1. Objetivo

Garantizar la disponibilidad y recuperación de la información mediante la implementación de procedimientos de respaldo confiables.

2. Alcance

Aplica a todos los sistemas críticos, bases de datos, configuraciones, software e imágenes del sistema utilizados por la organización.

3. Lineamientos

3.1 Creación de respaldos

- Se deben realizar copias de respaldo periódicas de la información crítica, software y configuraciones.
- La frecuencia de respaldo dependerá de la criticidad de la información: diaria, semanal o mensual.

3.2 Almacenamiento

- Las copias de seguridad deben almacenarse en medios seguros, tanto local como remotamente (offsite o en la nube).
- El acceso a los respaldos debe estar restringido únicamente a personal autorizado.
- Las copias deben estar cifradas si contienen información sensible.

3.2.1 Gestión de repositorios y código fuente

Se debe establecer una política formal para la gestión segura de los repositorios y el código fuente, que incluya como mínimo:

- Uso obligatorio de plataformas reconocidas y seguras para el alojamiento de repositorios (GitHub, GitLab, etc.).
- Aplicación del principio de mínimo privilegio para el control de accesos, incluyendo autenticación multifactor.
- Configuración por defecto de los repositorios como privados.

- Prohibición expresa del almacenamiento de contraseñas, claves privadas o datos sensibles en el repositorio.
- Revisión obligatoria del código mediante pull/merge requests antes de su integración en ramas principales.
- Escaneo automatizado para la detección de vulnerabilidades y secretos expuestos.
- Respaldo periódico de los repositorios críticos, con almacenamiento en ubicaciones seguras.
- Revocación inmediata de accesos cuando un desarrollador deja de pertenecer a la organización.
- Documentación y trazabilidad de cualquier eliminación, transferencia o reestructuración de repositorios.

Esta política tiene como objetivo salvaguardar la integridad, confidencialidad y disponibilidad del software y sus versiones en entornos de desarrollo, prueba y producción.

3.2.2 Protección de la información de registro (A.12.4.2)

Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado. Para ello, se implementarán las siguientes medidas:

- Almacenamiento centralizado de registros en servidores protegidos con control de acceso restringido.
- Monitoreo continuo de los archivos de registro y generación de alertas ante cambios no autorizados.
- Revisión periódica de los registros por parte del personal autorizado.

3.3 Retención y eliminación

- Las copias de respaldo se conservarán por un periodo determinado según los requisitos legales y operativos.
- Las copias obsoletas deben eliminarse de forma segura.

4. Responsabilidades

- El área de TI es responsable de la ejecución, monitoreo y prueba de los respaldos.
- Los usuarios deben asegurarse de guardar información relevante en ubicaciones incluidas en el plan de respaldo.

5. Sanciones

El incumplimiento de esta política puede dar lugar a acciones disciplinarias conforme a la normativa interna de la organización.

CARLOS HUMBERTO TRONCOSO AYALDE
GERENTE GENERAL

VERSIÓN	CAMBIO	VIGENCIA
1	Primera versión	25/06/2024