

Objetivo:

El objetivo de esta sección es detallar los mecanismos de protección de datos, incluyendo el uso de respaldos periódicos, el cifrado de datos sensibles y la implementación de controles de acceso estrictos para garantizar la seguridad y disponibilidad de la información crítica de la empresa.

1. Respaldo Periódico de Datos

- Implementación de una estrategia de respaldos en 3-2-1: tres copias de los datos, dos tipos de almacenamiento (local y en la nube), y una copia fuera del sitio.
- Realizar copias de seguridad de los datos críticos de manera diaria, semanal y mensual.
- Verificación regular de la integridad de los respaldos y pruebas de restauración periódicas.

2. Cifrado de Datos Sensibles

- Implementar cifrado de extremo a extremo para proteger los datos en tránsito.
- Cifrar los datos almacenados en repositorios críticos y bases de datos, asegurando que solo usuarios autorizados puedan acceder.
- Uso de algoritmos de cifrado robustos como AES-256.

3. Control de Acceso Estricto

- Implementación de políticas de acceso de acuerdo al principio de "mínimo privilegio".
- Uso de sistemas de gestión de identidades (IAM) para asegurar que solo usuarios autorizados tengan acceso a los sistemas críticos.
- Auditorías regulares de los accesos para detectar posibles vulnerabilidades o accesos no

autorizados.

Conclusión

El respaldo periódico de datos, el cifrado de información sensible y el control de acceso son medidas fundamentales para proteger los activos de información. Estas acciones contribuyen a garantizar la integridad, confidencialidad y disponibilidad de los datos críticos para la empresa.