actual:**

Podemos observar que la empresa es vulnerable a filtración o robo de información sensible. Ya que cualquier usuario puede visualizar.

No se respalda la información crítica, con lo que es sensible a pérdidas tanto por técnicas de robo informático como fallas de hardware.

PLAN

**Seguridad activa:**

1.Personalizar el software empleado para ocultar la información sensible. Encriptar la información en bases de datos utilizando algoritmos de cifrado vigentes.

2.Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.

Contratar protección para ataques DDOS

**Seguridad pasiva:**

3.Poseer al menos un servidor adicional a modo de redundancia.

4.Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.

**Seguridad lógica:**

5.Similar al caso de la seguridad activa, se encriptará la información y se limitaría el acceso visual a la información sensible, ya que si bien solamente 2 personas pueden editar, no es necesario que todos puedan verla con libre acceso ya que sería una brecha por donde se pueden filtrar datos.

**Seguridad preventiva:**

6.Capacitar a los usuarios de la empresa para utilizar contraseñas seguras, y prevenir ataques de contactos externos vía medios de comunicación ej. Mail.

**Seguridad física:**

7.Factor de doble autenticación.

UPS frente a un apagón eléctrico, seguir almacenando la información por un determinado tiempo.

8.Se deben realizar copias de seguridad o backups de los datos completos e incrementales.