



PROCEDIMIENTO DE BACKUP

Código: E-GI-P005

Tipo de Proceso: Estratégico

Versión: 05

Proceso: Gestión de Tecnología de Información y Comunicaciones

Vigencia: 07/09/2023

1. OBJETIVO(S)

Establecer los lineamientos para la gestión, almacenamiento, respaldo y verificación del Backup del IDEAM

2. ALCANCE

Inicia desde la necesidad del área o la identificación de infraestructura tecnológica (aplicaciones, bases de datos, logs etc.) que requiera tener una modificación al respaldo a corto y largo plazo, continúa con la definición de frecuencia de Backup, revisión de capacidad de almacenamiento configuración de la herramienta definida por la entidad y finaliza con el monitoreo y la verificación del Backup conforme a lo definido en las políticas de operación.

Este proceso va dirigido a todos los responsables de administrar, liderar, gestionar e interactuar con la infraestructura tecnológica y/o que tengan cualquier relación con información de la entidad incluidos terceros. Los cuales deben señalar y expresar el conocimiento de su contenido, alcance y solicitar los cambios pertinentes toda vez que sea necesario ante cualquier eventualidad.

Aplicable a toda la información digital que contengan datos considerados de información crítica del Instituto contenida en un sistema de información o aplicación, tanto a nivel misional como a nivel de apoyo

3. RESPONSABLE

Profesional Universitario

3.POLITICAS DE OPERACIÓN

- El procedimiento de respaldo involucra a todos los administradores y/o responsables de componentes de información digital alojada en la infraestructura tecnológica de IDEAM.
 - Para el resguardo de la información de los usuarios no se permite alojar información personal como: música, videos, documentos transitorios documentos confidenciales, Backup de equipos de escritorio, Backup de correo electrónico y demás que no sean relevantes en el cumplimiento de los objetivos de la Entidad.
 - Es responsabilidad de los Jefes, Directores, Subdirectores y coordinadores de los grupos y áreas identificar claramente la información crítica a su cargo identificar los riesgos y generar el plan de continuidad en el cual debe estar incluido la solicitud de respaldo a través de la mesa de servicio en el formato definido por la Oficina de Informática el cual será dirigido al gestor de Backup.
 - Los Jefes, Directores, Subdirectores y coordinadores de los grupos responsable de la administración de servidores y/o sistemas de información son los únicos autorizados para solicitar el respaldo y/o recuperación de información mediante un caso o requerimiento ante la mesa de servicios indicando los datos del solicitante, datos de la aplicación, datos de los archivos (tipo y ubicación), al igual que de definir la periodicidad de respaldo y tipo de respaldo.
 - Dada la crítica relevancia de preservar el control de versiones del código fuente y garantizar la trazabilidad exhaustiva de las acciones efectuadas en los sistemas de información, resulta imperativo incorporar estos elementos en la Política de Tecnologías de la Información (TI). Esto implica la inclusión de directrices específicas en las políticas relacionadas con la parametrización, almacenamiento, protección, integración y respaldo de logs, entre otros aspectos. Siendo este un acto administrativo de gran envergadura que adquiere una importancia y relevancia excepcionales en el contexto institucional.
 - Se debe garantizar que la información de Backup almacenada en la entidad cuente con una copia de respaldo digital externamente en una nube pública.
 - Cuando un usuario se retira de la entidad, el área es responsable de que la información de este quede almacenada en el repositorio del área
 - Se realizarán pruebas de restauraciones mínimo una vez al año y teniendo en cuenta las capacidades tecnológicas, humanas, etc. Con las que cuente la Oficina de Informática, así mismo cuando sea requerida por el área que lo solicite.
 - La retención de los Backup dependerá de lo definido por cada área en la solicitud que realicen ante la mesa de servicio.
- Se manejarán los siguientes estándares:
- > Diario: Se realiza Backup incremental de lunes a viernes retención 8 días.
 - > Semanal: Se realiza Backup full los sábados retención 30 días.
 - > Mensual: Se realiza Backup full los días 10 de cada mes retención 52 semanas.

4. NORMAS Y DOCUMENTOS DE REFERENCIA

- Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información Pública): Establece el deber de las entidades públicas de garantizar la disponibilidad integridad y seguridad de la información que generan, obtienen, adquieren, transforman, controlan y custodian. Además, establece la obligación de conservar los documentos y registros en los términos establecidos por la normatividad archivística.
- Ley 1581 de 2012 (Ley de Protección de Datos Personales): Regula el tratamiento de los datos personales por parte de entidades públicas y privadas estableciendo principios, obligaciones y derechos para garantizar la protección de la información personal.
- Ley 1273 de 2009 – De La Protección de la Información y de los Datos
- Ley 594 de 2000 (Ley General de Archivos): Establece las normas generales para la organización y funcionamiento de los archivos en Colombia incluyendo los requisitos para el almacenamiento, conservación y protección de los documentos de las entidades públicas.
- Decreto 620 de 2020: Establece disposiciones para el almacenamiento y custodia de archivos de gestión en formato electrónico.
- Decreto 2609 de 2012: Reglamenta la conservación del patrimonio documental en medios electrónicos y se dictan otras disposiciones relacionadas con la gestión documental electrónica en las entidades públicas.
- Resolución 1084 de 2015 (Guía para la gestión de documentos electrónicos): Establece los lineamientos técnicos y las directrices para la gestión de documentos electrónicos en las entidades públicas.
- Resolución 3564 de 2015 (Requisitos de seguridad de la información): Establece los requisitos mínimos de seguridad de la información que deber implementar las entidades públicas para proteger los sistemas y datos.

5. DEFINICIONES

- **Aplicaciones:** Programas informáticos que permiten a un usuario utilizar una computadora con un fin específico. Las aplicaciones son parte del software de una computadora, y suelen ejecutarse sobre el sistema operativo.
- **Archivo registro (Log):** Es un registro oficial de eventos durante un rango de tiempo en particular. Es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación. La mayoría de los registros son almacenados o desplegados en el formato estándar, el cual es un conjunto de caracteres para dispositivos comunes y aplicaciones. De esta forma cada log generado por un dispositivo en particular puede ser leído y desplegado en otro diferente.
- **Base de Datos:** Almacén de datos relacionados con diferentes modos de organización. Una base de datos representa algunos aspectos del mundo real, aquellos que le interesan al diseñador. Se diseña y almacena datos con un propósito específico. Con la palabra "datos" se hace referencia a hechos conocidos que pueden registrarse, como ser números telefónicos, direcciones, nombres, etc.
- **Custodia:** Implica la responsabilidad de proteger y gestionar los datos de respaldo de manera segura y confiable para garantizar su integridad y disponibilidad a lo largo del tiempo..
- **Copia de respaldo (Backup):** Copia de seguridad o copia de respaldo (Backup en inglés, el uso de este anglicismo está ampliamente extendido) se refiere a la copia de datos de tal forma que estas copias adicionales puedan restaurar un sistema después de una pérdida de información. La copia de seguridad puede realizarse sobre los datos, en los cuales se incluyen también archivos que formen parte del sistema operativo. Así las copias de seguridad suelen ser utilizadas como la última línea de defensa contra pérdida de datos y se convierten por lo tanto en el último recurso a utilizar.
- **Directorio:** Agrupación de archivos de datos, atendiendo a su contenido, a su propósito o a cualquier criterio que decida el usuario. Sirven para organizar mejor los archivos en un disco de almacenamiento. Dentro de un directorio pueden existir también otros directorios, llamados subdirectorios o subcarpetas; de hecho, en definitiva, todos los directorios son subdirectorios del directorio raíz (la unidad lógica).
- **Dispositivos de Almacenamiento:** Grupo de dispositivos de hardware o software dedicados a guardar datos.
- **Nube publica:** es un modelo de computación en la nube en el que los servicios y recursos informáticos se ofrecen a través de Internet por proveedores de servicios en la nube, permitiendo a los usuarios acceder a ellos según sea necesario.
- **Restauración (Restore):** técnicas empleadas para recuperar archivos que han sido perdidos o eliminados, desde una copia de respaldo realizada previamente, a través de algún medio de almacenamiento.
- **Sistema de Almacenamiento:** Dispositivo utilizado para grabar los datos de una computadora de forma permanente o temporal. Una unidad de disco, junto con los discos que graba, es un dispositivo de almacenamiento. El almacenamiento incluye los dispositivos de almacenamiento más permanentes, como unidades de disco y de cinta. A su vez la palabra log se relaciona con el término evidencia digital. Un tipo de evidencia física construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales, lo que implica la lectura del log y deja al descubierto la actividad registrada en el mismo.
- **Servidor:** Es una computadora que, formando parte de una red, provee servicios a otras denominadas clientes.
- **Sistema Operativo:** Sistema tipo software que controla la computadora y administra los servicios y sus funciones como así también la ejecución de otros programas compatibles con éste.
- **Tarea programada o automática:** es aquella que se desarrolla sin la intervención del usuario.

6. PROCEDIMIENTO

Nº.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	TIEMPOS	REGISTRO - PUNTO DE CONTROL
1	Solicitar Backup	P	Diligenciar y enviar por mesa de servicio la solicitud de Backup. En la solicitud se debe adjuntar el FORMATO SOLICITUD CAMBIO O ADICION COPIAS RESPALDO.	Líder funcional y/o temático del área solicitante.	1 día	
2	Validar formato	H	Recibir la solicitud y validar que el formato se encuentre plenamente diligenciado. En caso de estar plenamente diligenciado y si corresponde a un sistema de información se reasigna y continua con la ACTIVIDAD N.º 3 en caso de no corresponder a un sistema de información continua con la ACTIVIDAD N.º 4. En caso de que la información se encuentre incompleta se devuelve la solicitud y continua nuevamente con la ACTIVIDAD N.º 1.	Mesa de Servicio	30 minutos	Caso mesa de servicio - Validar que el formato se encuentre plenamente diligenciado.
3	Dar viabilidad técnica GSI	H	Validar la viabilidad de la solicitud. En caso de ser viable se reasigna al gestor de Backup, se pone el visto bueno en el FORMATO SOLICITUD CAMBIO O ADICION COPIAS RESPALDO y continua con la ACTIVIDAD N.º 4 En caso de no ser viable continua con la ACTIVIDAD N.º 8	Líder técnico del Grupo de Sistemas de Información de la Oficina de Informática		Caso mesa de servicio - Validar la viabilidad de la solicitud.
4	Dar viabilidad técnica GTC	H	Revisar el formato y validar técnicamente las capacidades de Backup a nivel de infraestructura. En caso de ser viable se pone el visto bueno en el FORMATO SOLICITUD CAMBIO O ADICION COPIAS RESPALDO y continua con la ACTIVIDAD N.º 5. En caso de no ser viable continua con la ACTIVIDAD N.º 8 y se justifica la razón de cierre dejando la anotación del porque técnicamente no procede.	Gestor de Backup del GTC	2 días	Caso mesa de servicio -Validar que el formato
5	Realizar Backup	H	Realizar el proceso de Backup a través de la herramienta definida por la entidad para las solicitudes que llegan a través de la mesa de servicio y para aquellos backups programados.	Gestor de Backup del GTC	2 días	

6. PROCEDIMIENTO

Nº.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	TIEMPOS	REGISTRO - PUNTO DE CONTROL
6	Verificar estado de Backup	V	Verificar a través de la herramienta el estado del Backup En caso de que el proceso haya sido exitoso continua con la ACTIVIDAD N.º 8 En caso de que el proceso haya quedado en un estado diferente a exitoso se debe validar la razón y volver a la ACTIVIDAD N.º 5 si sigue presentándose el error continua con la ACTIVIDAD N.º 7	Gestor de Backup del GTC	30 minutos	Caso mesa de servicio y caso soporte fabricante - Herramienta de Backup
7	Escalar al fabricante	A	En caso de no poder solucionar los errores generados por la herramienta se escala al fabricante por medio de un caso de soporte a través del portal de la herramienta Cuando este se solucione continua con la ACTIVIDAD N.º 8. NOTA: Esta actividad aplicará en los casos que se cuente con garantía por parte del fabricante.	Gestor de Backup del GTC	2 días	
8	Cerrar la solicitud en la mesa de servicio.	A	Cerrar la solicitud en la mesa de servicio con el respectivo soporte de cierre.	Gestor de Backup del GTC	30 minutos	
9	Archivar solicitud	A	Archivar Formato solicitud de Cambio o Adición de Copias de Respaldo y cerrar caso de mesa de Servicio. De acuerdo con los backups realizados continua con la ACTIVIDAD N.º 10	Gestor de Backup del GTC	1 hora	Formato solicitud de Cambio o Adición de Copias de Respaldo
10	Identificar Backup a restaurar	V	Identificar el Backup a restaurar el cual se elige de manera aleatoria o por solicitud conforme a las capacidades de infraestructura que cuenta la Oficina.	Gestor de Backup del GTC	1 hora	
11	Identificar el ambiente	V	Identificar en qué ambiente se encuentra el Backup: on-premise o nube.	Profesional Universitario GTC	1 hora	
12	Revisar accesos	V	Asegurar tener acceso al dispositivo de almacenamiento que contiene la copia de seguridad (por ejemplo, un disco duro externo, una unidad de red o una nube).	Profesional Universitario GTC	1 hora	
13	Seleccionar Backup	V	Seleccionar que el Backup que contiene los datos más recientes o la versión que necesita restaurar.	Profesional Universitario GTC	1 hora	
14	Realizar restauración	V	Realizar el proceso de restauración en un ambiente controlado. NOTA: Los tiempos de ejecución están sujetos a las características de la maquina virtual o física a restaurar.	Profesional Universitario GTC	5 días	Reporte de la herramienta de Backup
15	Verificar restauración	A	Realizar actividades de verificación de la restauración realizada. En caso de fallas en el proceso de restauración continua con la actividad 16. En caso que la restauración sea exitosa, se valida técnicamente y continua con la actividad 17	Profesional Universitario GTC	1 día	Reporte de la herramienta de Backup
16	Identificar otro punto de restauración	A	Realizar la identificación de otro punto de restauración y continuar con la actividad 14	Profesional Universitario GTC	1 hora	
17	Realizar pruebas funcionales	A	Realizar las pruebas con el área funcional para validar la correcta restauración. Para el caso se deberá remitir a través de correo electrónico la restauración realizada y deberá remitirse por el área funcional a vuelta de correo el visto bueno de la actividad ejecutada.	Líder funcional y/o temático del área solicitante.	1 día	Correo electrónico
18	Documentar	V	Informe o acta de la ejecución de la restauración dejándola como soporte en la mesa de servicio con el fin de contar con la trazabilidad del caso	Profesional Universitario GTC	3 días	Informe o acta