



GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

CÓDIGO: GTI-PR-04

VERSIÓN: 01

PROCEDIMIENTO RESPALDO DE INFORMACIÓN Y RESTAURACIÓN DE COPIAS DE SEGURIDAD

PÁGINA: 1 de 6

Documento de Carácter

Público

Reservado

Clasificado

1. OBJETIVO

Realizar el respaldo de los servicios e información de la entidad a través de una herramienta tecnológica que garantice la disponibilidad e integridad de la información.

2. ALCANCE

Este procedimiento inicia con la realización de la copia de la información crítica de cada proceso/área/dependencia en los repositorios definidos y finaliza con la custodia de dicha información.

3. ENTRADAS

A continuación, se definen las entradas necesarias para el presente documento:

- ✓ Información crítica por proceso/área/dependencia.
- ✓ Formato de solicitud de instalación de software, acceso a servicios de TI y permisos a unidades compartidas.
- ✓ Bitácora de Backup.
- ✓ Pruebas de restauración de copias de seguridad.

4. LINEAMIENTOS DE OPERACIÓN

- Los jefes o líderes de área son los responsables de garantizar que la información institucional que produzcan sea almacenada en las unidades organizativas de drive asignadas a cada área u oficina.
- Los jefes o líderes de área son los responsables de solicitar el acceso a los diferentes usuarios a través de la mesa de ayuda indicando los permisos correspondientes (Lector, editor, gestor de contenido) en el formato establecido para tal fin.
- La copia de seguridad de las cuentas institucionales de correo y drive, se realizarán a través de la herramienta que tenga habilitada el área de tecnología.
- La copia de seguridad de los servidores y documentos contenidos en las carpetas compartidas en red de los file Server, se ejecutan a través de un agente de copiado y se almacena la información en la nube.
- La copia de seguridad realizada al controlador de dominio, al servidor de BD y al servidor donde se aloja el sistema de biblioteca, es protegida a través de un medio de encriptación en la ejecución del backup.
- No se realiza backup a la información histórica almacenada en los file server de la cual se evidencie que no ha tenido modificaciones en el último año.
- El servicio de restauración y entrega de backup debe ser solicitado a través de la mesa de ayuda por el líder o jefe de área para información del drive del área o dependencia y por el funcionario o contratista para el drive personal; en caso de que el usuario se haya retirado del instituto éste puede realizar la solicitud de información del drive personal únicamente a través del área de correspondencia mediante petición formal y debe entregar el medio removible en el que se almacenará lo solicitado.
- Para la copia de seguridad de los servicios web, sistemas de información, servicios locales y cuentas de correo institucional, se establecen los criterios de copiado y periodos de retención como se muestra a continuación.



GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

CÓDIGO: GTI-PR-04

VERSIÓN: 01

PROCEDIMIENTO RESPALDO DE INFORMACIÓN Y RESTAURACIÓN DE COPIAS DE SEGURIDAD

PÁGINA: 2 de 6

Documento de Carácter

Público

Reservado

Clasificado

COPIA DE SEGURIDAD	GRADO	PROGRAMACIÓN
Bases de datos, Servidor de archivos, Servicios consumidos desde los servidores (Directorio Activo, WSUS, DHCP, DNS).	Incremental Diferencial Completo	Diario Semanal Mensual
Cuentas de correo electrónico y drive de usuarios	Completo	Semanal
Sistema Atlas Geográfico, OJS, OMP, SIG.	Completo Transaccional Diferencial	Mensual Diario
Sistema documental.	Incremental Completo	Diario Semanal Mensual

PERÍODOS DE RETENCIÓN			
INFORMACIÓN	TIEMPO		
	Diario	Semanal	Mensual
Información de servidores, servicios consumidos desde los servidores y SI en servidor local	2 semanas	4 semanas	26 semanas
Correo electrónico y drive	NA	8 semanas	NA
Sistema Atlas Geográfico, OJS, OMP, SIG	1 semanas	4 semanas	NA
Orfeo	2 semanas	4 semanas	26 semanas

- Se debe monitorear los eventos y estados de los trabajos programados en las herramientas de backup, en caso de generarse un error o falla en la ejecución de la copia de seguridad se debe repetir de nuevo el trabajo.
- Se deben realizar pruebas semestrales de recuperación de la información verificando la calidad de los datos de la copia de seguridad.
- Se deben realizar pruebas de restauración de la copia de seguridad realizada a las cuentas de correo institucional a través de la herramienta que disponga el área de Tecnología documentando el resultado.
- La bitácora de backup se debe actualizar diaria, semanal y mensualmente.
- Se establecen indicadores de gestión para el seguimiento y correcto funcionamiento de las copias de seguridad realizadas y restauradas.

NOMBRE	DESCRIPCIÓN	VARIABLE	FÓRMULA	PERIODICIDAD	UNIDAD DE MEDIDA
Porcentaje de restauraciones de datos exitosas	Mide la efectividad de las restauraciones según el porcentaje de restauraciones de datos exitosas.	PRE: Porcentaje de restauraciones de datos exitosas. RE: Número de restauraciones exitosas. TR: Total restauraciones realizadas.	$PRE = (RE/TR) * 100$	Semestral	Porcentaje
Porcentaje de copias de seguridad realizadas exitosamente	Mide el promedio de copias de seguridad de información realizadas con éxito.	PB: Porcentaje de backup de datos exitosos B: Número de backup ejecutados exitosamente TB: Total de backup realizados	$PB = (B/TB) * 100$	Semestral	Porcentaje



GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

CÓDIGO: GTI-PR-04

VERSIÓN: 01

PROCEDIMIENTO RESPALDO DE INFORMACIÓN Y RESTAURACIÓN DE COPIAS DE SEGURIDAD

PÁGINA: 3 de 6

Documento de Carácter

Público

Reservado

Clasificado

5. DEFINICIONES

- **Aplicaciones:** Son programas que apoyan los procesos o tareas concretas que realizan los usuarios en su labor diaria.
- **Base de datos:** Es un almacén de datos que permite almacenar un conjunto de información de manera organizada de forma que pueda ser administrada, consultada y utilizada.
- **Carpeta compartida en red:** Es el entorno de la red local del ICANH donde es posible conectar varios ordenadores, proporcionar accesos con distintos niveles de privilegios a los usuarios sobre las carpetas compartidas creadas a para cada dependencia, teniendo así acceso a los mismos archivos y trabajar de forma colaborativa.
- **Copia de seguridad - Backup:** Una copia de seguridad consiste en resguardar y salvaguardar la información del negocio, con el fin de recuperarla en caso de fallos garantizando la continuidad y conservación de la información.
- **Custodia:** Es el medio de supervisión y control de los soportes generados en la nube de la copia de seguridad, permitiendo la integridad y conservación de la información
- **Medio removible:** Dispositivo de almacenamiento independiente del computador que puede ser transportado libremente.
- **Servidor de archivos – File server:** Es un equipo físico que se coloca a disposición del cliente y proporciona a los usuarios un lugar de almacenamiento para los archivos y soportes de datos.
- **Unidad organizativa (Drive):** Son unidades compartidas que permiten almacenar información de las diferentes dependencias y facilita el trabajo colaborativo entre los miembros de estas unidades.

6. DESCRIPCIÓN DE ACTIVIDADES

No	Actividad	Descripción	Responsable Cargo y/o Grupo responsable / Dependencia	Registro resultado (Documento Evidencia)	Punto de Control
1.	Guardar la información en los servicios definidos y asignados por el área de tecnología	El funcionario o contratista debe cargar los documentos institucionales importantes y críticos en las carpetas o unidades compartidas asignadas tanto al drive personal como al del proceso/área/dependencia.	Funcionarios contratistas.	y Unidad de Drive, unidad de red,	
2.	Solicitar restauración de información.	Solicitar a través de mesa de ayuda la restauración de la información requerida especificando el tipo de información (correo, drive, etc.) a restaurar y el rango de fechas requerido (semana, mes, año, etc.) cuando aplique. En caso de que la información la solicite un exfuncionario la solicitud la debe realizar por medio del área de correspondencia mediante petición formal especificando la información requerida y facilitando el medio	Funcionarios contratistas, exfuncionarios	y Tiquete mesa de ayuda, Petición en sistema documental.	



GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

CÓDIGO:
GTI-PR-04
VERSIÓN:
01

PROCEDIMIENTO RESPALDO DE INFORMACIÓN Y RESTAURACIÓN DE COPIAS DE SEGURIDAD

PÁGINA:
4 de 6

Documento de Carácter

 Público

 Reservado

 Clasificado

6. DESCRIPCIÓN DE ACTIVIDADES					
No	Actividad	Descripción	Responsable Cargo y/o Grupo responsable / Dependencia	Registro resultado (Documento Evidencia)	Punto de Control
		o unidad de almacenamiento al área de tecnología para el suministro de dicha información.			
3.	Verificar si se requiere restaurar información.	Verificar si se requiere restaurar información de algún usuario para continuar en la siguiente actividad, de lo contrario pasar a la actividad No. 6.	Responsable infraestructura/ Área de tecnología	Tiquete mesa de ayuda, Petición en sistema de gestión documental.	
4.	Restaurar información solicitada.	De acuerdo con la información solicitada se procede a ubicar la copia de seguridad de ésta para realizar la restauración requerida.	Responsable infraestructura/ Área de tecnología	Tiquete mesa de ayuda, Petición en sistema de gestión documental.	
5.	Entregar información solicitada.	Entregar la copia de la información al solicitante de esta y proceder a cerrar el caso en mesa de ayuda o la petición correspondiente en el sistema de gestión documental y continuar en la actividad No. 11.	Responsable infraestructura/ Área de tecnología	Tiquete mesa de ayuda, Petición gestionada.	
6.	Realizar copia de seguridad a cada servicio.	De acuerdo con los criterios de copiado y periodos de retención estipulados en los lineamientos de este documento, se debe ejecutar la copia de seguridad de los servicios web, sistemas de información, servicios locales y cuentas de correo institucional.	Responsable infraestructura/ Área de tecnología.	Consola de Backup	
7.	Verificar la información de la copia de seguridad	Verificar la información de la copia de seguridad realizada a los diferentes servicios. Desde la consola de administración de backup se realiza el seguimiento con el fin de verificar que la copia de seguridad se haya ejecutado sin errores, en caso de presentar alguna inconsistencia se debe volver a ejecutar la tarea de backup hasta que quede ejecutada sin ningún tipo de error.	Responsable infraestructura/ Área de tecnología.	Consola de Backup	Validar que la ejecución del backup no presente ningún tipo de error.
8.	Diligenciar registro ejecución de copias de seguridad	Se debe llevar un registro de las copias de seguridad realizadas y almacenadas en el formato de bitácora de copia de seguridad.	Responsable infraestructura/ Área de tecnología.	Bitácora de copia de seguridad	
9.	Realizar pruebas de restauración.	Para verificar la integridad y calidad de la información se debe realizar semestralmente la restauración de los datos según lo definido en los lineamientos de este documento. En caso de que alguna de las pruebas realizadas presente fallas en la restauración se debe solicitar mediante la herramienta	Responsable infraestructura/ Área de tecnología	Registro y control de restauración de backup, Consola de backup	Verificar la integridad y calidad de la información.

	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	CÓDIGO:	GTI-PR-04
		VERSIÓN:	01
	PROCEDIMIENTO RESPALDO DE INFORMACIÓN Y RESTAURACIÓN DE COPIAS DE SEGURIDAD	PÁGINA:	5 de 6

Documento de Carácter

Público Reservado Clasificado

6. DESCRIPCIÓN DE ACTIVIDADES					
No	Actividad	Descripción	Responsable Cargo y/o Grupo responsable / Dependencia	Registro resultado (Documento Evidencia)	Punto de Control
		pertinente el soporte al proveedor de backup.			
10.	Mantener en custodia la información.	Se almacena la información del respaldo realizado en la nube, cumpliendo con los periodos de retención para cada servicio de acuerdo a los lineamientos establecidos en este documento.	Responsable infraestructura/ Área de tecnología.	Consola de backup	
11.	Evaluar servicios de restauración	Mediante la herramienta de mesa de ayuda se procede a enviar la encuesta de satisfacción al solicitante para evaluar el servicio recibido en calidad y oportunidad.	Responsable infraestructura/ Área de tecnología.	Evaluación del servicio.	

7. DIAGRAMA DE FLUJO
N.A.

8. REGISTROS (Documentos que generan evidencia de la ejecución del procedimiento)	
Nombre del registro	Almacenamiento
Copia de seguridad servicios web, sistemas de información, servicios locales y cuentas de correo institucional	Nube proveedor Backup
Registro y control de restauración copias de seguridad	Unidad compartida del área de tecnología/Registro backup/año
Bitácora Seguimiento de Backup.	Unidad compartida del área de tecnología/bitácora backup/año
Tiquete de mesa de ayuda.	Mesa de ayuda por consecutivo.
Petición de restauración.	Sistema de gestión documental.
Formato de solicitud de instalación de software, acceso a servicios de ti y permisos a unidades compartidas.	Unidad compartida del área de tecnología/Permisos/ año.

9. ANEXOS
Formato registro y control de restauración de backup
Bitácora Seguimiento de Backup

	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	CÓDIGO:	GTI-PR-04
		VERSIÓN:	01
	PROCEDIMIENTO RESPALDO DE INFORMACIÓN Y RESTAURACIÓN DE COPIAS DE SEGURIDAD	PÁGINA:	6 de 6

Documento de Carácter

Público

Reservado

Clasificado

10. CONTROL DE CAMBIOS		
Versión	Fecha	Descripción general del cambio
01	2022-12-09	Se actualiza el documento de acuerdo con el nuevo formato en el cual se incluyen los lineamientos de operación, entradas y registros que se generan como evidencia de la ejecución del procedimiento, a su vez se actualiza debido al cambio de herramienta para copias de seguridad del instituto.

COPIA NO CONTROLADA

ELABORÓ	REVISÓ	APROBÓ
Cargo: Profesional Área Funcional de Tecnología y Sistemas de Información.	Cargo: Líder del Área Funcional de Tecnología y Sistemas de Información. Jefe Oficina Asesora de Planeación	Cargo: Líder del Área Funcional de Tecnología y Sistemas de Información.
Fecha: 2022-11-11	Fecha: 2022-11-22	Fecha: 2022-12-09