

	Guía Institucional de Copias de Seguridad (Oracle Cloud y Microsoft 365)	CÓDIGO: G4_TIC
		VERSIÓN: 1
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 01/07/2025
		Página: 1 de 11

TABLA DE CONTENIDO

1. OBJETIVO	2
2. ALCANCE	2
3. DEFINICIONES	2
4. NORMATIVIDAD ASOCIADA	3
5. DESARROLLO	3
5.1. Generalidades	3
5.2. Frecuencia de Respaldo y Políticas de Retención	5
5.3. Restauración y Pruebas de Recuperación	7
5.4. Respaldo de Información en Microsoft 365	7
5.5. Copias de Seguridad en Oracle Cloud (Políticas Automatizadas)	9
5.6. Roles y Responsabilidades	10
6. ANEXOS	10
7. DOCUMENTOS DE REFERENCIA	10

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Guía Institucional de Copias de Seguridad (Oracle Cloud y Microsoft 365)	CÓDIGO: G4_TIC
		VERSIÓN: 1
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 01/07/2025
		Página: 2 de 11

1. OBJETIVO

Establecer los criterios, responsabilidades y buenas prácticas para la ejecución de copias de seguridad y restauración de datos en la infraestructura tecnológica de la entidad, orientadas a garantizar la continuidad institucional, la disponibilidad de los sistemas de información y la integridad de los datos almacenados en Oracle Cloud Infrastructure y Microsoft 365.

2. ALCANCE

Esta guía aplica a todos los sistemas, servicios, bases de datos, archivos y activos digitales que residan en la infraestructura cloud contratada por la entidad, específicamente:

- Oracle Cloud Infrastructure (OCI): incluye bases de datos Oracle y MySQL, servidores de aplicación, volúmenes de almacenamiento, file systems, y repositorios de código fuente.
- Microsoft 365: incluye correo electrónico institucional (Exchange Online), almacenamiento de archivos (OneDrive y SharePoint), Teams y otras aplicaciones relacionadas.

Aplica al personal técnico de la Subgerencia de Tecnologías de la Información y las Comunicaciones, contratistas responsables de la administración de estas plataformas y jefes de dependencia que gestionen solicitudes de restauración o acceso a información resguardada.

3. DEFINICIONES

- **Copia de seguridad** (Backup o Respaldo): Duplicado de los datos originales almacenado en un medio alterno seguro, realizado con el fin de poder recuperarlos en caso de pérdida, daño o fallo del sistema original. Es un mecanismo esencial de protección de la información.
- **Restauración** (Restore): Proceso de recuperar datos a partir de una copia de seguridad previamente realizada, devolviéndolos a su estado original o a un entorno operativo tras un incidente. Implica cargar o reintegrar la información respaldada en el sistema de producción para reanudar las operaciones.
- **Retención** (de respaldos): Periodo de conservación de las copias de seguridad antes de su eliminación o depuración. Una política de retención define cuánto tiempo se almacenan los respaldos (por ejemplo, 7 días, 1 mes, 1 año) antes de ser descartados automáticamente, asegurando un historial suficiente de versiones para recuperación.
- **Oracle Cloud**: Plataforma de servicios en la nube provista por Oracle, que incluye infraestructura como servicio (IaaS) –por ejemplo, instancias de cómputo (servidores virtuales), almacenamiento en bloque, redes– y plataformas de datos como bases de datos Oracle en la nube. En esta guía nos referiremos a Oracle Cloud para englobar todos estos servicios cloud bajo responsabilidad de la institución.
- **Microsoft 365**: Servicio en la nube de Microsoft que integra aplicaciones de productividad y colaboración (Exchange Online para correo, OneDrive y SharePoint para almacenamiento de archivos, Teams, entre otros). Aunque Microsoft 365 ofrece alta disponibilidad y ciertas capacidades nativas de retención, los datos alojados en esta plataforma también requieren

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Guía Institucional de Copias de Seguridad (Oracle Cloud y Microsoft 365)	CÓDIGO: G4_TIC
		VERSIÓN: 1
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 01/07/2025
		Página: 3 de 11

de algunas configuraciones relacionadas con políticas de retención adicionales bajo responsabilidad de la institución.

4. NORMATIVIDAD ASOCIADA

- Acuerdo No 002 del 2023, proferido por la comisión distrital de transformación digital, por el cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.
- Decreto 767 de 2022: Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Resolución 746 de 2022: Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021
- Directiva Presidencial No. 02 de 2022: Reiteración de la Política pública en materia de seguridad digital
- Resolución 500 del 10 de marzo de 2021 del Ministerio de Tecnologías de la Información y Comunicaciones.

5. DESARROLLO

A continuación, se detallan las buenas prácticas y directrices concretas que la institución adopta para la gestión de copias de seguridad en Oracle Cloud y Microsoft 365. Se abordan la frecuencia de los respaldos, las políticas de retención, los procedimientos de restauración, consideraciones específicas para Microsoft 365 y Oracle Cloud (respaldos automatizados), las estrategias según el tipo de servicio, y los roles y responsabilidades involucrados en su ejecución.

5.1. Generalidades

- Las copias de seguridad deben realizarse de forma automática y programada sobre los recursos críticos definidos y programados por la Subgerencia de Tecnologías de la Información y las Comunicaciones.
- Ninguna información institucional debe ser almacenada de forma local en equipos personales o institucionales, ya que estos no están incluidos en el esquema de respaldo institucional.
- Se deben usar los servicios de respaldo proporcionados por los proveedores (OCI y Microsoft) según su configuración, capacidades y garantías establecidas.
- La entidad hace uso de servicios en la nube para gestionar la infraestructura tecnológica y las copias de seguridad, conforme a las políticas definidas por los proveedores (Oracle y Microsoft).
- Todos los usuarios deben almacenar la información institucional en los repositorios de Microsoft 365, como lo son OneDrive y SharePoint de la dependencia.
- Las copias de seguridad se realizan de forma programada para:

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Guía Institucional de Copias de Seguridad (Oracle Cloud y Microsoft 365)	CÓDIGO: G4_TIC
		VERSIÓN: 1
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 01/07/2025
		Página: 4 de 11

- Bases de datos.
 - Servidores de aplicaciones.
 - Componentes de almacenamiento (block storage, file systems).
 - Código fuente (repositorios Git).
- Microsoft administra las copias de seguridad de sus servicios (OneDrive, SharePoint y correo) con políticas de retención de 14 a 93 días. Restauraciones completas pueden solicitarse, pero no se garantiza la recuperación parcial.
 - Cuando un usuario es inactivado o eliminado del sistema institucional (por retiro, traslado, finalización de contrato u otras causas), la información almacenada en su cuenta de OneDrive y buzón de correo se conserva temporalmente por parte del proveedor Microsoft 365:
 - OneDrive: permanece disponible por 30 días tras la eliminación del usuario.
 - Buzón de correo (Exchange Online): puede retenerse hasta 30 días, salvo que se aplique una política de retención extendida configurada por la Subgerencia de Tecnologías de la Información y las Comunicaciones.
 - En algunos casos, la información puede recuperarse hasta por 93 días, dependiendo del tipo de inactivación y de las políticas aplicadas por Microsoft.

Una vez cumplido el plazo de retención automática, la información es eliminada de forma irreversible, sin posibilidad de recuperación parcial o total.

- La Subgerencia de Tecnologías de la Información y las Comunicaciones brinda acompañamiento técnico para la entrega de respaldos en los casos permitidos.
- Las solicitudes de copias de seguridad o accesos a la información contenida en el buzón de correo y/o OneDrive de un usuario (activo o inactivo) deberán ser gestionadas únicamente por el Jefe de Oficina, Supervisor, Gerente, Subgerente o Director General.
- Toda solicitud que se realice para restaurar copias de seguridad deberá estar sustentada mediante memorando oficial radicado a través de SIGA a la Subgerencia de Tecnologías de la Información y las Comunicaciones o a través de la aplicación de la mesa de ayuda, la cual debe contener:
 - Nombre completo del usuario al cual se requiere tener acceso.
 - Motivo de la solicitud (por ejemplo: investigación, continuidad operativa, requerimiento de entes de control).
 - Alcance de la información requerida (correo completo, fechas específicas, carpetas de OneDrive, etc.).
- El acceso a esta información será otorgado solo si existe una justificación válida y documentada, conforme a los principios de privacidad y seguridad de la información establecidos por la entidad.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Guía Institucional de Copias de Seguridad (Oracle Cloud y Microsoft 365)	CÓDIGO: G4_TIC
		VERSIÓN: 1
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 01/07/2025
		Página: 5 de 11

- La Subgerencia de Tecnologías de la Información y las Comunicaciones será la encargada de evaluar, ejecutar y custodiar estas acciones de respaldo y restauración, garantizando la trazabilidad de la ejecución de las copias de seguridad.
- En caso de que no sea viable atender la solicitud por razones técnicas o normativas, o si el solicitante no cumple con los requisitos establecidos, se debe emitir una respuesta formal mediante el SIGA, que indique las razones de la negativa y registrar el cierre del procedimiento en el sistema de atención.

5.2. Frecuencia de Respaldo y Criterios de Retención

A continuación, se establecen los criterios generales, sobre la frecuencia de ejecución de las copias y su retención.

Frecuencia (Periodicidad):

- *Datos críticos (Sistemas de información misionales y de apoyo en sus ambientes de producción):* Respaldo diario como mínimo. En Oracle Cloud esto implica realizar snapshots o backups cada 24 horas (o con mayor frecuencia si el RPO lo exige).
- *Datos semi-críticos (sistemas de apoyo, entornos de prueba, datos con baja tasa de cambio en ambientes de pruebas o preproducción):* Respaldo semanal completo, complementado con incrementales diarios si corresponde.
- *Datos no críticos o redundantes:* Respaldo mensual o según necesidad.
- Configuraciones y Código Fuente: Repositorios de código y configuraciones de sistemas (scripts, definiciones de infraestructura) deben respaldarse al menos cada vez que hay cambios significativos o de forma continua mediante control de versiones. Idealmente, se utilizarán sistemas de versión distribuida (como Git) y además se generarán backups externos del repositorio de código de forma semanal o mensual para resguardo (por ejemplo, un dump/clone del repositorio guardado fuera de la plataforma principal).

Las copias de seguridad en Oracle Cloud se gestionan con políticas automatizadas desde la consola de Oracle Cloud Infrastructure (OCI), adaptadas a cada tipo de recurso. A continuación, se detalla la frecuencia y retención aplicadas:

Bases de datos Oracle Autónomas (sujeto a cambios normativos o técnicos por parte de Oracle):

- **Frecuencia:** Diaria (automática).
- **Tipos:** Full, incrementales y acumulativos.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Guía Institucional de Copias de Seguridad (Oracle Cloud y Microsoft 365)	CÓDIGO: G4_TIC
		VERSIÓN: 1
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 01/07/2025
		Página: 6 de 11

- **Retención:** 60 días por defecto. Se ha configurado retención extendida de 1 año para backups de largo plazo.
- **Almacenamiento:** Object Storage.

Bases de datos Oracle en DBSystem (sujeto a cambios normativos o técnicos por parte de Oracle):

- **Frecuencia:** Backups incrementales diarios.
- **Retención:** 65 días.
- **Almacenamiento:** Recovery Service (para producción) u Object Storage.
- **Extra:** Real-Time Data Protection con RPO cercano a cero.

Bases de datos MySQL DBsystem PaaS (sujeto a cambios normativos o técnicos por parte de Oracle):

- **Backups automáticos:** Diarios, con retención de 1 a 35 días (configurado a 15 días para los servicios productivos).
- **Backups manuales:** Hasta 365 días de retención, configurables desde consola o REST API.
- **Tipos:** Full e incrementales.
- Se tiene activo el point-in-time recovery el cual permite tener un RPO de aproximadamente 5 minutos para un DBsystem activo.

File Storage (sujeto a cambios normativos o técnicos por parte de Oracle):

- **Snapshots diarios** con retención de 7 días.
- **Almacenamiento:** Área oculta de solo lectura en el mismo sistema de archivos.

Block Volumes (Boot y Block) (sujeto a cambios normativos o técnicos por parte de Oracle):

- **Tipos:** Full o incremental.
- **Frecuencia y retención:** Definidas en políticas configuradas (pueden ser diarias, semanales, mensuales).
- **Backup manual y basado en políticas automatizadas.**

Retención:

- Todos los respaldos tienen una política de retención acorde a su criticidad y las capacidades institucionales. Para datos productivos correspondiente a block o boot storage, la retención típica será mantener backups diarios por 7 días, semanales por 4 semanas (1 mes) y mensuales por 12 meses (1 año). Este esquema asegura que ante una necesidad de restaurar versiones antiguas (por ejemplo, por detección tardía de corrupción de datos) se disponga de copias de hasta un año atrás.
- En Microsoft 365, la información almacenada en OneDrive permanece disponible por 30 días tras la inactivación del usuario. Para el buzón de correo (Exchange Online) este puede retenerse hasta 30 días, salvo que se aplique una política de retención extendida configurada

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Guía Institucional de Copias de Seguridad (Oracle Cloud y Microsoft 365)	CÓDIGO: G4_TIC
		VERSIÓN: 1
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 01/07/2025
		Página: 7 de 11

por la Subgerencia de Tecnologías de la Información y las Comunicaciones. En algunos casos, la información puede recuperarse hasta por 93 días, dependiendo del tipo de inactivación y de las políticas aplicadas por Microsoft.

5.3. **Restauración y Pruebas de Recuperación**

Los mecanismos de restauración disponibles en OCI permiten recuperar datos de forma granular o completa:

Restauración de bases de datos:

- **Oracle Autónomas:** Restauración directa o clonación desde la consola.
- **Oracle DBSystem:**
 - “Restore to latest”: para recuperación inmediata con mínimo RPO.
 - “Restore to a timestamp”: para recuperación a un punto anterior específico.
- **MySQL DBSystem:**
 - Point-in-time recovery (~5 minutos de RPO).
 - Restauración full o incremental.

Restauración de almacenamiento:

- **Block o Boot volumes:**
 - Opción de restaurar sobre nuevo volumen o reemplazar boot volume.
- **File Storage:**
 - Restauración desde snapshots o sincronización secundaria.

Pruebas de recuperación:

Se implementarán simulacros semestrales para asegurar:

- Validez de los backups.
- Documentación de tiempos de recuperación.
- Ajustes en políticas si se detectan desviaciones.

5.4. **Respaldo de Información en Microsoft 365**

La Agencia Distrital ATENEA reconoce la plataforma Microsoft 365 como un componente esencial para el desarrollo de sus actividades institucionales, facilitando la gestión del conocimiento, el trabajo colaborativo y la comunicación interna y externa. En este sentido, garantizar la protección, disponibilidad y acceso controlado a la información alojada en esta plataforma es una prioridad estratégica.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Guía Institucional de Copias de Seguridad (Oracle Cloud y Microsoft 365)	CÓDIGO: G4_TIC
		VERSIÓN: 1
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 01/07/2025
		Página: 8 de 11

Esta sección de la guía establece los lineamientos generales para la administración del respaldo, recuperación y acceso a la información contenida en los servicios de Microsoft 365, en conformidad con los principios de seguridad de la información y continuidad operativa.

Esquema General de Respaldo.

Microsoft 365 cuenta con mecanismos automáticos de retención y restauración integrados en la nube, los cuales no requieren intervención manual del usuario final, pero pueden ser gestionados por el equipo de Infraestructura de la Subgerencia de Tecnologías de la Información y las Comunicaciones, cuando así se requiera.

Características del respaldo en Microsoft 365:

- Retención por defecto de datos:
 - Outlook: Correos eliminados pueden recuperarse durante un periodo de hasta 30 días, dependiendo de la configuración aplicada por la entidad.
 - OneDrive y SharePoint: Archivos eliminados permanecen disponibles en la papelera de reciclaje durante un periodo de hasta 93 días.
 - Historial de versiones: Permite restaurar versiones anteriores de documentos si esta opción está habilitada.
- Opciones de recuperación administradas por Infraestructura TIC:
 - Restauración de archivos o correos eliminados (siempre y cuando no se supere el periodo de hasta 30 días).
 - Asignación de acceso delegado a cuentas activas.
 - Exportación de buzones completos.
 - Acceso temporal a carpetas de OneDrive o sitios de SharePoint con permiso de lectura.

Estas acciones están condicionadas por las capacidades técnicas de la plataforma, los períodos de retención vigentes, y requieren autorización expresa conforme a las políticas de privacidad y normativas legales aplicables.

Criterios para Solicitudes de Acceso o Recuperación.

El acceso a datos respaldados o la recuperación de información alojada en Microsoft 365 puede solicitarse en los siguientes escenarios:

- Cuentas activas: Cuando un usuario requiere recuperar información propia (en caso de eliminación se podrá recuperar dentro de un periodo de 30 días) o cuando una jefatura lo solicita con fines de supervisión, control o continuidad del servicio.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Guía Institucional de Copias de Seguridad (Oracle Cloud y Microsoft 365)	CÓDIGO: G4_TIC
		VERSIÓN: 1
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 01/07/2025
		Página: 9 de 11

- Cuentas inactivas: Cuando es necesario recuperar información de un colaborador cuyo vínculo con la entidad ha finalizado. Este acceso debe estar respaldado por un Jefe de Oficina, Supervisor, Gerente, Subgerente o Director General a través de un memorando suscrito o la solicitud a través de la aplicación de la mesa de ayuda y cumplir con los criterios legales y de conservación documental institucional.
- Solicitantes externos: Entes de control o instituciones públicas que, en ejercicio de funciones legales, soliciten acceso a información específica. En todos los casos, se deberá presentar una solicitud formal escrita y firmada. Esta será canalizada a través de la Oficina de Control Interno y verificada por la Subgerencia de Tecnología de la Información y las comunicaciones, en coordinación con la Dirección General o la Oficina Jurídica, para validar su competencia y procedencia.

Consideraciones en MS365.

- La disponibilidad de la información está sujeta a los tiempos de retención configurados en Microsoft 365, por lo cual se recomienda a los usuarios no depender únicamente de la papelera o versiones anteriores para la recuperación de información crítica.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones podrá implementar medidas adicionales de respaldo y contingencia, según evolución de los servicios y las necesidades de la entidad.

5.5. Copias de Seguridad en Oracle Cloud (Configuraciones Automatizadas)

OCI permite configurar políticas de backup con las siguientes características:

- **Tipo de backup:** Full o incremental.
- **Frecuencia:** Diaria, semanal, mensual, anual.
- **Retención:** Definida en días, semanas, meses o años.
- **Almacenamiento:** Cifrado en Object Storage.
- **Replicación:**
 - Automática entre ADs o FDs, según la configuración regional.
 - Manualmente replicable a otras regiones si se desea activar DRP.

Servicios sin respaldo nativo:

- **File Storage y Object Storage:** No admiten backups automatizados nativos. Se implementan soluciones alternas como:
 - Snapshots.
 - Instancia pivote con herramientas de terceros: rclone, restic.
 - Replicación entre regiones y file systems secundarios.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Guía Institucional de Copias de Seguridad (Oracle Cloud y Microsoft 365)	CÓDIGO: G4_TIC
		VERSIÓN: 1
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 01/07/2025
		Página: 10 de 11

5.6. **Roles y Responsabilidades**

Para la correcta ejecución y recuperación de los respaldos, se definen los siguientes actores clave:

Subgerencia de Tecnologías de la Información y las Comunicaciones.

- Configurar políticas de respaldo en OCI.
- Supervisar ejecuciones automáticas y verifica alertas.
- Coordinar procesos de restauración con usuarios o líderes de sistema.
- Establecer cronogramas de pruebas de recuperación.

Proveedor Oracle Cloud Infrastructure.

- Asegurar disponibilidad y rendimiento del servicio de backups.
- Mantener replicación y cifrado de datos.
- Ofrecer soporte en fallos y gestión de recuperación.

Profesional de la Subgerencia de Tecnologías de la Información y las Comunicaciones

- Validar integridad de datos recuperados.
- Solicitar restauraciones puntuales.
- Participar en pruebas de recuperación.

Profesional de Infraestructura de la Subgerencia de Tecnologías de la Información y las Comunicaciones

- Implementar respaldos para recursos sin política nativa.
- Manejar backups manuales.
- Documentar eventos de restauración.

Todos los involucrados deben documentar cada restauración y verificar la integridad posterior, dejando las evidencias correspondientes o a través del acta de reunión.

6. ANEXOS

No aplica

7. DOCUMENTOS DE REFERENCIA

- Política de Seguridad y Privacidad de la Información
- Manual de Políticas de Seguridad de la Información

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Guía Institucional de Copias de Seguridad (Oracle Cloud y Microsoft 365)	CÓDIGO: G4_TIC
		VERSIÓN: 1
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 01/07/2025
		Página: 11 de 11

8. RELACIÓN DE FORMATOS

CODIGO	NOMBRE DEL FORMATO
	No aplica

9. CONTROL DE CAMBIOS

Fecha (De la Versión del documento que se está actualizando)	Versión (Relacionar la última versión y código del documento que se está actualizando)	Descripción del Cambio

VALIDACIÓN	NOMBRE	CARGO	FECHA
Elaboró	Edwin Leon Martinez María Alejandra Suarez Jair David Calderín.	Contratista – Subgerencia de Tecnologías de la Información y las Comunicaciones	01/07/2025
Revisó	Juan Pablo Ceballos	Contratista – Subgerencia de Tecnologías de la Información y las Comunicaciones	01/07/2025
Aprobó	Carlos Andrés Ballesteros	Subgerente de Tecnologías de la Información y las Comunicaciones	01/07/2025

NOMBRE Y FIRMA DEL LÍDER DE PROCESO

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA