

COPIAS DE RESPALDO			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI02-POL04	09	1 de 5

1. INTRODUCCIÓN

Los presentes documentos desarrollan, precisan y operacionalizan la política general de seguridad y privacidad de la información, así como las políticas de seguridad de la información y de seguridad digital, las cuales fueron adoptadas por el Comité Institucional de Gestión y Desempeño (CIGD) en sesión celebrada el 10 de octubre de 2025, conforme a lo consignado en el Acta No. 10 de 2025.

2. OBJETIVO

Establecer los criterios y las responsabilidades para la realización de copias de seguridad diarias, semanales, mensuales, bimensuales, trimestrales, semestrales y anuales, de tipo total, incremental y diferencial. Su retención y protección se presenta con cifrado, segregación y pruebas de restauración verificables, de acuerdo con la criticidad del activo.

3. ALCANCE

Esta política aplica a todos los sistemas en sitio y nube (IaaS/PaaS/SaaS), bases de datos, Directorio Activo, Sistema de Nombres de Dominio - DNS, configuraciones de red, infraestructura, máquinas virtuales, repositorios de código, estaciones de trabajo, logs de seguridad y todos aquellos datos no estructurados que se hayan especificado en el inventario de activos. Cada activo tiene su propia criticidad alta, media o Baja, de acuerdo con su nivel de confidencialidad, integridad y disponibilidad.

4. DEFINICIONES

- **Copia total (full):** copia íntegra del conjunto de datos.
- **Copia incremental:** copia de cambios desde la última copia (full o incremental).
- **Copia diferencial:** copia de cambios desde la última copia full.
- **GFS (Abuelo-Padre-Hijo):** esquema de retención por niveles (diaria, semanal, mensual, bimensual, trimestral, semestral o anual).

5. GENERALIDADES

Hacer una copia de respaldo, se refiere a guardar información en un dispositivo de almacenamiento de tal forma que este pueda restaurar un sistema o grupo de archivos después de una pérdida o daño de información.

COPIAS DE RESPALDO			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI02-POL04	09	2 de 5

La copia de respaldo es útil por varias razones:

1. Para restaurar un dispositivo a un estado operacional después de un desastre natural o por intervención humana o artificial (copias de respaldo del sistema).
2. Para restaurar un pequeño número de archivos después de que hayan sido borrados o dañados accidentalmente (copias de respaldo de datos).

6. MEDIOS DE ALMACENAMIENTO

Las copias de respaldo de los componentes tecnológicos se realizan en medios o soportes de almacenamiento, garantizando la disponibilidad y recuperación de la información ante incidentes.

Se emplearán los siguientes tipos de almacenamiento según la plataforma:

Plataforma de Gestión: en discos magnéticos y de estado sólido de los sistemas de almacenamiento convergente e hiperconvergente, así como en la NAS dedicada a respaldo.

Plataforma Misional: en discos de estado sólido o flash y cintas magnéticas de alta capacidad, las cuales se rotan y envían a custodia externa.

Se prohíbe el uso de otros medios removibles (como memorias USB u otros dispositivos portátiles) ya que no están autorizados para la realización ni transporte de copias de respaldo.

El manejo, control, reutilización y disposición final de los medios se detalla en el documento GTI010-POL04 – Política para el uso de medios removibles, borrado seguro y disposición de medios.

7. ESQUEMAS DE RESPALDO

7.1. Plataforma de Gestión

Se implementa el esquema Abuelo–Padre–Hijo, con copias diarias, semanales, mensuales, bimensuales, trimestrales, semestrales o anuales, según la periodicidad definida por el GIT de Apoyo Informático.

COPIAS DE RESPALDO			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI02-POL04	09	3 de 5

Las copias se realizan sobre las plataformas convergente e hiperconvergente *onpremise* y se almacenan tanto en los repositorios primarios de backup como en una NAS dedicada a la gestión.

Adicionalmente, se realizan copias en nube (IaaS, PaaS, SaaS) a través de las directivas de copias de respaldo definidas por el GIT de Apoyo Informático para todos aquellos servidores configurados.

7.2. Plataforma Misional

Se ejecutan copias de respaldo diarias incrementales y full (*selective*) de los sistemas de archivos críticos (filesystem).

Las copias se almacenan en cintas magnéticas de alta capacidad, las cuales son rotadas y enviadas a custodia externa conforme al contrato vigente con el proveedor autorizado.

7.3. Usuarios finales y grupo de trabajo

La información del usuario es almacenada en el proveedor de nube con sus esquemas de replicación.

El usuario debe crear una carpeta con el nombre de usuario por ejemplo Imartinez, en donde guardará toda la información de índole laboral.

La información de uso compartido o colaborativo se almacena en la nube privada de la entidad y su copia de respaldo se realiza teniendo en cuenta el numeral 6.1.

7.4. Bóveda de contraseñas

Las copias de seguridad sobre la bóveda de contraseñas se realizan teniendo en cuenta el numeral 6.1.

8. RESTAURACIONES

Las restauraciones de los medios se pueden hacer en tres casos, a saber: 1. para verificar que las copias de seguridad están en perfecto estado y no tengan corrupción de su integridad, 2. por fallas en los servidores o filesystem en las diferentes plataformas o 3. por solicitud de los administradores del servicio o

COPIAS DE RESPALDO			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI02-POL04	09	4 de 5

servidor.

Para el caso de las verificaciones de las copias de seguridad, se deben realizar en un elemento de TI que no sea el mismo en el que se generó el backup de acuerdo con las siguientes recomendaciones:

- Para las copias de respaldo que se realizan con una periodicidad diaria, semanal, quincenal, mensual, bimensual, trimestral, semestral o anual, se realizarán las pruebas de recuperación de forma semestral.
- En caso de presentarse alguna falla en el servicio, servidor o *filesystem*, la restauración se realizará ejecutando las actividades necesarias para corregir la falla y cumpliendo los acuerdos de nivel de servicio establecidos en el catálogo de servicios.
- Se debe realizar restauración de la información de un usuario (planta o colaboradores) cuando se requiera, a través de la respectiva solicitud a mesa de servicio, autorizada por el correspondiente coordinador.

9. UBICACIÓN Y ALMACENAMIENTO

El almacenamiento de las copias de respaldo se realizará en medios como cintas, discos magnéticos de estados sólido o flash, asegurando la protección, trazabilidad y disponibilidad de la información respaldada.

Plataforma de Gestión

- Las copias de respaldo se deben almacenar en la **NAS de gestión**.
- Este repositorio actúa como almacenamiento para las copias del esquema **abuelo-padre-hijo**, asegurando la segregación entre los datos de producción y las copias de respaldo.
- El acceso a la NAS se restringe únicamente al personal autorizado del GIT de Apoyo Informático.
- Para los servidores que están en IaaS, las copias de respaldo reposan en almacenamiento dispuesto por el proveedor del servicio de nube.

Plataforma Misional

- Las copias de respaldo se realizan en **cintas magnéticas** y se registran en el documento Inventario Cintas.
- Posteriormente, las cintas se **envían a custodia externa certificada**, conforme al contrato vigente con el proveedor.
- La custodia externa debe asegurar las condiciones de **seguridad física**,

COPIAS DE RESPALDO			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI02-POL04	09	5 de 5

control ambiental, registro de acceso y trazabilidad completa de los movimientos de los medios hasta su retorno o reemplazo.

10. Retención de copias

En la plataforma de gestión se retienen tres copias de respaldo (Abuelo, Padre, Hijo) según la periodicidad (diaria, semanal, quincenal, mensual, bimensual, trimestral, semestral y anual) presentada en el cronograma realizado por el GIT de Apoyo Informático.

En la plataforma misional se retienen tres copias de respaldo de los file system de manera incremental y selectiva (full) según la periodicidad (diaria o semanal), reteniéndose por un periodo hasta de 60 días. La programación se establece en el cronograma de políticas de la plataforma misional.

Para las bases de datos de producción está definida una tarea diaria, programada para realizar backup de nivel 0, mediante un scrip que se realiza en crond.

Esta información es almacenada en la herramienta de copia de respaldo misional diariamente en la programación configurada y se envía a custodia la cinta de respaldo semanalmente.

Elaboró: Martha Zornosa Guerra

Revisó: Anuar Vargas Calderón e integrantes del EAOS

Aprobó: Freddy Castaño Pineda