

MacroProceso	Gestión tecnológica	Proceso	Gestión de servicios tecnológicos	Estado	Vigente
--------------	---------------------	---------	-----------------------------------	--------	---------

Contenido

1. OBJETIVO	2. ALCANCE
Planear, ejecutar, controlar, verificar y mejorar continuamente las copias de respaldo (backups) y las actividades de restauración de la información de ICETEX, asegurando la disponibilidad, integridad, confidencialidad y continuidad de los servicios tecnológicos que soportan los procesos misionales, estratégicos y de apoyo. Así mismo, establecer un esquema institucional de protección y custodia externa de la información respaldada, minimizando el riesgo de pérdida, corrupción o indisponibilidad de los datos.	El procedimiento inicia desde la identificación de la necesidad de respaldo de la información hasta la custodia externa y verificación periódica de los backups y pruebas de restauración. Aplica a las plataformas que soportan la operación de ICETEX, ubicadas en Data Center Principal, Data Center Alterno, Direcciones de ICETEX (incluida Aguas), ya sean de propiedad del ICETEX o del proveedor de servicios de Data Center y se articula con los procedimientos propios del proveedor de Data Center y telecomunicaciones, garantizando una traza completa desde la generación del backup hasta su custodia externa.
3. DEFINICIONES	
• Backup (Copia de Seguridad): Proceso mediante el cual se genera una réplica íntegra, consistente y verificable de la información, con el fin de garantizar su recuperación ante pérdida, corrupción, eliminación accidental o eventos de desastre. • Backup Incremental o Progresivo: Copia de seguridad de la información que realmente ha sido modificada día a día por las diferentes aplicaciones que se ejecutan en los servidores. • Cintoteca: Almacén donde reposan los medios magnéticos (cinta magnética, disquete, cartuchos, Discos removibles, CDS, etc.) y la información que estos contienen. • Custodia de Medios. Corresponde a la seguridad y cuidado de los medios magnéticos fuera de la Entidad. • Data Center (Centro de Datos): Instalación física diseñada para albergar, operar y mantener la infraestructura tecnológica crítica de la organización, incluyendo servidores, almacenamiento, redes, sistemas de respaldo, energía, climatización, seguridad física y lógica. • Full Backup: Copia de seguridad de la totalidad de los datos almacenados en los servidores de acuerdo a la aplicación. • IBD (Infraestructura de Backup y Recuperación): Conjunto de componentes tecnológicos y lógicos —servidores, librerías de cintas, repositorios, software de respaldo, políticas, procedimientos y redes— que habilitan los procesos de copia, almacenamiento, retención y restauración de la información. • Jobs: Tareas automáticas que se programan en el servidor. • LTO-7 (Linear Tape-Open 7): Es la séptima generación del estándar de cintas magnéticas LTO, utilizado para almacenamiento y respaldo de grandes volúmenes de información en entornos empresariales. • Medios de Almacenamiento: Dispositivos o soportes utilizados para almacenar las copias de seguridad, como cintas LTO-7, almacenamiento en discos o repositorios dedicados, según la criticidad y requerimientos de recuperación. • Operador de Backups: Persona o rol técnico responsable de la administración integral del proceso de respaldo, incluyendo programación, ejecución, monitoreo, validación y la atención de incidentes relacionados con la infraestructura de backup. • Outsourcing: Modelo de prestación de servicios mediante el cual un tercero especializado ejecuta, administra o soporta procesos tecnológicos definidos contractualmente, asegurando niveles de servicio y continuidad operativa. • Pool de cinta: Conjunto organizado de cintas de respaldo disponibles para su uso dentro de una infraestructura de almacenamiento o sistema de copias de seguridad. • 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. • Restauración: Proceso mediante el cual se recupera información previamente respaldada para restablecer datos, aplicaciones o servicios a su estado funcional. Incluye selección de punto de restauración y verificación posterior. • Retención: Política que define el tiempo durante el cual se conservarán las copias de seguridad antes de su depuración o eliminación, según criterios operativos, normativos o de auditoría. • RPO (Recovery Point Objective): Máximo punto de pérdida de información aceptable ante un incidente. Define cuánto puede retroceder la información restaurada respecto al último respaldo exitoso. • RTO (Recovery Time Objective): Tiempo máximo permitido para restablecer un servicio, sistema o conjunto de datos después de un incidente. • Snapshot (instantánea): Es una copia exacta del estado de un sistema, máquina virtual o volumen de datos en un momento determinado. Funciona como una	

"fotografía" que registra configuraciones, aplicaciones y archivos, permitiendo revertir el sistema a ese punto exacto rápidamente si algo sale mal.

4. CONDICIONES GENERALES

- 4.1. El presente procedimiento se fundamenta en las buenas prácticas de Plan de Continuidad del Negocio, ITIL y la normativa vigente sobre Gobierno, Seguridad Digital y Protección de datos personales.
- 4.2. Los detalles técnicos de la operación de backups se documentan en el Manual de Backups del proveedor, el cual se encuentra publicado como documento externo del proceso de Gestión de Servicios Tecnológicos.
- 4.3. La responsabilidad de la definición de criticidad de la información recae en los líderes de cada proceso.
- 4.4. Los colaboradores de ICETEX son responsables de respaldar la información sensible o relevante que gestionen, utilizando los medios institucionales definidos, conforme a los lineamientos divulgados por la Dirección de Tecnología.
- 4.5. Los backups deben cumplir criterios de confidencialidad, integridad, disponibilidad y trazabilidad.
- 4.6. Los informes de gestión de backup del proveedor deben documentar las evidencias sobre la operación, administración de los backup, planes de acción, fallas presentadas y toda la información que sea relevante, de acuerdo con los procedimientos establecidos.
- 4.7. Las copias de respaldo gestionadas a través de este procedimiento incluyen los siguientes elementos tecnológicos:
 - o Portal institucional (dominios, subdominios, configuraciones).
 - o Servidores de bases de datos.
 - o Servidores de aplicaciones.
 - o Sistemas de información misionales.
 - o Plataformas financieras, académicas y de recaudo.
 - o Plantillas y configuraciones de:
 - ✓ Equipos de seguridad (Firewall, WAF, otros appliance).
 - ✓ Equipos de comunicaciones (Switches, Routers, otros).
 - o Servidores virtuales y plataformas de virtualización (VMware, Azure u otros).
 - o Infraestructura y máquinas de la sede Aguas.

- 4.8. Los roles y responsabilidades establecidos frente a la gestión de backups de la información del ICETEX son los siguientes:

Rol	Responsabilidades
Dueño del proceso	Definir la criticidad de la información
Dirección de Tecnología	Diseñar, coordinar, ejecutar y monitorear backups
Administrador de Bases de Datos	Ejecutar y validar backups y restauraciones de BD
Oficial de Seguridad de la Información	Verificar cumplimiento de controles
Continuidad del Negocio	Alinear con DRP (Plan de Recuperación de Desastres) y BCP (Plan de continuidad de negocio)
Control Interno	Auditoría y seguimiento al cumplimiento

- 4.9. La información de la entidad tiene la siguiente clasificación, frente a la generación y custodia de backups:

Nivel	Descripción	Ejemplos
Crítica	Impacta la continuidad institucional	Core de crédito, recaudo
Sensible	Contiene datos personales	Beneficiarios, codeudores
Operativa	Soporte al negocio	Gestión documental
No crítica	Bajo impacto	Informes históricos

- 4.10. Tipos de respaldo: Se ejecutan los siguientes tipos de respaldo de la información:

- Completo (Full): Copia total de la información.
- Incremental: Respaldan solo cambios desde el último backup.
- Diferencial: Cambios desde el último backup completo.
- Snapshots: Copias de estado de máquinas virtuales.

- 4.11. Periodicidad: Se establece la siguiente periodicidad, tipo y tiempos de retención para los backups, de acuerdo con la clasificación de la información.

Clasificación	Tipo	Frecuencia	Retención
Crítica	Completo + incremental	Diario	30 días
Sensible	Completo	Semanal	60 días
Operativa	Incremental	Diario	30 días

- 4.12. Se presentan dos tipos de frecuencia o rotación de backups:

- Semanal: Se tiene contemplado un Pool de cinta para el respaldo incremental de backup durante la semana, una vez se cumpla la semana completa se manda a custodia externa con el fin de que esté disponible la siguiente semana para recuperar la información en caso de requerirse. El segundo pool de cinta respaldará la semana en la que la primera cinta esté en custodia externa, al completar la semana de respaldo se envía a custodia externa la segunda cinta; así sucesivamente se rotan las cintas para que mientras una respalda, la otra se encuentra en custodia externa de ser requerida alguna restauración.
- Mensual: corresponde a un pool de cintas que se utiliza al final del mes en un backup full, el cual quedará en custodia externa sin rotación hasta cuando se cumpla su retención por 12 meses.

MacroProceso	Gestión tecnológica	Proceso	Gestión de servicios tecnológicos	Estado	Vigente
--------------	---------------------	---------	-----------------------------------	--------	---------

4.13. Se aplica la siguiente regla, conocida como Regla 3-2-1, para los backups de información:

- 3 copias.
- 2 medios distintos.
- 1 copia fuera del sitio principal. Traslado a custodia externa (proveedor servicios data center).

4.14. Medios de almacenamiento: El ICETEX empleará cintas magnéticas y almacenamiento en disco, garantizando compatibilidad tecnológica y accesibilidad histórica de la información respaldada.

4.15. Fuentes de información a respaldar: La información a respaldar corresponde principalmente a la almacenada en:

- Base de Datos
- Aplicaciones
- Correo electrónico
- Configuraciones de sistemas
- Carpetas de usuarios

Observación: En este caso de las bases de datos, al tratarse de información crítica institucional, se aplican técnicas y herramientas especiales enfocadas en la recuperación ante desastres (DRP). Permite la copia online de cada transacción de forma remota entre los data center.

Aspectos mínimos a considerar para realizar la ejecución del procedimiento

4.16. El ICETEX, junto con el tercero contratado para la realización de backups, debe tener en cuenta los siguientes aspectos mínimos antes, durante y después de la ejecución de backup y subsanaciones en caso de fallas:

- Configuración y actualización de herramienta de backup por parte del proveedor
- Ventana de respaldo autorizada
- Verificar capacidades de almacenamiento
- Validar cronogramas de ejecución de los backup automáticos
- Revisar logs y alertas
- Registrar evidencia
- Reportar fallas, análisis de evento presentado y plan de mejoramiento
- Relanzamiento de copias para respaldo en caso de falla o incidente
- Validar cronogramas de pruebas de restauración de backup

4.17. Consideración para la Custodia externa: Se debe trasladar los medios de respaldo a un lugar de condiciones adecuadas situado fuera del sitio de donde se realizan dichas copias, de acuerdo con los procedimientos establecidos por la Entidad y proveedor para tal fin.

Consideraciones Gestión de restauraciones

4.18. Toda restauración deberá ser autorizada, registrada y validada.

4.19. Se realiza prueba de restauración por lo menos una mensual, junto con el proveedor y usuarios que intervienen.

4.20. Las evidencias sobre la operación y administración de los backups deben estar documentada en el informe de gestión mensual del proveedor.

4.21. El informe mensual de gestión que presenta el proveedor debe contener aspectos relevantes sobre las restauraciones realizadas, fallas presentadas, subsanaciones y planes de mejora (Cuando aplique).

4.22. Restauraciones por demanda: La restauración de la información se pueden solicitar en cualquier momento debido a daños, pérdida o pruebas requeridas, la cual se debe realizar de acuerdo con los procedimientos definidos.

4.23. Tipos de restauración:

Las restauraciones utilizadas son de tipo:

- Parcial (archivo, tabla, buzón)
- Completa (sistema o BD)
- Contingencia (DRP)

4.24. Con el fin de realizar las restauraciones de backups, se deben seguir los siguientes pasos:

- Recepción de solicitud formal
- Validación de autorización
- Validación de recursos técnicos necesarios para el respaldo (espacio discos, memorias, ubicación, servidor, entre otros)
- Identificación del punto de restauración
- Ejecución controlada
- Validación funcional

4.25. Pruebas de restauración: Se realizará solicitud a proveedor para realizar la prueba de restauración de los backups realizados, la cual contempla por lo menos una prueba de restauración mensual o las que se consideren necesarias en el ejercicio de validación.

Gestión de remediación a copias fallidas

4.26. En caso de falla de copia de respaldo el proveedor garantizará mediante un relanzamiento de la copia hasta el estado de éxito de cada una; de parte del proveedor se requiere realizar un análisis de causa raíz y los planes de mejora, con el fin de minimizar o evitar errores reiterativos en el proceso de copias y que pueden representar altos riesgos para la operación.

4.27. El informe mensual que presenta el proveedor debe contener aspectos relevantes de las fallas presentadas, subsanaciones y planes de mejora (Cuando aplique), considerar aspectos como:

- Infraestructura. Ampliaciones de Espacio y otros aspectos relacionados.
- Software. Actualización de parches o aplicaciones.

- Procedimiento. Validación de la secuencia de pasos y aspectos relacionados.

Verificación periódica de consistencia de la información respaldada

- 4.28. Lanzamiento de Pruebas de restauración: Verificar periódicamente la integridad y consistencia de la información respaldada de los backups realizados, Las pruebas de restauración se realizarán de forma mensual y deberán dejar evidencia documentada (informes y registros) que se conservarán para fines de trazabilidad y auditoría de restauración.
- 4.29. Se debe llevar una plantilla de seguimiento en la entidad para la entrega de las restauraciones solicitadas, indicando fecha de solicitud, solicitante, proceso a que hace parte el solicitante, fecha de entrega, ruta de soporte, nombre del servidor, ID radicado de solicitud al proveedor, estado, validación y observaciones/ resultado de la restauración, desde el inicio de la restauración hasta la validación de la consistencia de la data por parte del administrador del sistema o base de datos.

5. DESCRIPCIÓN DE ACTIVIDADES

Convenciones:

Actividad de control: Acuerdo de servicio: 

No.	Descripción	Frecuencia / tiempo máximo	Responsable	Registro o evidencia de la actividad	Actividad de control / Acuerdo de servicio
1	Realiza las actividades operativas y administrativas, así como de documentación, incluyendo tipo de copias, respaldo, frecuencia y restauración, de acuerdo con lo definido en el "Manual de Backups del Proveedor" (23) y las políticas de backup establecidas en conjunto entre el Grupo de Infraestructura y el proveedor.	Cada vez que se requiera	Operador / Outsourcing DataCenter	Informe mensual de gestión de backups	N/A
2	Elabora el respectivo informe de la gestión de backups y lo entrega a la Dirección de Tecnología. En el informe se deben documentar las evidencias sobre la operación, administración de los backup, planes de acción, fallas presentadas y toda la información que sea relevante, de acuerdo con las políticas de backup definidas.	Mensualmente	Operador / Outsourcing DataCenter	Informe mensual de gestión de backups	N/A
3	Revisa el informe y verifica que las actividades realizadas correspondan a las copias indicadas en las políticas de backup definidas y que estas se encuentren en estado "completo". ¿El informe está correcto? - Si, continúa con la actividad 5. - No, solicita ajuste y continúa con la actividad 4.	Mensualmente	Profesional encargado de seguimiento de Backup / Dirección de Tecnología	Correo electrónico	
4	Ajusta o aclara el informe de acuerdo con las observaciones realizadas por la Dirección de Tecnología del ICETEX. De acuerdo con la solicitud, vuelve a lanzar el backup y actualiza el informe. Regresa a la actividad 2.	Mensualmente	Operador / Outsourcing DataCenter	Informe de backups	N/A
5	Notifica al Outsourcing DataCenter (proveedor) la aprobación del informe.	Mensualmente	Profesional encargado de seguimiento de Backup / Dirección de Tecnología	Correo electrónico	N/A
6	Realiza programación mensual de pruebas de restauración de backups, seleccionando los servidores e información a restaurar y remite la solicitud al proveedor en el formato establecido por el mismo, con la información requerida.	Mensualmente	Profesional encargado de seguimiento de Backup / Dirección de Tecnología	Solicitud de restauraciones al proveedor, con formato a través de correo electrónico	
7	Realiza las actividades de restauración e informa a la Coordinación de Infraestructura, al solicitante de la restauración y al profesional encargado de seguimiento de backups.	Mensualmente	Operador / Outsourcing DataCenter	Correo electrónico	N/A

MacroProceso	Gestión tecnológica	Proceso	Gestión de servicios tecnológicos	Estado	Vigente
8	Validan la restauración de backups realizada e informan el resultado. Si es una restauración de bases de datos, se valida que la información originalmente restaurada es consistente. Si se realizó una restauración de software, se valida la correcta funcionalidad. ¿Se encuentran inconsistencias en la restauración? - Si, informan al proveedor para su correspondiente ajuste (con copia a Coordinación de Infraestructura ICETEX). Regresa a la actividad 7. - No, informan al proveedor la validación exitosa (con copia a Coordinación de Infraestructura ICETEX). Continúa con la actividad 9.	Mensualmente	Administradores - Usuarios funcionales de los sistemas de información y/o bases de datos / Procesos ICETEX	Correo electrónico	
9	Documenta las acciones realizadas y evidencias de las restauraciones, en el informe mensual de gestión.	Mensualmente	Operador / Outsourcing DataCenter	Informe mensual de gestión	N/A
10	Actualiza información en la matriz de programación y seguimiento de restauraciones dispuesto por la Dirección de Tecnología.	Mensualmente	Profesional encargado de seguimiento de Backup / Dirección de Tecnología	Matriz de seguimiento de restauraciones	N/A
6. DOCUMENTOS RELACIONADOS					
Nombre del documento			Código		
Manual de Backups del Proveedor			23		
Políticas de Backup			N/A		
Formato de solicitud de restauración establecido por el proveedor			N/A		
Matriz de programación y seguimiento de restauraciones			N/A		
7. ANEXOS					
7.1 DIAGRAMA DE FLUJO (Ver Anexo)					
7.2 OTROS					
No aplica					

Anexos:

[A7-1-10 Gestión de backups V6.png](#)

Editado por Adriana Esperanza Aranguren Prieto, ago 14 2026 10:53 a.m.

Modificaciones

Descripción de cambios

Se amplió la descripción de las actividades y se complementaron las condiciones generales. Se migró al formato F100 en su nueva versión.

Historial de Versiones

Fecha Vigencia (Acto Adtvo)	Versión	Descripción de Cambios
2026-08-21	6	Se amplió la descripción de las actividades y se complementaron las condiciones generales. Se migró al formato F100 en su nueva versión.
2021-11-29	5	1. En condiciones generales se agrega "Los backups correspondientes a la información sensible e importante para el Instituto que manejen los colaboradores del ICETEX, son responsabilidad de cada uno de los colaboradores. Resguardando la información en los medios de almacenamiento dispuestos y establecidos en la Entidad para tal fin, para garantizar su respaldo y disponibilidad de información desde cualquier lugar. Estos son divulgados por los medios de comunicación internos. 2. En medios de almacenamiento se agrega el siguiente párrafo "(Cinta Magnética para almacenamiento de datos) de acuerdo a los equipos que disponga el proveedor." 3. En rotación de Backups mensual se elimina clon pool mensual.
2020-02-07	4	Se realiza actualización del documento en el tipo cinta y manual de proveedor de datacenter.
2013-01-22	3	• En el punto 1 se modifica el objetivo definiendo un plan de pruebas de restauración. • En la actividad 5.2.3 se reemplaza la palabra "verifica por válida".
2012-12-14	2	Se actualiza procedimiento para incluir el Manualde Backups del Proveedor como documento Externo y Políticas del Icetex en condiciones generales.
24/6/2010	1.0	-

¿Ha revisado el documento en su totalidad?

SI