1. OBJETIVO

Definir las actividades para atender los requerimientos de copias de respaldo o restauración que permitan la preservación, uso y recuperación de la información en caso de un fallo o desastre en la infraestructura tecnológica de la Unidad Administrativa Especial Direcciónde Impuestos y Aduanas Nacionales - UAE DIAN.

2. ALCANCE

Inicia con la solicitud de la copia por parte de los dueños de la información, definición de políticas, programación, ejecución, verificación y finaliza con las pruebas de restauración de la información contenida en las copias de respaldo según lo establecido.

3. DOCUMENTOS RELACIONADOS

Tipo de documento	Código	Titulo	Modo de uso	Clasificación documento
Manual	MN-IIT-0072	Manual de políticas y lineamientos de seguridad de la información	Digital	Interno
Procedimiento	PR-IIT-0460	Gestión de Requerimientos	Digital	Interno
Formato	FT-IIT-2815	Políticas de Copias de Respaldo	Digital	Interno
Formato	FT-IIT-2816	Pruebas de Restauración Copias de Respaldo	Digital	Interno

4. DEFINICIONES Y SIGLAS

- **Administrador de Servicio**. Es la forma en que los equipos de TI administran la prestación de servicios de TI, de extremo a extremo, a los clientes. Esto incluye todos los procesos y actividades para diseñar, crear, ofrecer y dar soporte a los servicios de TI.

  Fuente: Consultado en https://inlogiq.com/que-es-la-administracion-de-servicios-de-ti-itsm/

- **Administrador de Servidor**. Es una consola de administración que ayuda a los profesionales de TI a aprovisionar y administrar servidores locales y remotos desde sus escritorios, sin necesidad de tener acceso físico a los servidores

  Fuente: Consultado en https://learn.microsoft.com/es-es/windows-server/administration/server-manager/server-manager

- **Copia de respaldo.** Una copia de todo o parte del software o archivos de datos en un sistema preservado en medios de almacenamiento, como cinta magnética o disco, o en un sistema separado para que los archivos puedan restaurarse si los datos originales se eliminan o dañan.

  Fuente: Libro: A Glossary of Archival and Records Terminology. Autor: Richard Pearce-Moses.Página: 45

- **Restauración de información.** Recuperar los datos y las aplicaciones y las operaciones empresariales de las que dependen en caso de que los datos y las aplicaciones originales se pierdan o resulten dañados debido a un corte de energía, un ciberataque, un error humano, un desastre o cualquier otro suceso imprevisto.

  Fuente: Copia de seguridad y restauración: una guía esencial | IBM (https://www.ibm.com/mx-es/topics/backup-and-restore

- **Sistemas de archivos.** Un sistema de archivos, sistema de ficheros o file system es el conjunto de procesos y normas que se llevan a cabo para el almacenamiento de un dispositivo de memoria. Este sistema le permite al usuario identificar la ubicación de los archivos y poder acceder a ellos de una forma rápida

  Fuente: Consultado en https://keepcoding.io/blog/que-es-un-sistema-de-archivos

- **TRD – Tabla de retención documental.** Se define como el listado de series, con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos, es decir se considera como el Instrumento que permite establecer cuáles son los documentos de una entidad, su necesidad e importancia en términos de tiempo de conservación y preservación y que debe hacerse con ellos una vez finalice su vigencia o utilidad.

  Fuente: Archivo General de la Nación –Colombia https://www.archivogeneral.gov.co/transparencia/gestion-informacion-publica/Tablas-de-Retencion-Documental-TRD

5. DESARROLLO DEL TEMA

5.1 Condiciones Generales

- El presente documento describe las actividades de solicitud, programación, ejecución, verificación y pruebas de restauración de las copias de respaldo sobre la infraestructura tecnológica que soporta los servicios, aplicaciones y plataformas priorizadas en el documento BIA (Análisis de Impacto de Negocio) de la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales - UAE DIAN.

- La estrategia consiste en generar dos copias de respaldo alojadas en diferentes sitios de acuerdo con los tiempos de retención definido por los procesos de la Entidad. Esto significa la replicación de backups entre los dos datacenter SITE1 Y SITE2.

- Las copias de respaldo se realizan en cinco etapas, las cuales se explican en el desarrollo del presente documento:

El administrador de las copias de respaldo debe garantizar copias de seguridad vigentes de la herramienta de respaldo donde incluya: la configuración del servidor, la configuración de la herramienta, la base de datos de la herramienta.

- Se realizará el respaldo de los activos tipo información y software, clasificados como se indica en el documento “PR-IIT-0366 Gestión de activos de información”.

- Entre los activos de información o software a respaldar se encuentra:

  - Bases de datos
  - Servidores de archivos
  - Servidores WEB
  - Servidores de Aplicaciones
  - Dispositivos de Red
  - Dispositivos de Seguridad
  - Equipos de usuario final

- Se realizará copia de los equipos de usuario final que estén en situación administrativa como: retiro, pensión o fallecimiento, o por motivos de investigación, de acuerdo con solicitud registrada en la mesa de servicio. Para los funcionarios activos aplica los lineamientos informados a través del Memorando 000255 del 29 de diciembre 2021 y sus anexos.

- Las copias de respaldo se realizan con frecuencia diaria, mensual, semestral, anual o por demanda cuando existan situaciones particulares o reprocesos en caso de falla.

- Cuando se realicen las restauraciones se informará al área o proceso solicitante, el tiempo de la actividad para que se tenga en cuenta para los RPO´s definidos en el documento “Análisis de Impacto de Negocio – BIA (Business Impact Analysis)”.

- El tiempo de retención preestablecido en todos los casos, con excepción de aquellos en los que el administrador del servicio disponga algo diferente, será así:

Frecuencia	Descripción	Tiempo de Retención
Diarios	Copias diarias tomadas de lunes a domingo	60 días
Mensuales	Copias tomadas al inicio o fin de mes	1 año
Semestral	Copias tomadas el 30 junio	5 años
Anual	Copias tomadas cada 31 de diciembre	5 años
SIGLO XXI	Copias incrementales	10 años
No programado y a solicitud	Copias tomadas cada que se necesitan	60 días

- Las copias de respaldo se definirán como incremental y completa.

- La información de los activos respaldados se almacenará teniendo en cuenta técnicas de compresión y cifrado como lo establece el documento “MN-IIT-0072 Manual de políticas y lineamientos de seguridad de la información en el numeral 5.4.13 Copia de seguridad de la información”.

- La Subdirección de Infraestructura Tecnológica y Operaciones se compromete a respaldar las copias de acuerdo con su periodo de retención.

- Las pruebas de restauración de copias de respaldo se realizan de acuerdo con la solicitud del área o proceso solicitante.

5.2 Descripción de actividades

5.2.1 Solicitud de Copias de Respaldo

El área o Proceso de la Entidad solicitante, debe realizar el requerimiento de copia de respaldo a través de la Mesa de Servicio, entregando la siguiente información como mínimo:

- Nombre del Solicitante
- Dirección Organizacional a la que pertenece en la Entidad
- Subdirección Organizacional a la que pertenece en la Entidad
- Nombre de la copia (el nombre debe estar relacionado con el tipo de información contenida o nombre de la base de datos)
- Activo de información
- Descripción
- Proceso
- Aplicación o servicio de la entidad a la que pertenece.
- Tipo de Información, frecuencia, origen (ubicación) y tamaño de la información a respaldar.
- Lo anterior debe estar aprobado por el dueño del proceso de la Entidad que requiere implementar las copias de respaldo.

5.2.2 Programación de Copias de Respaldo

El administrador de las copias a cargo incluye dentro de la agenda de la herramienta de respaldos, la programación de las copias de respaldo de acuerdo con las políticas solicitadas. También mantiene un registro actualizado en el Formato FT-IIT-2815. Registro de Políticas de Copias de Respaldo para cada activo de información a respaldar.

5.2.3 Ejecución de la copia de respaldo

El administrador de las copias de respaldo debe realizar seguimiento a la ejecución de estas, verificando que se hagan en las fechas y horas programadas. Debe verificar la ejecución tanto de la copia 1 como de la copia 2. Es importante también llevar un control y registro diario de los tiempos de ejecución y del tamaño de las copias con el fin de identificar alertas de capacidad y decisiones oportunas en crecimientos.

5.2.4 Verificación de la ejecución de la copia de respaldo

El administrador de las copias de respaldo, a través de la herramienta, debe verificar el estado de

la ejecución de la copia, concluir si se realizó correctamente en cuanto a completitud, frecuencia, y ubicación. En caso de identificarse un error debe tomar las acciones necesarias que garanticen que la copia se ejecute correctamente. Se debe registrar el resultado de esta verificación y acciones tomadas.

5.2.5 Restauración de información de las copias de respaldo

La restauración se realiza como control y a solicitud del área o proceso dueño de la información a respaldar:

Como control:

- Se debe generar un cronograma de pruebas de restauración de copias de respaldo acordado con el área o proceso solicitante, las cuales pueden ser priorizadas o aleatorias, con el fin de evitar la restauración innecesaria de datos.

- Se deben hacer como mínimo 1 vez por semestre.

- El administrador de las copias de respaldo debe realizar la verificación de la integridad de la copia de respaldo:

  - Comprobar el tamaño de los datos, que determinará si el tamaño coincide con el tamaño esperado para verificar que la copia de seguridad esté completa y sin errores.

  - Confirmar la fecha y hora de creación, para determinar si corresponde con la fecha en que se realizó la copia y verificar que sea una copia válida y sin modificaciones.

- El área o proceso solicitante debe realizar la verificación de los datos:

  - Revisar la estructura de datos para verificar que todos hayan sido restaurados.

  - Verificar que los datos se encuentren en su ubicación correspondiente.

  - Validar que no haya datos faltantes o duplicados.

- Si se encuentra algún error o inconsistencia en la información, se debe realizar nuevamente el procedimiento de restauración.

- Las pruebas y los resultados de la restauración serán debidamente documentados y en caso de presentar alguna incidencia que no pueda ser solucionada se debe reportar en la documentación como una situación específica observada.

- El registro de las pruebas y resultados de la restauración se deberán registrar en el formato FT-IIT-2816. Pruebas de Restauración de Copias de Respaldo.

  - Las pruebas de restauración quedarán registradas en la herramienta de recuperación y demás evidencia que se generen en el desarrollo del procedimiento.

Por solicitud

- Se deben solicitar a través de la mesa de servicios.
- Realizar la verificación de la integridad y de datos de la copia de respaldo como en el numeral anterior.
- Si se encuentra algún error o inconsistencia en la información, se debe realizar nuevamente el procedimiento de restauración.
- Las pruebas y los resultados de la restauración serán debidamente documentados y en caso de presentar alguna incidencia que no pueda ser solucionada se debe reportar en la documentación como una situación específica observada.
- Realizar el registro de las pruebas y resultados de la restauración como en el punto anterior
- Las pruebas de restauración quedarán registradas en la herramienta de recuperación y demás evidencia que se generen en el desarrollo del procedimiento.

6. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de Cambios	Tipo de información
	Desde	Hasta		
1	10/09/2021	14/11/2022	Versión inicial, Se deroga el procedimiento: • PR-SI-0343 Toma y custodia de copias de respaldo Se derogan los siguientes instructivos: • IN-SI-0172 Toma de Copias de Respaldo MCAFEE WEB GATEWAY • IN-SI-0173 Toma de Copias de Respaldo SYMANTEC • IN-SI-0174 Respaldo de Logs y Configuraciónen FIREWALL CHECKPOINT	No aplica
2	15/11/2022	20/04/2025	Versión 2 que reemplaza lo establecido en la versión 1. Se modifica Objetivo, Numeral 3. *Definiciones y Siglas* y Numeral 4. *Desarrollo del Tema.* Se actualiza la plantilla del presente documento, de acuerdo con la versión 5 del procedimiento"*PR-PEC-0001 Documentación del sistema de gestión*".	Esta versión corresponde a información pública
3	21/04/2025		Versión 3 que reemplaza lo establecido en la versión 2. Se modifica título, objetivo, alcance, condiciones generales, definiciones y siglas, Desarrollo del tema de acuerdo con lo establecido en el numeral 5.4.13 Copia de seguridad de la información del documento MN-IIT-0072 Manual de políticas y lineamientos de seguridad de la información.	Esta versión corresponde a información pública

Elaboró:	Angela Paola Maldonado García **Elaboración técnica**	Gestor	Subdirección de Infraestructura Tecnológica y Operaciones
	Claudia Marcela Lucena Pérez **Elaboración técnica**	Gestor	
	Gilbert Darío Ortega Samboní **Elaboración técnica**	Gestor	
Revisó:	Hector Leonel Mesa Lara	Inspector	Subdirección de Infraestructura Tecnológica y Operaciones
	Diego Mauricio Calderón Pérez	Inspector	
Aprobó:	Juan Carlos Vizcaíno Novoa	Subdirector	Subdirección de Infraestructura Tecnológica y Operaciones