LINEAMIENTOS DE BACKUP Y RECUPERACIÓN DE INFORMACIÓN Referencia: ISO/IEC 27001:2022, control 8.13 (copias de seguridad de la información)

Sistema de Gestión de Seguridad de la Información
Secretaría de Educación Del Distrito

Versión 1.0
Febrero 2026

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN
BOGOTÁ

Tabla de Contenido

Índice de Tablas

VOCABULARIO

Activo de Información: Cualquier cosa de valor que tiene que ver con la información (ej. datos, sistemas, software, equipos o personal).

Archivo Central: Fase de la gestión documental donde las copias de respaldo son almacenadas después de que su uso activo disminuye, por un período de 3 años, antes de su disposición final (Eliminación).

Archivo de Gestión: Fase de la gestión documental donde las copias de respaldo son utilizadas de forma activa y se conservan por un período de 17 años.

AZURE: Plataforma de computación en la nube de Microsoft con productos y servicios para crear, ejecutar y administrar aplicaciones.

Backup (Copia de Respaldo): Una copia de la información de datos, software e imágenes del sistema que se mantiene para el propósito de recuperación, según el control A.8.13.

Copias de Respaldo de los Sistemas de Información Institucional: La subserie documental específica, compuesta por archivos digitales y cintas de seguridad, que se rige por una retención total de 20 años (17 en gestión y 3 en central) antes de su eliminación.

Cifrado (Encryption): Proceso de codificar la información de backup, tanto en tránsito como en reposo, para protegerla del acceso no autorizado, cumpliendo con el requisito del Control A.8.13.

Disposición Final: Proceso de eliminación documental de las copias de respaldo al cumplirse el periodo total de retención, ya que no poseen valores secundarios.

Infraestructura Híbrida: El entorno de TI que combina recursos de computación en la nube (OCI y Azure) con recursos On-Premise (local) de la organización.
Inmutabilidad (WORM) Una característica de almacenamiento que previene que los datos de backup sean modificados o eliminados durante un período de tiempo definido, protegiéndolos contra ransomware y corrupción.

ISO/IEC 27001:2022: Estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

OCI: Oracle Cloud Infrastructure, es la plataforma de Oracle que ofrece servicios de computación, almacenamiento y seguridad, combinando hardware dedicado con la flexibilidad de la nube.

ON-PREMISE: modelo donde el software y los datos se instalan y ejecutan en los servidores y la infraestructura física de una empresa.

REGIÓN (AZURE Y OCI): Área geográfica que contiene uno o más centros de datos físicos para ofrecer servicios de nube pública

RPO (Recovery Point Objective): La máxima cantidad de tiempo aceptable que los datos se pueden perder después de un incidente. Define la frecuencia con la que se deben realizar los backups.

RTO (Recovery Time Objective): El tiempo máximo aceptable para recuperar las funciones críticas del negocio después de un incidente. Define la velocidad con la que se debe realizar la restauración.

1 INTRODUCCION

La Secretaría de Educación del Distrito (SED) ha determinado la necesidad de contar con lineamientos de respaldo, almacenamiento y recuperación de la información crítica que garantice la disponibilidad e integridad de los activos informáticos dispuestos en sus centros de datos.

El presente documento describe los lineamientos de respaldo de información y almacenamiento junto con los procedimientos y mecanismos para la realización de las actividades relacionadas, con el fin de apoyar a los distintos actores en la reducción de los impactos de los riesgos que puedan ser generados por fallas en servicios internos y externos de la entidad que involucren la pérdida total o parcial de información.

2 OBJETIVO

El propósito de estos lineamientos es establecer los requisitos y procedimientos para la adecuada ejecución de los procesos de respaldo, almacenamiento, custodia y recuperación de la información mediante la creación, mantenimiento, prueba y protección de copias de seguridad de la información crítica de la organización. Esto asegura la disponibilidad (Availability) de la información y la capacidad de recuperación (Resilience) ante fallos, desastres o incidentes de seguridad, en cumplimiento con los requisitos de negocio, legales, reglamentarios y contractuales.

3 ALCANCE

Este lineamiento aplica a toda la **información crítica** de la organización, incluyendo datos, configuraciones de sistemas, máquinas virtuales, bases de datos y aplicaciones, independientemente de si residen en:

- Infraestructura On-Premise (Local).
- Oracle Cloud Infrastructure –OCI (Nube).
- Microsoft Azure (Nube).

4 ROLES Y RESPONSABILIDADES

Tabla 1 Roles y Responsabilidades

Rol	Responsabilidad Clave
Oficial de Seguridad de la Información (CISO)	Aprobación, revisión y cumplimiento de los lineamientos.
Administradores de Infraestructura (OCI, Azure, On-Premise)	Implementación, monitoreo y gestión diaria de los procesos de backup.

Rol	Responsabilidad Clave
Equipo de Recuperación de Desastres	Ejecución de pruebas de restauración y del plan de recuperación ante desastres (DRP).
Dueños de la Información	Identificación de la información crítica, requisitos de RTO (Recovery Time Objective) y RPO (Recovery Point Objective).

5 RESPALDO DE LOS LINEAMIENTOS

Los presentes lineamientos están fundamentados en los requisitos del A.8.13 de la norma internacional ISO/IEC 27001:2022, incluyendo los aspectos clave que exige el control:

Tabla 2 Cumplimiento Control 8.13

Componente de los Lineamientos	Requisito de A.8.13 cubierto
ítem b (Tipos, Frecuencia, Ubicación)	*"...reflejando los requisitos comerciales de la organización (por ejemplo, el objetivo de punto de recuperación, ver 5.30), los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización en cuanto al alcance (por ejemplo, copia de seguridad completa o diferencial) y la frecuencia de las copias de seguridad..."*
ítem f (Protección de los Backups: Cifrado, Inmutabilidad)	*"...proteger las copias de seguridad mediante cifrado según los riesgos identificados (por ejemplo, en situaciones donde la confidencialidad es importante)."*
ítem e (Procedimientos y Pruebas)	*"... probar regularmente los medios de respaldo para asegurarse de que se puedan utilizar de manera confiable en caso de emergencia cuando sea necesario. Probar la capacidad de restaurar los datos respaldados en un sistema de prueba, sin sobrescribir los medios de almacenamiento originales en caso de que el proceso de respaldo o restauración falle y cause daños o pérdida irrecuperable de datos."*

6 REQUISITOS DE BACKUP Y FRECUENCIA

El dueño de la información debe determinar la criticidad de los datos para establecer el RPO (Recovery Point Objective) y el RTO (Recovery Time Objective), los cuales definirán la frecuencia de los backups y la velocidad de restauración.

Tabla 3 Requisitos y Frecuencia

Clasificación de Datos	Ejemplo de RPO	Frecuencia Mínima de Backup
Crítico (Tier 1)	< 1 hora	Continua o cada 15 min

Clasificación de Datos	Ejemplo de RPO	Frecuencia Mínima de Backup
Alto (Tier 2)	< 4 horas	Diaria (Incremental o Diferencial)
Medio (Tier 3)	< 24 horas	Diaria (Completa o Diferencial)

Todos los sistemas deben implementar una combinación de **backups completos, diferenciales e incrementales** según lo permita la tecnología y lo exijan los objetivos de RPO/RTO.

7 TIPOS Y FRECUENCIA DE BACKUP

- Se debe implementar una combinación de **backups completos, diferenciales e incrementales** según lo requiera la estrategia de RPO/RTO y la eficiencia del almacenamiento.
- **Frecuencia Mínima:** Los datos de **máxima criticidad** deben tener una frecuencia de backup que permita cumplir con un RPO de **no más de 24 horas**.

8 ESTRATEGIA DE ALMACENAMIENTO HÍBRIDO (3-2-1)

Se debe implementar la estrategia **3-2-1** como estándar de resiliencia: 3 copias de los datos, en 2 tipos de medios diferentes, y 1 copia fuera del sitio o aislada.

Tabla 4 Estrategia Almacenamiento

Plataforma	Almacenamiento Primario (Tipo de Medio)	Almacenamiento Secundario (Copia Fuera del Sitio)
On-Premise	Servidores de backup locales (ej. NAS/SAN).	Replicación a OCI Object Storage o Azure Blob Storage.
OCI	OCI Object Storage (replicación dentro de la misma región o a otra región).	**OCI Object Lock** debe usarse para inmutabilidad.
Azure	Azure Backup Vault / Azure Storage.	Almacenamiento con **Redundancia Geográfica (GRS)** o **Inmutabilidad de Blobs** (WORM).

Requisitos por Plataforma:

- **On-Premise:** Los backups deben almacenarse en medios separados (ej. NAS, SAN o cinta) y una copia debe ser replicada a una ubicación geográfica diferente (ej. OCI/Azure o un sitio secundario).
- **OCI:** Se utilizarán servicios como **OCI Object Storage** para el

almacenamiento de backups, aprovechando las capacidades de redundancia dentro de la región y replicando a una región secundaria (Cross-Region Replication).

- **Azure:** Se utilizarán servicios como **Azure Backup** y **Azure Storage** (LRS, GRS, ZRS) para almacenar los datos, garantizando la **redundancia geográfica** (GRS) o de zona (ZRS) para los datos más críticos.

9 PROTECCIÓN Y SEGURIDAD DE LOS BACKUPS

El control A.8.13 exige que los backups estén protegidos contra pérdida, daño y acceso no autorizado.

1. **Cifrado (Encryption):** Todos los datos de backup deben estar **cifrados** (en reposo y en tránsito) utilizando algoritmos fuertes. En OCI y Azure, se debe garantizar que el cifrado gestionado por la plataforma esté activo (ej. CMK o claves de plataforma).

2. **Control de Acceso:** El acceso a los datos de backup debe ser limitado (Principio de Mínimo Privilegio) mediante controles de identidad (IAM) que separen las credenciales de producción de las credenciales de backup (Segregación de Redes y Funciones).

3. **Inmutabilidad (WORM):** Siempre que sea técnicamente posible (ej. OCI Object Lock, Azure Immutable Storage), la copia de seguridad fuera del sitio debe configurarse con una política de **"Write Once, Read Many" (WORM)** para protegerla contra el ransomware y la eliminación accidental.

10 PRUEBAS Y MONITOREO

Para garantizar la fiabilidad, los medios de backup deben probarse regularmente para confirmar que los datos pueden restaurarse cuando sea necesario.

- **Pruebas de Restauración:**
  - Se deben realizar pruebas de restauración de los datos al menos semestralmente o después de cambios significativos en el sistema de producción o la infraestructura de backup.
  - La restauración debe realizarse a un entorno de prueba o "sandbox" separado para no sobrescribir los datos originales.
  - Las pruebas deben simular escenarios realistas de fallo (ej. pérdida de un servidor, corrupción de datos) para validar la integridad de los datos de backup y la eficacia de los procedimientos de restauración para cumplir con el RTO.
  - Los resultados de las pruebas, incluyendo cualquier deficiencia o lección aprendida, deben ser documentados y presentados al CISO.
- **Monitoreo:**

- Los administradores deben monitorear diariamente el estado de finalización de todos los jobs de backup para detectar fallas y asegurar la integridad de los datos.
- Los registros (logs) de backup deben conservarse durante un período no menor a [Periodo definido, ej. 1 año] para fines de auditoría.
- Se realizarán auditorías internas periódicas para verificar el cumplimiento de estos lineamientos.

- **Procedimientos Documentados:** Se deben mantener procedimientos operativos detallados y probados para la ejecución de backups y restauraciones en cada plataforma (On-Premise, OCI, Azure) para asegurar que se cumplan los objetivos del plan de continuidad de TI (Control A.5.30).

11 RETENCIÓN Y DISPOSICIÓN FINAL (AJUSTE CONFORME A T.R.D.)

Los lineamientos de retención de los datos de backup debe ser consistente con la **Tabla de Retención Documental (TRD)**[1] de la entidad, específicamente para la serie documental **"COPIA DE RESPALDO DE LOS SISTEMAS DE INFORMACIÓN INSTITUCIONAL"**.

11.1 Períodos de Retención

La retención de las copias de respaldo, los archivos digitales y cintas de seguridad, se regirá por la siguiente tabla de retención para la Subserie documental:

Tabla 5 Periodo de Retención

Serie Documental (Código 5320-240)	Proceso	Archivo de Gestión (A Gestión)	Archivo Central (A Central)	Retención Total	Disposición Final
COPIA DE RESPALDO DE LOS SISTEMAS DE INFORMACIÓN INSTITUCIONAL [2]	Infraestructura y Gestión Tecnológica	17 años	3 años	**20 años**	**Eliminación (X)**

[1] https://www.educacionbogota.edu.co/portal_institucional/sites/default/files/inline-files/Tablas_retencion_documental_Ofi_Aadministrativa_REDP.pdf

11.2 Justificación de Disposición Final

- Una vez cumplido el tiempo de retención de **20 años** en el Archivo de Gestión y Central, se procederá a la **Eliminación Documental (X)**.
- La eliminación se aplica debido a que se trata de **copias de información** que están en constante actualización. Por lo tanto, una vez agotados los valores primarios (legales, administrativos, operativos), los datos de backup carecen de valores secundarios (históricos o de investigación) y deben ser eliminados de forma segura e irrecuperable.

Aprobado por: MILENA DEL PILAR SANDOVAL GOMEZ
Jefe Oficina de Tecnologías de la Información y las Comunicaciones - OTIC

Elaborado: Juan Carlos Parra Moreno
Oficial Seguridad Informática - OTIC

Revisado: Jairo Alberto Orduz Salamanca
Profesional Especializado – OTIC

Revisado: Omar Ardila Torres
Contratista – OTIC

Revisado: Camilo Arturo Sierra
Contratista – OTIC

Revisado: Rodrigo Bernal Abril
Contratista – OTIC

Revisado: Jorge Mauricio Barragán B
Profesional Especializado – OTIC