
	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

## LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN DE BASES DE DATOS

**SECRETARÍA GENERAL**

**EQUIPO DE INFRAESTRUCTURA Y SOPORTE TECNOLÓGICO**

**ABRIL 2026**

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

## INTRODUCCIÓN

La Agencia Nacional de Tierras ha determinado la necesidad de contar con una política de respaldo, almacenamiento y recuperación de la información de bases de datos, que garantice la disponibilidad e integridad de los activos informáticos dispuestos en toda la infraestructura de la Agencia Nacional de Tierras.

El presente documento describe las políticas de copias de respaldo de información de bases de datos y su almacenamiento, junto con las políticas y mecanismos para la realización de las actividades relacionadas, con el fin de apoyar a los administradores de servicios de tecnología a reducir los impactos de los riesgos generados por fallas en la prestación de servicios internos y externos de la entidad que involucren la pérdida total o parcial de información.

Este documento es propiedad de la Agencia Nacional de Tierras – ANT; toda la información contenida aquí deberá mantenerse en forma estricta y confidencial.

Está prohibido realizar copias y/o reproducir parcial o totalmente este documento sin autorización.

## OBJETIVO

Definir los lineamientos generales aplicables para el respaldo, custodia y recuperación de información de las bases de datos en la Agencia Nacional de Tierras.

## ALCANCE

Esta política aplica a todos los sistemas de información y dispositivos de almacenamiento de datos que contengan información catalogada como crítica para la prestación de servicios internos y externos de la Agencia Nacional de Tierras, alojada en servidores on-premise o cloud.


La presente política es de obligatorio cumplimiento para todo el personal que, de manera permanente o eventual, sea responsable de administrar, liderar, gestionar e interactuar con la infraestructura tecnológica y/o que tenga cualquier relación con información de la entidad, incluidos terceros.

Todo el personal involucrado debe manifestar expresamente el conocimiento de su contenido y alcance, y solicitar los cambios pertinentes toda vez que sea necesario.

## NORMATIVIDAD

El presente documento se basa en las buenas prácticas, leyes y normas relacionadas con la seguridad de la información:

**Ley 1273 de 2009** – De La Protección de la Información y de los Datos

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

**Ley 594 de 2000.** Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones

**Ley General de Archivos Decreto 1080 de 2015.**

**ISO/IEC 27002:2005** – Código para la Práctica de la Gestión de la Seguridad de la Información

**ISO 30301: 2011** Sistema de Gestión de Registros Política de Gestión Documental de la Agencia.

**ISO 22301:2012** – Seguridad de la Sociedad: Sistemas de Continuidad del Negocio

**ISO/IEC 27001:2013** – Sistemas de Gestión de Seguridad de la Información (SGSI)

La Norma Técnica Colombiana NTC- ISO: 9001.

Decreto Único del Sector Cultura.

## DEFINICIONES

**ACUERDO DE NIVEL DE SERVICIO (ANS):** Convenio entre un proveedor de servicios de TI y un cliente. Describe las características del servicio de TI, los niveles de cumplimiento (tiempos máximos los cuales se definen en conjunto) y las sanciones, y especifica las responsabilidades del proveedor y del cliente. Un ANS puede cubrir múltiples servicios de TI o múltiples clientes.

**AGENTE:** Servicio del sistema operativo que ejecuta tareas administrativas programas de la base de datos, denominados trabajos (jobs).


**ANT:** Agencia Nacional de Tierras.

**ARQUITECTURA EMPRESARIAL:** Es una práctica estratégica (una capacidad), que consiste en analizar integralmente las empresas desde diferentes perspectivas o dimensiones (el negocio, la información, las aplicaciones, la infraestructura, entre otras), con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria para alcanzar un estado deseado. El objetivo es generar valor a las compañías a través de las Tecnologías para que se ayude a materializar la visión y/o los objetivos de negocio de la organización.

**BACKUP / COPIA DE SEGURIDAD:** Respaldo de archivos o datos contenidos en un sistema informático y que son considerados como críticos para la operación de los servicios, copia de respaldo alternativa al almacenamiento original.

**BACKUP SERVER:** Es un tipo de servidor que tiene mucha capacidad de almacenamiento en discos duros (u otros medios) disponible para ser usado con el propósito de almacenar copias de seguridad de la información de base de datos, aplicaciones, imágenes de equipos de cómputo o archivos en general.

**BD:** Base(s) de Datos.

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

**CLOUD:** Recurso de procesamiento y almacenamiento provistos por un tercero especializado, facturados según consumo.

**COPIA DE SEGURIDAD COMPLETA (FULL):** Una copia de seguridad que incluye la totalidad de la información de la(s) base(s) de datos que conforman un sistema de información y que no requieren elementos de datos adicionales para su recuperación.

**COPIA DE SEGURIDAD INCREMENTAL:** Una copia de seguridad que respalda los archivos creados o modificados de una base de datos desde la última copia de seguridad completa (full). La restauración de los datos debe realizarse con la última copia de seguridad completa y las copias de seguridad incrementales posteriores.

**COPIA DE SEGURIDAD EN FRÍO:** Copia de información de los archivos de las bases de datos, sin que esta esté disponible para los usuarios.

**COPIA PROGRAMADA:** Copia de información que se encuentra planificada con anterioridad a su ejecución, se realiza de forma automática y puede ser almacenada en diversos medios de respaldo.

**DGOSP:** Dirección de Gestión del Ordenamiento Social de la Propiedad.

**ELEMENTO DE CONFIGURACIÓN:** Cualquier componente que se requiera gestionar para entregar un servicio de TI, ya sea un elemento lógico o físico, que se conjuga con otros para soportar un servicio.

**FILE SERVER:** El servidor de archivos (file server) es un equipo adjunto a una red que proporciona una ubicación para el acceso compartido de archivos, es decir, el almacenamiento compartido de archivos de ordenador (tal como texto, imagen, sonido, video) al que se puede tener acceso desde las estaciones de trabajo que pueden alcanzar el equipo que comparte el acceso.

**HARDWARE Y SOFTWARE:** comprende toda la dotación y administración de inventarios de los equipos de cómputo, servidores, impresoras, escáneres, audiovisuales, así como el software requerido para su operación, necesarios para que la organización cuente con los recursos tecnológicos para desarrollar las actividades administrativas.


**IMPACTO:** Resultado de la evaluación de una consecuencia.

**IMPACTO DEL CAMBIO:** medición del efecto de implementar un cambio sobre los procesos de negocio o demás elementos de configuración de la infraestructura tecnológica.

**INCIDENTE:** interrupción no planeada de un servicio de TI, o la reducción en la calidad de un servicio de TI. También se considera como incidente la falla de un elemento de TI que aún no ha afectado el servicio.

**INFRAESTRUCTURA TECNOLÓGICA:** software, hardware, redes y telecomunicaciones que hacen parte del ecosistema tecnológico de la Agencia Nacional de Tierras, en detalle lo pueden componer servidores, equipos de redes y comunicaciones, sistemas de almacenamiento, seguridad y backup, licenciamiento de software de datacenter, entre otros elementos.

**JOB:** Es un proceso automático, propio de la base de datos, que se ejecuta previo a una programación establecida.

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

**LÍDER DE PROCESO:** Responsable de la conducción operativa de un proceso y de la ejecución de las actividades, métodos y documentos que rigen y se generan dentro del mismo; garante del seguimiento, medición, análisis y mejora de este.

**LÍDERES DE PROCESOS DE LA SSIT:** Toda persona adscrita a la Subdirección de Sistemas de Información de Tierras (SSIT) de la ANT que tiene a cargo la administración de Tecnologías de la Información y las Comunicaciones tales como: aplicaciones (misionales y/o de apoyo), sistemas de información, servidores, bases de datos, redes y todo aquello que involucre información relacionada con la operación de la entidad en el cumplimiento de sus objetivos mediante herramientas tecnológicas.

**LOGS:** Reporte con registros de los eventos de hardware, software operativo o aplicativo.

**MinTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

**NORMATIVIDAD:** Leyes, decretos y demás desarrollos normativos que guían las acciones para implementar el Marco de Referencia de AE para la gestión de TI.

**ON-PREMISE:** Alojada en el centro de datos de la ANT.

**PETI:** Plan Estratégico de Tecnología de Información.

**PROBLEMA:** Es un incidente recurrente o mayor que requiere un tratamiento especial para encontrar la causa raíz y plantear una solución temporal o definitiva del mismo.

**RECUPERACIÓN:** Hace referencia a las técnicas empleadas para recuperar la información (archivos) a partir de una copia de seguridad (medio externo); esto se aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers.

**SERVICIO TECNOLÓGICO:** Conjunto de actividades que buscan responder a las necesidades de un cliente por medio de un cambio de condición en los bienes informáticos (llámese activos), potenciando el valor de estos y reduciendo el riesgo inherente del sistema.

**SGEN:** Secretaría General.


**SISTEMAS DE INFORMACIÓN:** Medios de almacenamiento y procesamiento de los datos de la entidad y que ofrecen algún servicio tecnológico específico.

**SSIT:** Subdirección de Sistemas de Información de Tierras

**STORAGE SERVER:** El servidor de almacenamiento es un tipo de servidor que se utiliza para almacenar, acceder, asegurar y administrar datos digitales, archivos y servicios. Se trata de un servidor utilizado para almacenar y tener acceso a una cantidad grande de datos en una red compartida o en Internet.

**TAREAS DE RESPALDO:** Programación de las copias de seguridad que incluyen: la fuente, el destino y la periodicidad.

**TIC:** Tecnologías de la Información y las Comunicaciones.

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

## 1. DISPOSICIONES GENERALES

### 1.1 Frecuencia de actualización de los lineamientos

Los lineamientos tendrán una revisión de actualización semestral o anual (dependiendo de las decisiones tomadas en el comité de arquitectura, mesa técnica o quien haga sus veces), de igual forma, se revisarán cuando hayan surgido actualizaciones o cambios significantes a los procesos, procedimientos, servicios tecnológicos, sistemas de información, leyes o normatividad aplicable.

### 1.2 Generalidades de los procesos de Backup


Es responsabilidad de los líderes de procesos y jefes de dependencias, garantizar que la información institucional catalogada como crítica en el inventario de activos de información, es decir: “aquella necesaria para mantener operativos los procesos de la entidad”, sea almacenada en los servidores de la entidad on-premise o cloud.

Cada respaldo que se realice deberá quedar registrado en los LOGS de los servidores y en un archivo electrónico (Texto, Planilla, etc.) en las carpetas de lectura pública de tal forma de habilitarlos a las áreas encargadas e interesadas.

Cada respaldo deberá quedar registrado en la máquina donde son realizados (logs de servidor) y en un archivo externo (texto, planilla, etc.) que permita dejarlo disponible para controles o auditoría.

Por ningún motivo se permite alojar en servidores de la entidad información catalogada como personal, música, videos, documentos transitorios, documentos confidenciales personales, backups de equipos de escritorio, backups de correo electrónico y demás que no sea relevante en el cumplimiento de los objetivos de la Entidad.

1. El encargado de los respaldos (Equipo de Infraestructura y Soporte tecnológico) es el responsable de documentar todas las actividades relacionadas con los respaldos de información.
2. Mensualmente debe ser [ilegible] un informe por parte del Equipo de Infraestructura con el [ilegible] los respaldos del mes e indicando la información que fue respaldada.
3. Las claves de usuario de bases de datos NO serán respaldadas.
4. Los respaldos de las bases de datos se realizarán en el período establecido y en el medio de almacenamiento definido por la entidad. El tiempo será detallado en el documento más adelante; se realizará según las características de la base de datos y se realizará en el medio alternativo dispuesto por la Agencia (SAN, centro de datos, cloud, etc.); se iniciará desde la fecha de implementación del nuevo sistema de respaldo.
5. El subdirector y los líderes de procesos de la SSIT – Subdirección de Sistemas de Información de Tierras, son los únicos autorizados para solicitar el respaldo y/o recuperación de información a través de la Mesa de Servicio, mediante el formato dispuesto para tal fin, indicando los datos del solicitante, datos de la aplicación, datos de los archivos (tipo y ubicación), datos de la BD (ubicación, motor y versión), accesos, periodicidad del respaldo y tipo de respaldo. Siempre que exista alguna modificación o adición en la fuente de la información, se debe generar el formato descrito y entregarlo al responsable del Equipo de Infraestructura y Soporte Tecnológico.

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

### 1.3 Copias de Respaldo

Toda la información de la ANT del ámbito prioritario definida en las tablas de retención documental (TDR) será periódicamente respaldada en soportes de *backup*.

Las copias de respaldo deben abarcar toda la información necesaria para recuperar el servicio en caso de corrupción (daño de la información) o pérdida de la información. Tal información puede incluir datos, programas, ficheros de configuración e incluso la imagen del sistema operativo.

#### 1.3.1 Tipos de Copias de Respaldo

Tabla 1. Tipos de Copias de Respaldo

<b>Completa (full):</b>	Se efectúa una copia de seguridad completa de todos los ficheros y bases de datos. Puede consumir bastante tiempo si el volumen de datos a salvaguardar es elevado. La ventaja derivada de este tipo de copia es que se tiene la seguridad de tener una imagen completa de los datos en el momento de la salvaguarda.
<b>Incremental</b>	Se copian los datos modificados desde la anterior copia incremental. Siempre se debe partir de una salvaguarda completa inicial. Si se realiza con frecuencia, el proceso no consumirá un tiempo excesivo, debido al bajo volumen de datos a copiar. Por el contrario, la restauración es lenta, toda vez que requiere restaurar una copia completa y todas las copias incrementales posteriores realizadas hasta el momento al que se quiera restaurar el sistema.
<b>Diferencial</b>	Se copian los datos modificados desde la anterior copia completa. La restauración se hace a partir de una salvaguarda completa inicial.
<b>LOG</b>	Se realizan copias del log de la base de datos, el cual es un registro de cada operación que se realiza sobre la base de datos.


## 2. LINEAMIENTOS PARA LA GENERACIÓN DE BACKUP DE BASE DE DATOS

Para la realización de los backups de base de datos se tendrán en cuenta tres factores principales:

- La transaccionalidad de la base de datos.
- La necesidad de restablecer la información al menor tiempo posible.
- El análisis de volumetría de crecimiento de la data.

Estos se tomarán en cuenta para establecer su configuración y la política de backup que corresponda. Estos lineamientos toman como base las recomendaciones para bases de datos SQL Server que son las principales en la ANT, pero aplican a la mayoría de las arquitecturas de motores de bases de datos relacionales.

Los lineamientos para la toma de backup según estos 3 factores se especifican a continuación.

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

## 2.1 Backup Ambientes Productivos:

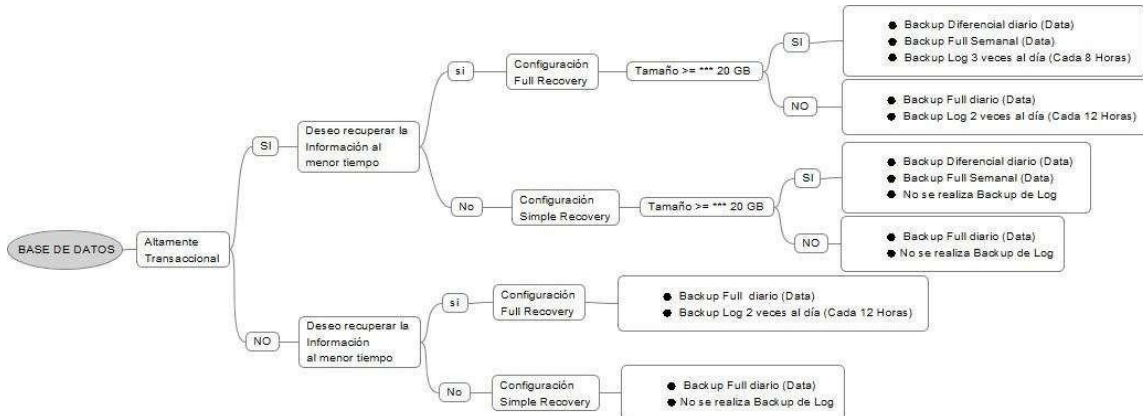


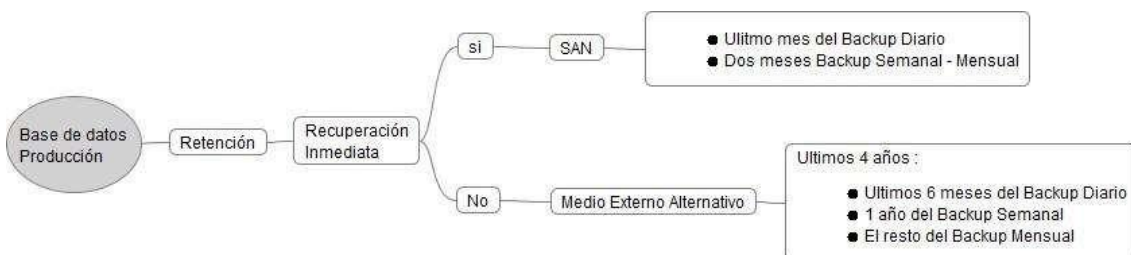
Ilustración 1. Esquema de Backup Ambientes Productivos

\*\*\* El tamaño indicado en el esquema es sugerido; la decisión de la toma de los **backups** está supeditada al incremento de la base de datos y a la disponibilidad de espacio.

Como se indica en el esquema, según su transaccionalidad, su configuración, tamaño y necesidades, se indica la frecuencia del *backup*, qué tipo de *backup* y a qué sistema de archivos le debemos realizar las copias de respaldo.

## 2.2 Retención Backup Ambientes Productivos:

Para la retención y almacenamiento de los **backups** en ambientes productivos, se definen según el siguiente esquema.




\*El tiempo de Retención puede ser modificado según la información respaldada y la tecnología utilizada

Ilustración 2. Esquema de Retención Backup Ambientes Productivos

El tiempo de Retención puede ser modificado según la información respaldada y la tecnología utilizada.

Cada vez que se realiza una copia de seguridad, se debe realizar un proceso de integridad; para verificar el correcto estado del *backup*, también se recomienda realizar una comprobación de los *backups* que estén almacenados en el medio externo alternativo **una vez cada 3 meses**, dependiendo de su **período** de retención

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

### 2.3 Backup y Retención de Ambientes de Desarrollo y Pruebas:

Para los ambientes de desarrollo y pruebas, los lineamientos de *backup* y de retención de estos se definen a continuación:

*El tiempo de retención puede ser modificado según la información respaldada, los recursos existentes y la tecnología utilizada.*

Se debe realizar una comprobación de los *backups* que estén almacenados una vez por mes.

### 2.4 Proceso de Backup en la Base de Datos.

Los *backups* de las bases de datos se deben generar a través de *jobs* o agentes del motor de base de datos. Los *backups* de cada instancia se almacenarán en el servidor donde se encuentre instalado, en el disco o donde se haya especificado; se debe tener en cuenta los lineamientos y buenas prácticas de Bases de Datos de la ANT.

La estructura de nombres del *job* debe describir la base de datos a la cual se le está tomando el *backup* y el tipo de copia de seguridad que se extrae; este tipo de *backup* se define de acuerdo con los lineamientos establecidos anteriormente según la configuración que se tenga de la base de datos y el ambiente de la aplicación.

#### Nombres de objetos de Jobs y Archivo de Backup

- **JOB:** Los nombres de Job deben ser en mayúsculas siguiendo la siguiente estructura <Nombre Base de Datos>\_<Tipo de Backup> separando las palabras por el símbolo “\_”. Si se considera necesario y el backup se realiza solo una vez al día, incluir el horario, por ejemplo:
  - BAL\_EDP\_FULL\_1430.
  - BAL\_EDP\_DIF.
  - BAL\_RESTITUCIÓN\_LOG.
- **ARCHIVOS:** Los nombres de los archivos deben ser en mayúsculas siguiendo la siguiente estructura <Nombre Base de Datos>\_<Tipo de Backup>\_<Fecha\_Hora> separando las palabras por el símbolo “\_”, por ejemplo:
  - BAL\_EDP\_FULL\_20180227\_1653.bak
  - BAL\_EDP\_DIF\_20180227\_1653.bak
  - BAL\_RESTITUCION\_LOG\_20180227\_16.bak \*\*\*

**Para el caso de los LOGs solamente se le colocará la hora al final y no horas/minutos.**


Los backups de una base de datos que solo tengan un esquema de backup full no se les especificará el tipo de backup (diferencial, incremental o full); se realizará de la siguiente manera:

- BAL\_EDP\_20180227\_1653.bak

Los backups de tipo Log solo se sobrescribirán siempre y cuando se tenga un backup ya sea diferencial o full anterior al último backup del Log; solo se tendrán los backup con una retención máxima de un día.

#### Tiempo de programación de Jobs y Archivo de Backup

El tiempo de programación se ajustará de acuerdo con la malla de ejecución de los **backups** detallada en el formato definido para el registro de backup a bases de datos y aplicaciones.

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

### Infraestructura de almacenamiento de backup de base de datos

Para el almacenamiento de los **backups** se propone la siguiente infraestructura; se pretende tener un esquema de almacenamiento por fases:

- **Primera fase:** el almacenamiento se realizará en la misma unidad del servidor (virtual o físico), para tener la manera de restauración y recuperación de la base de datos inmediata.
- **Segunda fase:** si es un servidor de tipo físico, se realizará en una unidad aparte expuesta como una unidad de red en el **file server** o en un servidor utilizado como **backup server** o **storage server**, donde se permita almacenar los archivos de backup con un período de retención mayor, según los lineamientos expuestos anteriormente. Se debe configurar un agente o, a través de la herramienta de **ETL**, pasar los archivos de backup a este repositorio. Si el servidor es de tipo virtual, se deberá pasar al almacenamiento externo alternativo que disponga la Agencia, según el procedimiento indicado.
- **Tercera fase** (*segunda si el servidor es de tipo virtualizado y en la misma SAN*): pasar el almacenamiento desde el servidor de backup o **file server** al externo alternativo que disponga la Agencia (nube, centro altemo de datos), según la política de retención ya mencionada. Esta labor se debe realizar posterior a la terminación de la totalidad de los backups del servidor, con el fin de que la totalidad de los backups hayan terminado.

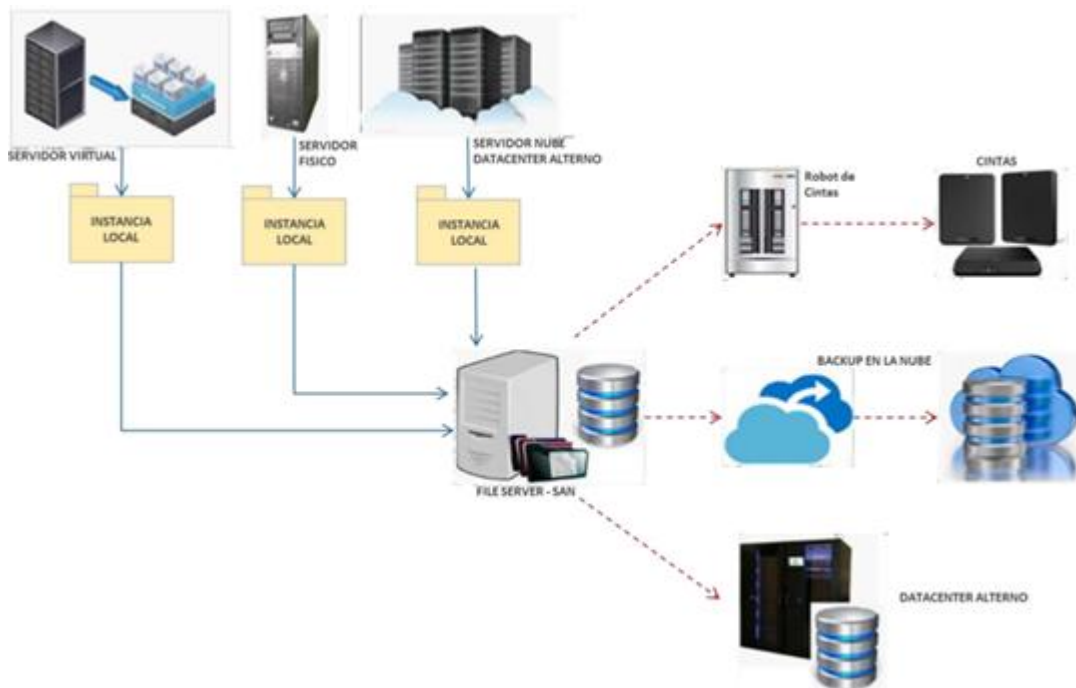



Ilustración 3. Infraestructura de almacenamiento de backup de base de datos

La línea punteada indica que se puede utilizar diferentes alternativas según la disposición de recursos de la Agencia.

### Esquema de almacenamiento de Backup de bases de datos.

La estructura que se debe tener para el almacenamiento de los **backups** debe seguir los siguientes lineamientos, ya sea si en el servidor se tienen dos o más instancias y según el tipo de **backup** que se estén tomando de las

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

bases de datos; ver el documento de **LINEAMIENTOS Y BUENAS PRÁCTICAS DE BASES DE DATOS** para el nombramiento de las instancias:

La ruta de los archivos para los **Backup** sería la siguiente:

E:\ BACKUP \ <NOMBRE DE INSTANCIA> \ (Si existen más de una instancia) \  
E:\ BACKUP \ (Si solo se tiene una instancia) \

Dentro de la carpeta de las instancias o de backup, según lo visto anteriormente, tendríamos dos carpetas así:

- **DIARIO (Producción)**
- **QUINCENAL (Pruebas y Desarrollo)**
- **HISTÓRICO (Producción, Pruebas y Desarrollo)**

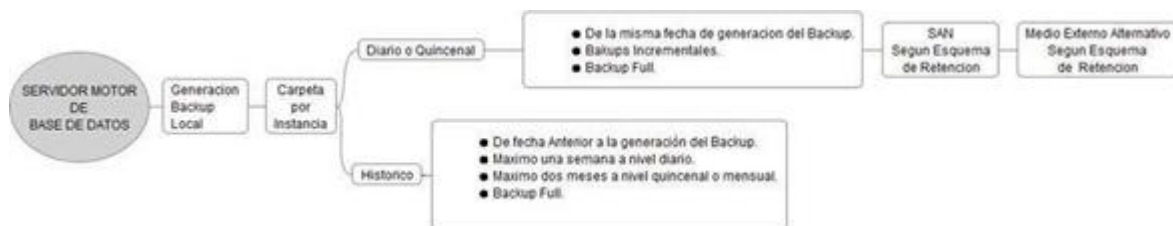
Dentro de la carpeta de diario se crearían 3 subcarpetas:

- **TOTAL:** Backup Full.
- **DIFERENCIAL:** Backups diferenciales. \*\*\*
- **LOG:** Backup Log. \*\*\*

*Los ambientes de Pruebas y Desarrollo no tienen backup diferencial ni log.*

Para los servidores que manejan backups diferenciales y completos, se define crear backups completos con una periodicidad no mayor a 7 días. Los backups totales se determinara el mejor esquema de retención.

A estas carpetas irán los backups según su generación y tipo, siguiendo el siguiente esquema.




*Ilustración 4. Esquema de almacenamiento de backup de bases de datos*

De acuerdo con el anterior esquema, en la carpeta Diario o Quincenal solo se tendrán los backups, tanto diferenciales como full, de la misma fecha de generación; es decir, no habrá archivos de backup con fecha del día anterior a su generación.

Todos los archivos de la carpeta Diario o Quincenal se copiarán a la SAN (file server, backup server o dispositivo que la entidad disponga) y se mantendrán o se pasarán al medio de almacenamiento alternativo externo de acuerdo con las políticas de retención, vistas en los numerales anteriores de retención de backup de este documento.

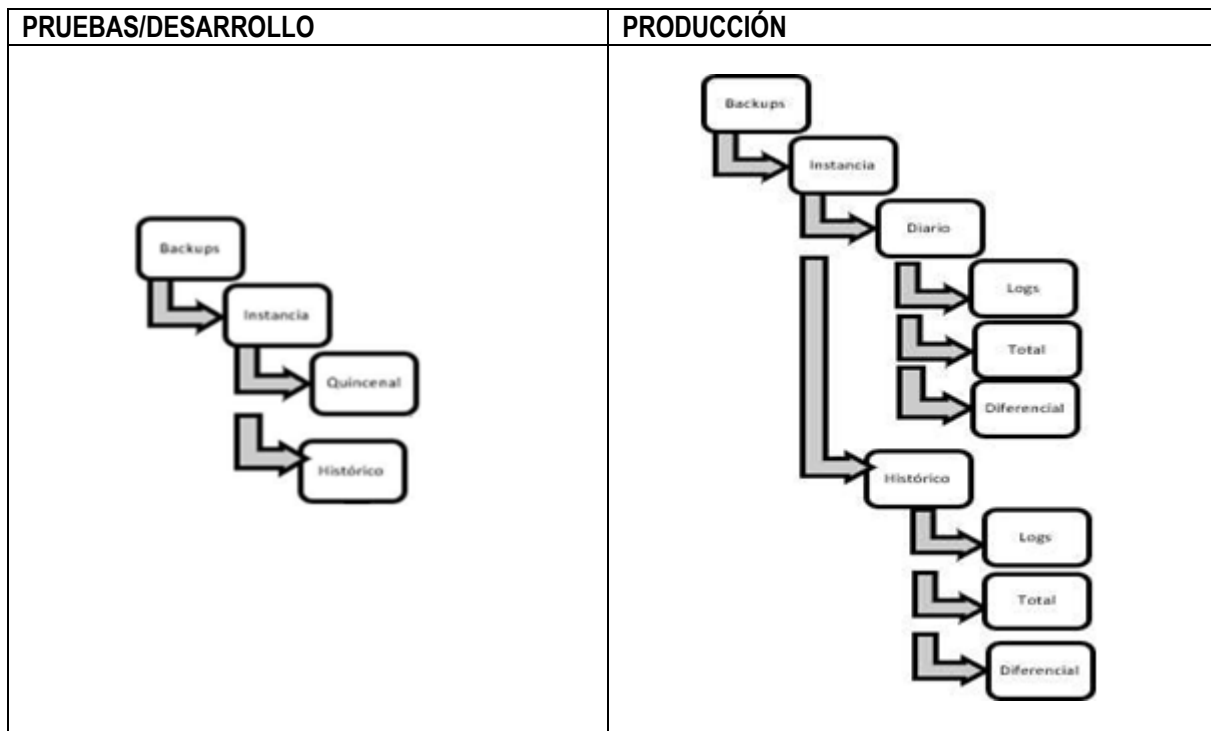
Una vez el archivo tenga un tiempo de generación mayor a un día, se deben mover a la carpeta Histórico, donde se mantendrán según el tipo de backup con un período no mayor a una semana (backup diario) o 2 meses (backup semanal o mensual).

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

En la carpeta Histórico, en el ambiente de pruebas o desarrollo, no debe haber más de una copia de seguridad de una misma base de datos y, cuando se realicen diferenciales de la misma base de datos, se eliminarán los archivos de backup que no cumplan con el tiempo de retención mencionado.

### Estructura de folders para los Backup

Tabla 2. Esquema de Carpetas Backup.




Para ver **cómo** se realiza el proceso a detalle de toma de los backups y su posterior restauración, se debe revisar el procedimiento definido para **backup** de bases de datos.

### 3. ADMINISTRACIÓN Y CUSTODIA DE LOS BACKUPS

La custodia y administración de los **backups** estarán a cargo del área de soporte tecnológico y/o el proveedor que la ANT designe para tal función; los tiempos de restauración estarán concertados entre el Equipo de Infraestructura y Soporte Tecnológico y la Subdirección de Sistemas de Información.

Los cambios de programaciones ya existentes deben ser realizados por el Equipo de Infraestructura y Soporte Tecnológico basándose en los lineamientos definidos en este documento. Adicionalmente, la creación de tareas de **backup** nuevas la realizará el Equipo de Infraestructura y Soporte Tecnológico a partir de solicitud previa de la Subdirección de Sistemas de Información.

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

### 3.1 Análisis sistema de backup actual para plan de contingencia

**Leve:** Pérdida por daño de la base de datos, falla eléctrica o física de disco; se mantienen copias de seguridad locales.

**Grave:** Pérdida de información por daño grave del servidor, cortocircuito, incendios, inundación, local del centro de cómputo; se mantienen copias de seguridad locales.

**Catastrófica:** Pérdida de información por daño grave del o de los servidores, cortocircuito, incendios, inundación, en todas las instalaciones de la ANT, o por daño total que no permita la recuperación de copias de seguridad locales, como es el caso de terremotos.

## 4. ROLES Y RESPONSABILIDADES


Las responsabilidades personales derivadas de las actividades descritas en el presente Lineamiento son las siguientes:

*Tabla 3 Roles y Responsabilidades*

<b>Roles</b>	<b>Responsabilidades</b>
<b>Personal del Equipo de Infraestructura y Soporte Tecnológico de la Secretaría General.</b>	Gestionar las copias de respaldo de los activos recogidos en el alcance de la Política y lineamiento, siguiendo las directrices previamente señaladas.
<b>Equipo Mesa Técnica.</b>	Aprobar el contenido y cambios de la política.
<b>Responsable del Equipo de Infraestructura y Soporte Tecnológico de la Secretaría General.</b>	Custodiar los soportes de almacenamiento extraíbles donde se almacenan las copias de respaldo de la ANT.
	Garantizar la correcta ejecución de las operaciones periódicas de copias de respaldo.
	Ejecutar las comprobaciones periódicas de las políticas de restauración de la ANT.
<b>Responsables de los Activos de Información. (Líderes de proceso y jefes de área)</b>	Tramitar, a través de la SSIT, las solicitudes de inclusión de activos en la(s) copia(s) de respaldo.
	Canalizar, a través de la SSIT, las solicitudes de recuperación de activos alterados, dañados o destruidos desde la realización de la(s) copia(s) de respaldo.
	Validar las operaciones de restauración de activos de información, gestionados por el personal de la SSIT
<b>Líder de Infraestructura tecnológica de la Secretaría General.</b>	Aprobar las solicitudes de inclusión de activos en la(s) copia(s) de respaldo solicitadas por los responsables de los Activos (SSIT).
	Aprobar las solicitudes de recuperación de activos a partir de copias de respaldo, solicitadas por los responsables de los Activos (SSIT).

## 5. GESTIÓN DE SOPORTES

Las herramientas de gestión de copias de respaldo de la ANT contarán con una librería de soportes que permita la inserción de múltiples volúmenes para facilitar la gestión automatizada de las operaciones.

	<b>POLÍTICA</b>	<b>LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN.</b>	<b>CÓDIGO</b>	GINFO-Política-020
	<b>ACTIVIDAD</b>	ADMINISTRACIÓN Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA, BASES DE DATOS, SERVICIOS TIC Y SEGURIDAD INFORMÁTICA	<b>VERSIÓN</b>	2
	<b>PROCESO</b>	GESTIÓN DE LA INFORMACIÓN	<b>FECHA</b>	12/05/2026

Estos soportes se insertarán antes de una operación de copia y se retirarán para su almacenamiento, tras la verificación de esta.

## 6. RECUPERACIÓN DE ACTIVOS A PARTIR DE COPIAS DE RESPALDO

### 6.1 Solicitud de recuperación de activos

La operación de recuperación de activos a partir de copias de respaldo se iniciará a petición del responsable del activo y deberá ser previamente aprobada por el jefe del área solicitante competente.

Para solicitar una recuperación, el responsable del activo creará una solicitud en la Mesa de Servicios de la ANT, a la que adjuntará el formato definido para la solicitud de respaldo y restauración de información.

HISTORIAL DE CAMBIOS		
Fecha	Versión	Descripción
27/03/2020	01	Primera versión del documento
08/05/2026	02	Segunda versión, se actualiza contenido y lineamientos acordes al estado actual de la entidad, cambia formato y se actualiza versión.

APROBACIÓN				
	NOMBRE	CARGO	FIRMA	FECHA
<b>ELABORÓ</b>	John Edinson Camacho Romero	Contratista – Subdirección Sistemas de Información de Tierras	<b>ORIGINAL FIRMADO</b>	14/11/2025
<b>REVISÓ</b>	Roberto Andrés Zabala Barrera	Contratista – Secretaría General	<b>ORIGINAL FIRMADO</b>	14/12/2025
<b>APROBÓ</b>	Angela Lorena Ortiz Rosero	Secretaría general	<b>ORIGINAL FIRMADO</b>	08/05/2026

*La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia.*

*La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.*