Aguas del Cesar
S.A. E.S.P.

# PROTOCOLO COPIAS DE SEGURIDAD - MSPI

| | |
|---|---|
| Nombre completo de la entidad | Aguas del Cesar S.A E.S.P |
| NIT | 900.149.163-8 |
| Municipio / Departamento | Valledupar, Cesar |
| Dirección sede principal | Calle 28 Nº 6A – 15 |
| Sitio web | https://aguasdelcesar.gov.co/ |
| Correo de contacto TIC | sistemas@aguasdelcesar.com.co |

Contenido

## 1. INTRODUCCIÓN

El presente documento establece la Política y el Plan de Generación de Copias de Respaldo (Backup) de **Aguas del Cesar S.A. E.S.P.**, con fundamento en las mejores prácticas internacionales (ISO/IEC 27001:2022, ITIL, GEL) y el marco normativo colombiano aplicable a entidades públicas.

Su propósito es garantizar la disponibilidad, integridad y confidencialidad de los activos de información institucionales mediante estrategias de respaldo, recuperación y custodia, de modo que la entidad pueda restablecer su operación ante cualquier incidente de seguridad, falla técnica o desastre.

## 2. OBJETIVO

### 2.1 Objetivo General

Definir los lineamientos, procedimientos y responsabilidades para la generación, almacenamiento, verificación y restauración de copias de respaldo de los activos de información de **Aguas del Cesar S.A. E.S.P.**, en cumplimiento de la normativa vigente y las políticas de Seguridad de la Información.

### 2.2 Objetivos Específicos

- Establecer un modelo operativo estándar para las copias de seguridad.
- Definir los tipos de backup, periodicidades y tiempos de retención según criticidad del activo.
- Fijar criterios de etiquetado, almacenamiento y custodia de medios.
- Garantizar la realización periódica de pruebas de restauración.
- Asignar roles y responsabilidades mediante la Matriz RACI.
- Cumplir con los lineamientos de la estrategia de Gobierno en Línea GEL, la Política de Seguridad Digital y el MSPI del MinTIC.

## 3. ALCANCE

El presente documento aplica a todos los activos de información administrados bajo la infraestructura tecnológica de **Aguas del Cesar S.A. E.S.P.**, incluyendo:

- Bases de datos en producción.
- Código fuente de aplicaciones.
- Activos de información (imágenes, PDF, videos, documentos electrónicos).
- Configuración de infraestructura (servidores, redes, nube).
- File Server / Directorio Activo.
- Cuentas de correo corporativo.
- Infraestructura en nube (IaC).

Inicia con la planeación de la generación del respaldo de acuerdo con el presente Plan y finaliza con la ejecución, verificación y custodia de las copias de seguridad.

## 4. MARCO NORMATIVO Y DE REFERENCIA

| Norma / Instrumento | Referencia |
|---|---|
| Constitución Política de Colombia | Arts. 15, 20 y 74 — derecho a la información y habeas data. |
| Ley 527 de 1999 | Comercio electrónico y valor probatorio de documentos electrónicos. |
| Ley 594 de 2000 (Ley General de Archivos) | Gestión documental en entidades públicas. |
| Ley 1341 de 2009 (TIC) | Principios rectores del sector TIC en Colombia. |
| Ley 1712 de 2014 (Transparencia) | Acceso a la información pública. |
| Ley 1581 de 2012 + Decreto 1074/2015 | Protección de datos personales. |
| CONPES 3854 de 2016 | Política Nacional de Seguridad Digital. |
| Decreto 1008 de 2018 | Política de Gobierno Digital (antes Decreto 1078/2015). |
| MSPI | Modelo de Seguridad y Privacidad de la Información. |
| NTC-ISO/IEC 27001:2022 | Sistema de Gestión de Seguridad de la Información. |
| NTC-ISO/IEC 27002:2022 | Controles de Seguridad de la Información — Control 8.13 Backup. |
| ITIL 4 | Buenas prácticas para gestión de copias de seguridad. |

## 5. DEFINICIONES

| Término | Definición |
|---|---|
| BACKUP / Copia de respaldo | Copia de datos que sirve de protección ante pérdida de integridad o disponibilidad de los originales |
| Backup FULL | Copia íntegra (100%) de un conjunto de datos seleccionado. |
| Backup Incremental | Copia de los datos modificados desde el último respaldo de cualquier tipo. |
| Backup Diferencial | Copia de los datos modificados desde el último FULL. |
| Backup Snapshot | Captura del estado y datos de una máquina virtual en un instante determinado. |
| Backup File System | Respaldo de una ruta específica del sistema de archivos de una MV. |
| Backup por Integración (BD) | Copia autónoma sobre el motor de base de datos (mysqldump, pg_dump, T- SQL BACKUP). |
| RTO (Recovery Time Objective) | Tiempo máximo tolerable para restaurar un servicio tras un incidente. |
| RPO (Recovery Point Objective) | Punto en el tiempo al que se puede restaurar la información sin impacto inaceptable. |
| Restauración Granular | Restauración de elementos individuales (un correo, una tabla, un archivo) desde un respaldo completo. |
| Glacier (AWS) / Archive (Azure) | Almacenamiento en nube de bajo costo para respaldos de largo plazo (>30 días). |
| RFC (Request for Change) | Solicitud formal de cambio en la configuración de un servicio de TI. |
| Activo de información | Todo elemento que contiene o procesa información de valor para la entidad. |
| SIG | Sistema Integrado de Gestión de la entidad. |
| MSPI | Modelo de Seguridad y Privacidad de la Información del MinTIC. |
| Custodia de medios | Servicio externo de almacenamiento físico de cintas u otros medios. |
| RODC | Read-Only Domain Controller — réplica de solo lectura del Directorio Activo. |

## 6. ROLES Y RESPONSABILIDADES — MATRIZ RACI

| Actividad | Jefe TIC | Equipo Infraestructura | Equipo Seguridad | Custodia Documental | Proveedor |
|---|---|---|---|---|---|
| Estrategias de Respaldo | I | C | | | |
| Requerimiento Proveedor | R | R | C | | |
| Programación Copias de Respaldo | | R | C | | |
| Monitoreo / Troubleshooting | I | R | C | | |
| Etiquetado | | R | | | |
| Validación Respaldos | | R | A | | |
| Recepción / Almacenamiento | I | R | C | | |
| Restauración Copias de Respaldo | | C | R | | |

| Código | Significado |
|---|---|
| R — Responsible | Ejecuta la actividad. |
| A — Accountable | Responde por la calidad y el resultado (solo uno por actividad). |
| C — Consulted | Aporta información o criterio previo a la ejecución. |
| I — Informed | Recibe información sobre la ejecución o resultado. |

## 7. POLÍTICAS GENERALES DE BACKUP

- Todo servidor y base de datos debe contar con una política de backup vigente, como mínimo mensual.
- Los sistemas no transaccionales deben tener respaldo semanal, mensual y anual.
- Los ambientes de pruebas y certificación podrán tener máximo un respaldo semanal (no diario).
- Las bases de datos deben respaldarse por integración; el servidor que las contiene debe tener respaldo mensual.
- Las copias de seguridad deben almacenarse en ubicación física diferente a la sede donde se generaron (offsite).
- Todas las políticas de backup deben tener una retención mínima de 3 años, salvo

disposición documental superior.

- No se podrá eliminar ni desactivar una política de backup asociada a un sistema en producción sin RFC aprobado.
- Solo los coordinadores de la Oficina TIC están autorizados para modificar una política de backup existente.
- Se deben realizar pruebas de restauración periódicas (mínimo 1 vez al mes por activo crítico) para garantizar la recuperabilidad.
- Se debe llevar el registro 'Bitácora de Backup' (diaria) con: activo, tipo, fecha, tamaño, resultado y responsable.
- En caso de falla en la ejecución de un backup, se debe notificar inmediatamente al Gestor de Backup para tomar correctivos.
- Las modificaciones, eliminaciones o inclusiones de políticas de backup deben tramitarse mediante RFC o solicitud formal ante la Mesa de Servicios.

## 8. TIPOS DE BACKUP, PERIODICIDADES Y RETENCIÓN

| Tipo | Descripción | Periodicidad | Retención | Aplica a |
|---|---|---|---|---|
| FULL | Copia íntegra de todos los datos | Mensual (mínimo) | 30 días activo / 3 años total | Servidores, BD en producción |
| INCREMENTAL | Solo datos modificados desde el último respaldo | Semanal | 30 días activo / 3 años total | Servidores, BD en producción |
| DIFERENCIAL | Datos modificados desde el último FULL | Quincenal | 30 días activo / 3 años total | Servidores virtuales |
| SNAPSHOT | Estado puntual de VM en nube | Diario (automatizado) | 30 días en nube | Infraestructura AWS/Azure/GCP |
| FILE SYSTEM | Ruta específica de archivo | Diaria automática | 30 días activo / 3 años total | File Server, activos de información |
| INTEGRACIÓN BD | Dump directo sobre motor BD | Diaria automática | 30 días activo / 3 años total | MySQL, PostgreSQL, SQL Server |

El Jefe de la Oficina TIC definirá, en coordinación con las áreas usuarias, los RTO y RPO para cada sistema de información crítico, los cuales deben quedar documentados en el inventario de activos.

## 9. PLAN DE GENERACIÓN DE COPIAS DE RESPALDO POR ACTIVO

| Activo de Información | Tipo Backup | Periodicidad | Retención | Responsable | Herramienta |
|---|---|---|---|---|---|
| Servidores Virtuales (ON PREMISE) | FULL + Incremental | Mensual / Quincenal | 3 años | Equipo Infraestructura | Veritas NetBackup / Backup Exec |
| File Server | File System | Diaria | 3 años | Equipo Infraestructura | Veritas NetBackup / Backup Exec |
| Bases de Datos ON PREMISE | Integración (dump) | Diaria | 3 años | Equipo Infraestructura | Script nativo BD (mysqldump / pg_dump / T- SQL) |
| Bases de Datos en Nube (RDS) | Snapshot automatizado | Diaria (01:05 a.m.) | 30 d. activo → Glacier | Equipo Infraestructura | AWS RDS / Cron + S3 + Glacier |
| Código Fuente | Repositorio GIT | Continuo | Indefinido | Equipo Desarrollo | GitLab / GitHub corporativo |
| Activos de Información (imágenes, PDF, shapes) | tar.gz / restic incremental | Diaria | 3 años | Equipo Infraestructura | Script bash / Restic |
| Directorio Activo | Réplica RODC en nube | Tiempo real (replicación) | Snapshot mensual | Equipo Infraestructura | AWS t2.medium + VPN |
| Correo Corporativo | PST / MBOX completo | Al retiro del usuario o solicitud | 3 años | Equipo Infraestructura | Google Takeout / herramienta GSUIT |
| Configuración Dispositivos de Red | Archivo de configuraci | Diaria automática | 3 años | Equipo Infraestructura | IMC + SNMP v2c/v3 + |

| | | | | | |
|---|---|---|---|---|---|
| | ón | | | | SSH |
| Infraestructura en Nube (IaC) | Script Terraform | Por cambio de infraestructura | 3 años | Equipo Infraestructura | Terraform v0.11+ |

### 9.1 Servidores Virtuales (ON PREMISE)

| Campo | Detalle |
|---|---|
| Tipo | Servidores Virtuales + File Server |
| Ubicación | Infraestructura ON PREMISE — Data Center AGUAS DEL CESAR S.A. E.S.P. |
| Almacenamiento | Data Storage internos referenciados por tipo y fecha |
| Prueba de restauración | 1 vez al mes por máquina virtual — en ambiente de pruebas |
| Restauración granular (File Server) | Soportada — permite restaurar archivos o carpetas individuales |

### 9.2 Bases de Datos ON PREMISE

| Campo | Detalle |
|---|---|
| Tipo | Bases de datos (MySQL, PostgreSQL, SQL Server u otros motores vigentes) |
| Ubicación | Infraestructura ON PREMISE |
| Verificación | (a) Fecha de creación del archivo; (b) Tamaño en columna 'size' |
| Registro | Bitácora Backup Diario (Excel o herramienta de gestión) |
| Prueba de restauración | 1 vez al mes por base de datos — verificar integridad post-restauración |
| Cintas LTO Ultrium | Verificación visual en herramienta de backup (modo wizard) |

### 9.3 Código Fuente de Aplicaciones

| Campo | Detalle |
|---|---|
| Tipo | Código fuente (repositorio GIT) |
| Ubicación | GitLab / GitHub corporativo |
| Esquema de redundancia | 3 copias: repositorio oficial + servidor de despliegue + desarrollador |
| Política | Todos los desarrollos web y de aplicaciones deben estar en el repositorio de la entidad |

### 9.4 Activos de Información (imágenes, PDF, shapes)

| Campo | Detalle |
|---|---|
| Tipo | Activos de información (volúmenes de aplicaciones) |
| Ubicación | Volumen del servidor de aplicaciones con persistencia de activos |
| Periodicidad | Diaria automática (definida por Oficina TIC) |
| Ventaja de restic | Backup incremental tipo GIT: comparación de versiones, detección de inyección de archivos |

### 9.5 Directorio Activo

| Campo | Detalle |
|---|---|
| Tipo | Directorio Activo (réplica RODC en nube) |
| Ubicación | Servidor local + réplica en nube ([proveedor]) |
| Acciones | Crear RODC en servidor nube; configurar lectura desde DC local; promover a DC el servidor nube |
| Snapshot | Definir task de snapshot con temporalidad aprobada por TIC |

### 9.6 Correo Corporativo

| Campo | Detalle |
|---|---|
| Evento disparador | Retiro o desvinculación del usuario, o solicitud formal |
| Formato de salida | PST / MBOX |

| | |
|---|---|
| Nombre del archivo | USUARIO_DD-MM-AAAA.PST (ej. jperez_01-01-2025.PST) |
| Almacenamiento | File Server en carpeta con nombre del usuario |
| Prueba de restauración | 1 vez al mes — montar archivo en cliente compatible y verificar lectura |

### 9.7 Configuración de Dispositivos de Red

| Campo | Detalle |
|---|---|
| Tipo | Archivos de configuración de dispositivos activos de red |
| Ubicación | Data Center AGUAS DEL CESAR S.A. E.S.P. |
| Herramienta | IMC (Intelligent Management Center) + SNMP v2c/v3 + SSH |
| Procedimiento | Configurar SNMP en equipo → configurar IP del colector → habilitar SSH<br>→ configurar plantillas IMC → descubrir equipo → vincular al plan<br>automático |
| Periodicidad | Diaria automática; ventana de 30 min configurable |
| Retención automática | 30 días (hasta 35 días configurables) |
| Contingencia | Si falla el servidor: generar backup manual y almacenar en drive corporativo con permisos |
| Puertos requeridos | Bidireccionales entre servidor y red de gestión de equipos activos |

### 9.8 Infraestructura en Nube (IaC)

| Campo | Detalle |
|---|---|
| Tipo | Scripts de aprovisionamiento de infraestructura en nube |
| Ubicación | Repositorio GIT corporativo + cuenta activa en proveedor de nube |
| Política | Toda modificación de infraestructura debe reflejarse en el script IaC antes de aplicarse |
| Referencia | Guía para el Manejo de la Infraestructura de AGUAS DEL CESAR S.A. E.S.P. |

## 10. ESTRATEGIA DE GESTIÓN (PHVA)

| Fase | Actividades |
|---|---|
| PLANEAR | Definir estrategias, lineamientos, tipos de backup, periodicidades, retenciones y pruebas de restauración para cada activo. |
| HACER | Ejecutar las copias de respaldo según la programación; realizar actividades de recuperación cuando se requiera. |
| VERIFICAR | Supervisar los backups por tamaño y fecha de modificación; registrar resultados diariamente en la Bitácora de Control de Backups. |
| ACTUAR | Ejecutar periódicamente pruebas de restauración; ante fallas, notificar al responsable e implementar correctivos; actualizar políticas según hallazgos. |

## 11. PROCEDIMIENTOS

### 11.1 Solicitar Backup

| No. | Descripción | Responsable | T. Mín. | T. Máx. |
|---|---|---|---|---|
| 1 | CREACIÓN DE SOLICITUD O RFC El usuario o área interesada genera la solicitud indicando: (a) Lanzar tarea puntual → paso 2 (b) Inclusión a política → paso 4 (c) Restauración → paso 10 | Usuario / Área solicitante | Permanente | Permanente |
| 2 | EJECUTAR TAREA DE BACKUP Se lanza la tarea y se envía evidencia al solicitante. | Gestor de Backup | 0 h | 3 h |
| 3 | CIERRE DE CASO Se documenta y cierra en la herramienta de gestión→ Finaliza procedimiento | Gestor de Backup | 0 h | 0.5 h |
| 4 | NOTIFICAR SOLICITUD DE INCLUSIÓN El usuario especifica tipo (Snapshot / File System / Integración) y periodicidad. | Usuario / Área solicitante | Permanente | Permanente |
| 5 | VALIDAR TIPO DE BACKUP • Snapshot → paso 6 • File System → paso 6 • Integración BD → paso 8 | Gestor de Backup | 0.5 h | 1 h |
| 6 | CONFIGURAR POLÍTICA EN HERRAMIENTA DE BACKUP | Gestor de Backup | 0.5 h | 1 h |

| | | | | |
|---|---|---|---|---|
| 7 | CIERRE Y COMUNICACIÓN Se envía evidencia y se actualiza el registro de políticas. → Finaliza procedimiento | Gestor de Backup | 0.5 h | 0.5 h |
| 8 | INCLUIR BASE DE DATOS POR INTEGRACIÓN Coordinación con especialistas de redes y SO para configurar agente. | Gestor de Backup | 1 h | 2 h |
| 9 | CIERRE Y COMUNICACIÓN Idem paso 7. → Finaliza procedimiento | Gestor de Backup | 0.5 h | 1 h |

## 11.2 Restauración de un Backup

| No. | Descripción | Responsable | T. Mín. | T. Máx. |
|---|---|---|---|---|
| 10 | NOTIFICAR SOLICITUD DE RESTAURACIÓN Indica si es servidor, base de datos o archivo. | Usuario / Área solicitante | Permanente | Permanente |
| 11 | VALIDAR SOLICITUD ¿Se restaura sobre el mismo sistema? • Sí → paso 12 • No → paso 14 | Gestor de Backup | 0 h | 0.5 h |
| 12 | INFORMAR AL USUARIO que la restauración está lista para validación. | Gestor de Backup | 0 h | 0.5 h |
| 13 | CIERRE DE CASO → Finaliza procedimiento | Gestor de Backup | 0 h | 0.5 h |
| 14 | ALISTAMIENTO Identificar componentes. Verificar ubicación de la cinta/respaldo (librería interna o custodia externa). | Gestor de Backup | 0 h | 0.5 h |
| 15 | SOLICITAR MEDIO AL PROVEEDOR DE CUSTODIA (si aplica) | Gestor de Backup | 2 h | 4 h |
| 16 | APROVISIONAMIENTO Reserva de servidores, BD, redes. Si es solo aplicación: omitir paso 18. | Gestor de Infraestructura | 1 h | 2 h |
| 17 | RESTAURACIÓN DE SERVIDORES Crear servidores, configurar tarjetas de red, encender. | Gestor de Backup | 2 h | 4 h |
| 18 | RESTAURACIÓN DE BASES DE DATOS Instalar motor, restaurar datos. | Gestor de BD | 2 h | 4 h |
| 19 | CONFIGURACIÓN DE APLICACIÓN Subir servicios e informar al usuario para pruebas. | Gestor de Aplicaciones | 2 h | 4 h |
| 20 | PRUEBAS FUNCIONALES Validación por parte del usuario final. | Usuario / Área solicitante | 2 h | 4 h |
| 21 | CIERRE DE CASO → Finaliza procedimiento | Gestor de Backup | 0 h | 0.5 h |

# 12. ETIQUETADO Y CUSTODIA DE MEDIOS

## 12.1 Estándar de Etiquetado

Todo medio físico (cinta LTO, disco externo) debe etiquetarse con:

- Nombre del activo respaldado.
- Tipo de backup (FULL / INCREMENTAL / DIFERENCIAL).
- Fecha de creación (DD/MM/AAAA).
- Responsable del proceso.
- Número de secuencia dentro del esquema de rotación.
- Fecha de vencimiento (retención máxima).

## 12.2 Almacenamiento Offsite

- Los medios físicos deben custodiarse en una ubicación diferente a la sede de origen.
- El proveedor de custodia debe garantizar condiciones ambientales adecuadas (temperatura, humedad, protección magnética).
- La solicitud de medios al proveedor de custodia debe realizarse con un mínimo de [8] horas de anticipación.
- El movimiento de medios debe registrarse en el log de custodia.

## 12.3 Eliminación Segura

- Los medios que superen su tiempo de retención deben eliminarse de forma segura (borrado certificado o destrucción física).
- La eliminación debe documentarse con acta firmada por el Jefe TIC y el responsable de custodia.

## 13. PRUEBAS DE RESTAURACIÓN

### 13.1 Frecuencia y Alcance

| Activo | Frecuencia mínima de prueba |
|---|---|
| Servidores virtuales (ON PREMISE) | 1 vez al mes — por cada MV |
| Bases de datos ON PREMISE | 1 vez al mes — por cada BD |
| Bases de datos en nube | 1 vez al mes — por instancia RDS |
| File Server | 1 vez al mes — muestra representativa de carpetas |
| Correo corporativo (PST/MBOX) | 1 vez al mes — sobre muestra de cuentas |
| Activos de información | 1 vez al mes — por aplicación |
| Directorio Activo | Trimestral — validación de réplica RODC |
| Configuración de red | Trimestral — restauración en ambiente de pruebas |

### 13.2 Procedimiento de Prueba

1. Seleccionar el backup a restaurar.
2. Descomprimir / montar el backup.
3. Restaurar en ambiente de pruebas (nunca en producción, salvo emergencia justificada).
4. Verificar integridad y funcionalidad del activo restaurado.
5. En caso de falla: actualizar el backup, corregir el procedimiento y repetir la prueba.
6. Registrar resultado en la Bitácora de Pruebas de Restauración.

## 14. INDICADORES DE GESTIÓN

| Indicador | Fórmula / Medición |
|---|---|
| % Backups exitosos | (Backups exitosos / Backups programados) × 100 — Meta: ≥ 99% |
| % Pruebas de restauración realizadas | (Pruebas realizadas / Pruebas programadas) × 100 — Meta: 100% |
| Tiempo promedio de restauración (MTTR) | Suma tiempos de restauración / Número de restauraciones — Meta: ≤ RTO definido |
| % Políticas con retención vigente | (Políticas con retención correcta / Total políticas) × 100 — Meta: 100% |

| | |
|---|---|
| Incidentes por falla de backup | Número de incidentes asociados a fallo de backup por período — Meta: 0 |

## 15. PROCEDIMIENTOS ASOCIADOS

| Procedimiento |
|---|
| Gestión de Incidentes de TI |
| Gestión de Incidentes Mayores |
| Gestión de Incidentes de Seguridad de la Información |
| Gestión de Cambios (RFC) |
| Gestión de Solicitudes de TI |
| Plan de Continuidad del Negocio / Plan de Recuperación ante Desastres |
| Gestión Documental y Custodia de Medios |
| Inventario y Clasificación de Activos de Información |
| Modelo de Seguridad y Privacidad de la Información — MinTIC |

## 16. REGISTROS Y EVIDENCIAS

| **Registro** | Responsable de diligenciar |
|---|---|
| Bitácora de Backup Diario | Gestor de Backup |
| Log de Pruebas de Restauración | Gestor de Backup |
| Registro de Políticas de Backup (tipo, retención, RFC) | Gestor de Backup |
| Log de Movimiento de Medios (custodia) | Equipo Infraestructura |
| Acta de Eliminación Segura de Medios | Jefe TIC + Custodia |
| Tickets / RFC en herramienta de Mesa de Servicios | Mesa de Servicios |

## 17. BIBLIOGRAFÍA Y REFERENCIAS


- MinTIC. (vigente). Modelo de Seguridad y Privacidad de la Información (MSPI). https://www.mintic.gov.co/
- MinTIC. (vigente). Marco de Referencia de Arquitectura Empresarial (GEL). https://www.mintic.gov.co/arquitecturati/
- MinTIC. (s.f.). Respaldo y recuperación de los servicios tecnológicos. https://www.mintic.gov.co/arquitecturati/630/w3-article-8862.html
- ICONTEC. (2022). NTC-ISO/IEC 27001:2022 — Sistemas de Gestión de Seguridad de la Información.
- ICONTEC. (2022). NTC-ISO/IEC 27002:2022 — Controles de Seguridad de la Información.
- AXELOS. (2019). ITIL 4 Foundation. TSO.
- CONPES 3854. (2016). Política Nacional de Seguridad Digital. DNP — Colombia.
- Ley 594 de 2000. Ley General de Archivos. Congreso de la República de Colombia.
- Decreto 1008 de 2018. Política de Gobierno Digital. Presidencia de la República de Colombia.
- Ministerio de Ambiente y Desarrollo Sostenible. (2022). Plan para la Generación de Copias de Respaldo (Backup). DS-A-GTI-02 v2.
- Ministerio de Educación Nacional. (s.f.). Procedimiento Backup y Restauración. ST-PR-21 v1.