Instructivo para la generación de copias de respaldo (BACK-UP)

Proceso
Gestión de Servicios de Información y Proyectos Tecnológicos
Versión 1
15/06/2023

TABLA DE CONTENIDO

INTRODUCCIÓN 3
1 OBJETIVO 4
2 ALCANCE 4
3 ROLES Y RESPONSABILIDADES 5
4 DEFINICIONES 5
5 DESCRIPCIÓN DEL PLAN 7
6 PLAN DE GENERACIÓN DE COPIAS DE RESPALDO (INFRAESTRUCTURA) 8
7 BIBLIOGRAFIA 19

INTRODUCCIÓN

El presente documento define las actividades relacionadas con la generación de copias de respaldo de la entidad, aplicando las mejores prácticas y estándares internacionales, los cuales proporcionan lineamientos mínimos para proteger y garantizar que los activos de la entidad (infraestructura en nube, aplicaciones, código fuente, bases de datos y activos de información entre otros), se mantengan respaldados y sean fácilmente recuperables en el momento que se necesite, manteniendo su integridad, confidencialidad y disponibilidad.

En este contexto es importante resaltar que, para la correcta ejecución de las actividades establecidas en el plan de generación de copias de respaldo de los activos, se deben analizar detenidamente las políticas de operación, como premisa a la aplicación de las actividades relacionadas en este documento.

El propósito principal de este documento es establecer e implementar estrategias que permitan generar, recuperar y mantener las copias exactas de la información y datos vitales almacenados en los componentes tecnológicos del centro de datos del Ministerio de Ambiente y Desarrollo Sostenible, en caso de presentarse un incidente de seguridad o una falla operativa en alguno de los equipos o componentes tecnológicos, para garantizar la restauración de los mismos y que de alguna manera la entidad pueda recuperarse a tal eventualidad. Dentro de las estrategias principales definidas en el presente documentos se encuentran:

- Proporcionar un modelo operativo estándar para las copias de seguridad de la información de la entidad.
- Establecer un estándar para el almacenamiento y la recuperación de la información.
- Generar lineamientos para la generación de las copias de seguridad para crear, recuperar y mantener las copias de la información generada por la Entidad, a fin de cumplir con su misionalidad y funcionamiento.

1 OBJETIVO

Definir los lineamientos para la generación de copias de respaldo (Back-up), siguiendo las mejores prácticas para proteger la información, activos de información, bases de datos, configuración e información crítica acorde con el inventario de activos de información del Ministerio de Ambiente y Desarrollo Sostenible, permitiendo salvaguardar la integridad, confidencialidad y disponibilidad de la información, con el propósito de mitigar las consecuencias de incidencias, problemas, siniestros o posibles desastres que llegase a ocurrir y de alguna manera la entidad pueda recuperarse a tal eventualidad.

2 ALCANCE

Inicia con la planeación de la generación del respaldo de la información almacenada bajo la infraestructura del Ministerio de Ambiente de acuerdo con el Plan de Backups, y finaliza con la ejecución y verificación de las copias de seguridad. Estos lineamientos aplican para los siguientes activos de información:

- ✓ Bases de datos en producción
- ✓ Código fuente
- ✓ Activos de información
- ✓ Configuración de infraestructura
- ✓ Configuración de redes
- ✓ File Server
- ✓ Directorio activo
- ✓ Correo electrónico

Las actividades relacionadas con la ejecución de copias de respaldo finalizan las pruebas aleatorias de la restauración de las copias de respaldo el cual debe asegurar la recuperación de los datos y garantizar la integridad de estos.

3 ROLES Y RESPONSABILIDADES

Basado en la Matriz RACI (*Responsible, Accountable, Contribute, and Inform*), los siguientes grupos y/o personas son identificados para asegurar que la información sea respaldada y almacenados correctamente.

ACTIVIDAD	JEFE OFICINA TIC	EQUIPO DE INFRAESTRUCTURA	EQUIPO DE SEGURIDAD
Estrategias De Respaldo	I		C
Programación Copias De Respaldo		R	C
Monitoreo/*Troubleshooting*	I	R	C
Etiquetado	I	R	
Validación Respaldos		R	A
Recepción/Almacenamiento	I	R	C
Respaldo de Acuerdo A La Programación	I	R	C
Restauración Copias De Respaldo	I	C	R

***Fuente**: Elaboración propia*

R: Responsable **A**: A quién Informar **C:** Consultado **I:** Informado

Equipo de Infraestructura: Se encuentra conformado por el personal asignado por la jefatura de la Oficina TIC (Funcionarios y/o contratistas), quienes gestionan y administran los diferentes componentes de hardware y software implementados en la infraestructura tecnológica de la entidad.

Equipo de Seguridad de la información: Se encuentra conformado por personal de la entidad, responsables de gestionar los elementos del Sistema de Gestión de Seguridad de la información, que incluye procedimientos, lineamientos, políticas, entre otros; diseñadas para proteger los activos de información de la entidad, para garantizar su confidencialidad, disponibilidad e integridad.

4 DEFINICIONES

BACK-UP: Es una copia de seguridad de los archivos, aplicaciones y bases de datos originales, disponibles en unidades de almacenamiento (generalmente discos extraíbles, unidades de cinta), con el fin de poder recuperar la información en caso de un daño, borrado accidental, accidente imprevisto o pérdidas. Es conveniente realizar copias de seguridad y verificación de estas a intervalos temporales fijos (diario, semanal, mensual, por ejemplo), en función de la importancia de los datos manejados o la criticidad que ello represente

para garantizar la continuidad de servicio de la entidad. Estas copias son útiles ante de diferentes eventos tales como: Catástrofes naturales, informáticas o ataque informáticos.

Base de Datos: Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente. En una base de datos, la información se organiza en campos y registros. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo.

Contingencia: Conjunto de actividades de recuperación. Las acciones por contemplar aplican para Antes-Durante- Después con el fin de reducir las pérdidas de información generadas por eventos inesperados.

Plan de Contingencia: Actividades alternativas de una entidad cuyo fin es permitir el normal funcionamiento de esta y garantizar la continuidad de las operaciones, aun cuando algunas de sus funciones se vean afectadas por un accidente interno o externo.

Recuperación: Hace referencia a las técnicas empleadas para recuperar 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: Volver a poner algo en el estado inicial. Una base de datos se podría restaurar en otro dispositivo después de un desastre.

Directorio Activo: Servicios que se ejecutan en Windows Server para administrar permisos y acceso a recursos en red. El directorio activo almacena datos como objetos. Un objeto es un elemento único, como un usuario, grupo, aplicación o dispositivo, como una impresora.

Activos de información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, hardware, software, sistemas de información, edificios, personas, imagen, etc.) que tenga valor para la entidad. Ej.: La información física y digital; el software; el hardware; los servicios de información, de comunicaciones, de almacenamiento, etc.; las personas y otros, recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.

Repositorio: Es una ubicación de almacenamiento donde puede almacenar paquetes de software o el código fuente de una aplicación. Se puede acceder e instalar estos paquetes de software, cuando sea necesario, en la infraestructura de la entidad. El uso de estos repositorios facilita el almacenamiento, el mantenimiento y la copia de seguridad del código fuente**.**

File Server: Instancia de servidor central de una red de ordenadores que permite a los clientes conectados acceder a sus propios recursos de almacenamiento.

5 DESCRIPCIÓN DEL PLAN

El propósito del presente instructivo para la generación de copias de respaldo es establecer e implementar las diferentes actividades para crear, recuperar y mantener las copias de la información generada por la entidad, a fin de cumplir con su misionalidad y funcionamiento. En el caso de un desastre, es vital que la información esté disponible en una ubicación alternativa para ser utilizado con fines de recuperación. Este documento define las actividades que la entidad debe cumplir para seguir los estándares y normas aplicadas en el procesamiento de los respaldos.

Estrategias del Plan (PHVA)

- **Planeación:** Establecer cada una de las estrategias y lineamientos para garantizar la realización de las copias de respaldo, así como sus respectivas pruebas de restauración y almacenamiento.
- **Hacer:** Desarrollar cada una de las actividades contempladas en el proceso de Backup. Realizar actividades para la recuperación de información cuando sea necesario.
- **Verificación:** Supervisión de los BKF o Backup Datos por tamaño y fecha de modificación y registro diario en la bitácora de control de Backups.
- **Actuar**: Hacer seguimiento al proceso de Backups, mediante la ejecución de manera periódica de pruebas de restauración de algunas copias de backup para garantizar su correcto funcionamiento. En caso de que los Backups no se estén realizando correctamente se deberá informar inmediatamente al responsable de esta actividad para tomar los correctivos necesarios.

6 PLAN DE GENERACIÓN DE COPIAS DE RESPALDO (INFRAESTRUCTURA)

En el presente apartado se describen las diferentes estrategias para garantizar el correcto funcionamiento del esquema de backups, definiendo los diferentes escenarios que hacen parte de la arquitectura tecnológica actual de la entidad, los cuales son necesarios para proteger y respaldar los activos de información y de esta manera garantizar fácilmente su recuperación en el momento de ser requerido.

DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE RESPALDO SERVIDORES VIRTUALES	
ACTIVIDADES ESENCIALES	▪ Realizar las copias de respaldo de los servidores virtuales actualmente en producción, de una manera óptima y práctica, para su posterior almacenamiento por fechas y disposición para restauraciones programadas y de emergencia. ▪ Es necesario realizar una copia de seguridad de las máquinas virtuales en producción, que contenga la estructura en hardware virtual, tales como Memoria, Procesamiento, Dispositivos de red, Discos duros virtuales, entre otros, compatible con la estructura de virtualización VMWARE ESXi 6.5 actualmente en producción en el Ministerio. ▪ Realizar copias de respaldo de la información almacenada en el SERVIDOR DE ARCHIVOS FILE SERVER, enfocada a la Data contenida en los recursos compartidos asignados a las áreas de trabajo en el Ministerio de Ambiente y Desarrollo Sostenible
TIPO	Servidores Virtuales – Servidor File Server
UBICACIÓN	Infraestructura *ON PREMISE*
PASO A PASO PARA GENERAR LA COPIA DE RESPALDO	▪ Por medio de la herramienta generadora de copias de respaldo, se realiza la integración con la infraestructura de los servidores virtuales, y se seleccionan los que correspondan a producción, entre ellos: MV de Aplicaciones, MV de Base de Datos, **SERVIDOR DE ARCHIVOS FILE SERVER y MV** que correspondan al funcionamiento de la infraestructura tecnológica, además de los otros que sean previamente solicitados. ▪ Mediante la herramienta generadora de copias de respaldo, se realiza una programación por medio de JOBs de una tarea donde se ejecutarán periódicamente dos tipos de Backups: • Backup Tipo Full: Realizado al inicio de la ejecución del JOBs. Este tipo de backup contendrá una copia íntegra 100% de la Máquina virtual previamente seleccionada. • Backups completos Tipo FULL: Como su propio nombre indica, este tipo de respaldo copia la totalidad de los datos. La ventaja principal de la realización de un backup completo en cada operación es que se dispone de la totalidad de los datos en un único conjunto. Esto permite restaurar los datos en un tiempo mínimo, lo cual se mide en términos de objetivo de tiempo de recuperación (RTO). No obstante, el inconveniente es que lleva más tiempo

	realizar un respaldo completo que de otros tipos (a veces se multiplica por un factor 10 o más), y requiere más espacio de almacenamiento. • Backups Tipo Incremental: Este tipo de respaldo sólo copia los datos que han variado desde la última operación de backup realizada de cualquier tipo. Se suele utilizar la hora y fecha de modificación de los archivos, comparándola con la hora y fecha de la última copia de seguridad. Las aplicaciones de respaldo identifican y registran la fecha y hora de realización de las operaciones de respaldo para identificar los archivos modificados. Dado que la copia de seguridad incremental sólo copia los datos a partir del último respaldo de cualquier tipo, se puede ejecutar tantas veces como se desee, pues sólo guarda los cambios más recientes. La ventaja de una copia de seguridad incremental es que copia una menor cantidad de datos que un respaldo completo. Por ello, esas operaciones se realizan más rápido y exigen menos espacio para almacenar la copia de seguridad. Este tipo de Backup debe ser ejecutado cada 15 días calendario, es decir, los primeros días de cada mes y a mediados del mismo. ▪ Una vez realizada la tarea programada por el JOB, las copias de seguridad se deberán almacenar en los Data Storage (Discos duros de almacenamiento en la infraestructura del Ministerio) referenciados por tipo de Backup y fecha de creación, dispuestos por la herramienta de generación de Backup. ▪ Se cuenta con un esquema para realizar la revisión de restauración. Esta operación se debe realizar 1 vez al mes, sobre cada una Máquinas Virtuales de forma tal que se garantice que la copia de seguridad quedó generada de forma correcta y su retención se hará de acuerdo con lo especificado por los propietarios de la información. ▪ Para realizar las actividades de restauración de las copias de respaldo, se deben seguir los siguientes lineamientos: • Seleccionar el backup que se quiere restaurar, uno por cada Máquina Virtual. • Descomprimir el backup. • Restaurar el backup en un ambiente de Pruebas. • Comprobar el funcionamiento de la restauración y en caso de ser fallido actualizar el backup y el paso a paso de este, y probar nuevamente. • La restauración del backup del SERVIDOR DE ARCHIVOS FILE SERVER se realiza por medio de la restauración granular mediante las herramientas actuales implementadas en la entidad. La restauración granular consiste en recuperar solo una parte de los datos, permitiendo conservar todos los datos más actualizados hasta la fecha, en sustitución de pequeñas piezas de datos que hayan sido borrados o dañados accidentalmente.
RESPONSABLE	Equipo de Infraestructura Minambiente (Infraestructura)

DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE RESPALDO CUENTA CORREO CORPORATIVO	
ACTIVIDADES ESENCIALES	Generar las copias de respaldo de las cuentas de correo corporativo correspondiente a la solicitud o finalización de responsabilidades con el Ministerio de Ambiente y Desarrollo Sostenible.
TIPO	Cuenta de correo corporativo (completo)
UBICACIÓN	INFRAESTRUCTURA *Nube Microsoft*
PASO A PASO PARA GENERAR LA COPIA DE RESPALDO	Por medio de la herramienta de administración de Correo electrónico Micrososft 365, se realiza una copia completa de la información contenida en las cuentas corporativas pertenecientes al Ministerio de Ambiente y Desarrollo Sostenible, ya sea cuando se requiera una copia de este por medio de una solicitud, o cuando se finalicen responsabilidades del usuario con la entidad. Dicha información debe ser almacenada en el Servidor de Archivos (File Server) contenida en una carpeta con el nombre del usuario al cual pertenece la cuenta de correo. El archivo debe contener el nombre del usuario y la fecha de ejecución de la copia de seguridad, con el siguiente formato: “USUARIO 01-01-2023.PST”, donde USUARIO corresponde al nombre de la cuenta y 01-01-2023 corresponde a la fecha de ejecución del backup. PASO A PASO COPIA DE CORREO ELECTRÓNICO OUTLOOK 365 EN MICROSOFT **Opción 1 - Office365 Generado por usuario** • Abrir el programa de Outlook y hacer clic en "Archivo" en la parte superior izquierda de la ventana. • Seleccionar "Abrir y Exportar" en el menú desplegable. • Seleccionar "Importar/Exportar" en la lista de opciones. • En la ventana "Importar y Exportar", se selecciona "Exportar a un archivo". • Seleccionar "Archivo de datos de Outlook (.pst)" y hacer clic en "Siguiente". • Seleccionar la carpeta que se desea exportar. Si se requiere exportar toda la cuenta de correo electrónico, se selecciona "Correo". • Para exportar la carpeta completa y todas sus subcarpetas, la casilla "Incluir subcarpetas" deberá estar marcada. A continuación, hacer clic en "Siguiente". • Seleccionar la ubicación donde se va a guardar el archivo .pst. • Clic en "Finalizar" para comenzar el proceso de exportación. • Una vez que se completa el proceso de exportación se genera un archivo.pst, que contiene todos los correos electrónicos de la carpeta seleccionada. • Seleccionar el backup que se quiere restaurar uno por archivo .pst **Opción 2 – Backup generado por administrador de plataforma Office 365** • Una vez eliminada la cuenta de usuario, cualquier licencia de Exchange Online asociada a la cuenta estará disponible para asignarla a uno nuevo. Para que un buzón esté inactivo, debe tener una licencia correcta para que se pueda aplicar una suspensión al buzón antes de que se elimine.

- La configuración de retención debe configurarse para conservar el contenido o conservar y eliminar el contenido. Si la acción de retención está configurada para eliminar solo contenido, el buzón no estará inactivo cuando se elimine la cuenta de usuario.
- En la lista de buzones de usuario se deberá hacer clic en el buzón que desea colocar en Suspensión por juicio y a continuación, seleccionar en la página de propiedades de buzones características de buzón.
- Para la página retención por juicio se debe especificar la siguiente información:

    - Duración de retención por juicio (días): especificar cuánto tiempo se conservan los elementos de buzón, cuando el buzón se coloca en suspensión por juicio, la duración se calcula desde la fecha en que un elemento de buzón se recibe o se crea. Si deja este cuadro en blanco, los elementos se conservan indefinidamente o hasta que se elimine la retención.
    - Guardar en la página retención por juicio y, después, guardar en la página de propiedades del buzón.
    - Para comprobar que un buzón se ha colocado correctamente en retención por juicio, se deben realizar las siguientes verificaciones:
      En el EAC: Ir a Buzones de destinatarios.
      En la lista de buzones de usuario, hacer clic en el buzón para el que desea comprobar la configuración de suspensión por juicio.
      En la página de propiedades de buzones clic en Características de buzón.
      En Retención por juicio, comprobar que la retención está habilitada.
      Hacer clic en Ver detalles para comprobar cuándo se colocó el buzón en retención por juicio y quién lo hizo. También puede comprobar o cambiar los valores de las casillas opcionales Duración de retención por juicio (días), Nota y Dirección URL.

Opción 3 Generar Backup por búsqueda de contenido.

En el portal de cumplimiento Microsoft Purview, seleccionar Mostrar todo y, a continuación, se puede realizar una de las siguientes acciones:

- Seleccionar Búsqueda de contenido y, a continuación, seleccione una búsqueda.
- Digite el nombre de la búsqueda o referencia a la búsqueda a realizar.
- En Ubicaciones, seleccionar Ubicaciones específicas y, a continuación, seleccionar Modificar.
- Realice una de las siguientes acciones, en función de si está buscando en una carpeta de buzón o en una carpeta de sitio:
    - Buzones de Exchange
    - Sitios de SharePoint
    - carpetas públicas de Exchange
- En la columna Incluido, seleccionar/todo/ Elija usuarios, grupos o equipos
- Ingrese el nombre de buzón, grupo o equipo.
- Seleccione el nombre completo de la búsqueda.

- Al crear o editar una búsqueda de exhibición de documentos electrónicos, la opción para mostrar y usar el editor de KQL se encuentra en la página Condiciones del Asistente para búsquedas o colecciones.
- Después de realizar la configuración de la búsqueda, haga clic en Enviar y después en listo.
- El primer paso es preparar los resultados de búsqueda para la exportación. Al preparar los resultados, se cargan en una ubicación de Azure Storage proporcionada por Microsoft en la nube de Microsoft. El contenido de buzones y sitios se carga a una velocidad máxima de 2 GB por hora.
- En el menú Acciones de la parte inferior de la página desplegable, seleccionar Exportar resultados.
- Se muestra la página flotante Exportar resultados. Las opciones de exportación disponibles para exportar contenido dependen de si los resultados de la búsqueda se encuentran en buzones o sitios o en una combinación de ambos.
- En Opciones de salida, elija una de las siguientes opciones:
    - Todos los elementos, excepto los que tienen formato no reconocido, se cifran o no se indexan por otros motivos. Esta opción solo exporta elementos indizados.
    - Todos los elementos, incluidos los que tienen formato no reconocido, se cifran o no se indexan por otros motivos. Esta opción exporta elementos indexados y sin indexar.
    - Solo los elementos que tienen un formato no reconocido se cifran o no se indexan por otros motivos. Esta opción solo exporta elementos sin indexar.
- En Exportar contenido de Exchange se despliegan las siguientes opciones:
    - Un archivo PST para cada buzón: exporta un archivo PST para cada buzón de usuario que contiene resultados de búsqueda. Los resultados del buzón de archivo del usuario se incluyen en el mismo archivo PST. Esta opción reproduce la estructura de carpetas de buzón desde el buzón de origen.

    - Un archivo PST que contiene todos los mensajes: exporta un único archivo PST (denominado Exchange.pst) que contiene los resultados de la búsqueda de todos los buzones de origen incluidos en la búsqueda. Esta opción reproduce la estructura de carpetas de buzón para cada mensaje.
    - Un archivo PST que contiene todos los mensajes de una sola carpeta: exporta los resultados de la búsqueda a un único archivo PST donde todos los mensajes se encuentran en una única carpeta de nivel superior. Esta opción permite a los revisores revisar los elementos en orden cronológico (los elementos se ordenan por fecha de envío) sin tener que navegar por la estructura de carpetas del buzón original para cada elemento.
    - Mensajes individuales: exporta los resultados de búsqueda como mensajes de correo electrónico individuales, con el formato .msg. Si selecciona esta opción, los resultados de búsqueda de correo electrónico se exportan a una carpeta del sistema de archivos. La ruta de acceso de la carpeta para mensajes individuales es la misma que la que se usa si exportó los resultados a un archivo PST.

	▪ Otras configuraciones opcionales que se encuentran dispuestas en la plataforma son: o Excluir los mensajes duplicados desde la casilla Habilitar des duplicación para el contenido de Exchange. Seleccionando esta opción, solo se exportará una copia de un mensaje, incluso si se encuentran varias copias del mismo mensaje en los buzones que se buscaron. El informe de resultados de exportación (que es un archivo denominado Results.csv) contendrá una fila por cada copia de un mensaje duplicado para que pueda identificar los buzones (o carpetas públicas) que contienen una copia del mensaje duplicado. o Para exportar todas las versiones de documentos de SharePoint se puede activar la casilla Incluir versiones para archivos de SharePoint. o Seleccionar la carpeta Exportar archivos en una carpeta comprimida (comprimida). Incluye solo mensajes individuales y la casilla documentos de SharePoint para exportar resultados de búsqueda a carpetas comprimidas. • En cuanto a los resultados de búsqueda correspondiente a la búsqueda por contenido se relacionan entre otros los siguientes: ▪ En la página de control flotante en Clave de exportación, seleccione Copiar en el Portapapeles. ▪ Si se le pide que instale la herramienta de exportación de eDiscovery, se elige Instalar, este complemento es solo para Microsoft Edge. ▪ En la herramienta de exportación de eDiscovery, haga lo siguiente: o Elegir Examinar para especificar la ubicación donde desea descargar los archivos de resultados de búsqueda. o Descargar los resultados de la búsqueda en el equipo.
RESPONSABLE	Equipo de Infraestructura Minambiente (Nube)

DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE RESPALDO BASES DE DATOS	
ACTIVIDADES ESENCIALES	Realizar el proceso de backup de las bases de datos que se encuentran sobre la infraestructura *on premise* de la entidad para cada una de las aplicaciones teniendo en cuenta cada uno de los motores.
TIPO	Bases de datos
UBICACIÓN	Infraestructura *ON PREMISE*
PASO A PASO PARA GENERAR LA COPIA DE RESPALDO	• Realizar un dump de la base de datos. El dump de la base de datos debe depender del tipo de base de datos respectivo: ▪ Mysql: *mysqldump -u dbreader -h {$ip} -p {$nombreBd} > {$volumen respectivo/$nombrebd_fecha.sql}* ▪ Postgresql: *pg_dump -Fd {$nombreBd} -j 5 > {$volumnrespectivo/$nombrebd_fecha.sql}*

	▪ SqlServer script T-SQL: *BACKUP DATABASE [$nombreBD] TO DISK = N '{$volumen respectivo\$nombreBD_fecha.bak}'*; • Una vez se realiza la copia se debe comprimir en un formato tar.gz. La verificación se debe hacer de dos formas: ▪ Fecha de modificación o creación: Para verificar si el backup se realizó en la fecha estipulada, se debe ubicar en la carpeta *($nombre servidor*). Al abrir encontrará los archivos generados por la tarea programada en cada una de las unidades de almacenamiento externas, los cuales aparecen de la siguiente manera: *nombrebd_fecha-sql y nombreBD_fecha.bak* como se ve en el ejemplo anterior el backup crea un nombre con la fecha (DD,MM,AA). ▪ Tamaño de Archivo: La verificación por tamaño de archivo se hará por cada una de las carpetas, en las unidades de almacenamiento externo de la siguiente manera: • **Backups DB**: se abre la carpeta y se verifica el tamaño del archivo en la columna "tamaño" o "size" de la ventana. Ejm: **Back_DB "size" 826,102 KB** **Backup_Diferencial:** se abre la carpeta y se verifica el tamaño del archivo en la columna "tamaño" o "size" de la ventana. Ejm: **Back_Diferencial "size" 262,156,980 KB.** • Para hacer el esquema de revisión de restauración. Esta operación se debe realizar 1 vez al mes, y sobre cada una de la base de datos de forma tal que se garantice que el backup quedó de forma correcta. ▪ Seleccionar el backup que se quiere restaurar, uno por cada base de datos. ▪ Descomprimir el backup. ▪ Restaurar el backup dependiendo de la base de datos. ○ Para *mysql, mysql -u {$user}* ○ Para *postgresql, -i -h localhost -p {port} -d {basedaatos} -U {usuario} -v {archivo}* ○ Para Sql Server, *USE [master] RESTORE DATABASE [$nombreBD] FROM DISK = N '{$volumen respectivo\$nombreBD_fecha.bak} ' ;*
RESPONSABLE	Equipo de Infraestructura Minambiente (Infraestructura)

DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE RESPALDO BASES DE DATOS EN NUBE	
ACTIVIDADES ESENCIALES	Realizar copias de respaldo de las bases de datos que se encuentran en nube sobre la infraestructura de RDS y su paso al esquema de Glaciar luego de los 30 días para tener una retención mensual sobre el *snapshot* de la base de datos.
TIPO	Bases de datos en nube

UBICACIÓN	AMAZON WEB SERVICES (NUBE)
PASO A PASO PARA GENERAR LA COPIA DE RESPALDO	Amazon RDS crea y guarda copias de seguridad automáticas de su instancia de base de datos de forma segura en Amazon S3. Se tienen dos esquemas: un snapshot de la base de datos diario que se ejecutan a las 1:05:56 am UTC-5 (local) y un segundo con un paso a paso manual sobre la base de datos sobre una instancia de S3. • Para snapshot: ▪ Entre a la consola de Amazon https://console.aws.amazon.com/rds/. ▪ Vaya a la sección de RDS ▪ Seleccione el RDS ▪ Defina el backups y su respectiva periodicidad ▪ Ejecute el task ▪ Luego de los días de backups se debe descargar la copia y se debe subir al esquema de glacier • Para dump a través de cron: ▪ Se define en el contenedor de cron, un cron para extracción de la bd respectiva ▪ Se define la hora de ejecución del cron ▪ Se genera la base de datos en una carpeta local ▪ Se envía el tar.gz generado a la instancia S3 ▪ Se crear un usuario IAM en la instancia S3 para tener acceso a esta información en el bucket respectivo • Para realizar el proceso de restore a través de snapshot: ▪ Se debe realizar la creación de un RDS ▪ Se debe seleccionar el snapshot de la bd ▪ Se le da la opción de restore • Para realizar el proceso de restore a través de SQL: ▪ Se debe entrar a la instancia bastion ▪ Se debe instalar el cliente respectivo del tipo de base datos ▪ Se debe ejecutar el comando de restore **Consideraciones:** La copia de seguridad ocurre durante un período diario de 30 minutos configurable por el usuario conocido como la ventana de copia de seguridad. Las copias de seguridad automatizadas se guardan durante un número configurable de 30 días (denominado período de retención de la copia de seguridad). Su período de retención de respaldo automático se puede configurar hasta treinta y cinco días. Durante el periodo de backup se puede tener una latencia sobre la instancia RDS.
RESPONSABLE	Equipo de Infraestructura Minambiente (Nube)

DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE CODIGO FUENTE APLICACIONES EN NUBE	
ACTIVIDADES ESENCIALES	Realizar la copia de seguridad sobre el código de las aplicaciones que son desplegadas en la infraestructura de la nube. Es importante tener en cuenta que el código tiene un esquema redundante, por sí solo, es decir, una copia existe en el repositorio de la entidad, una segunda copia en el servidor

	donde se despliega y una tercera copia con el desarrollador. Sin embargo, el repositorio oficial de la entidad con el código fuente se encuentra sobre el repositorio de GIT en la nube.
TIPO	Código Fuentes de las aplicaciones
UBICACIÓN	GITLAB.COM
PASO A PASO PARA GENERAR LA COPIA DE RESPALDO	La entidad cuenta con un repositorio bajo GIT en la nube https://gitlab.com/ bajo la cuenta de serviciosweb@minambiente.gov.co. Todos los desarrollos Web debe estar en el repositorio de la entidad. **Consideraciones:** se debe contar con una cuenta en gitlab.com, la cual es una cuenta que es gratuita y permite compartir el código fuente con la cuenta privada del Ministerio de Ambiente.
RESPONSABLE	Equipo de Infraestructura Minambiente (Aplicaciones)

DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE ACTIVOS DE INFORMACIÓN	
ACTIVIDADES ESENCIALES	Realizar la copia de seguridad de cada una de las aplicaciones que tienen persistencia de activos de información (imágenes, pdf, shapes) que son cargadas por el usuario o generadas automáticamente por la herramienta específica.
TIPO	ACTIVOS DE INFORMACIÓN
UBICACIÓN	Volumen del servidor de aplicaciones sobre el cual existe persistencia de activos de información
PASO A PASO PARA GENERAR LA COPIA DE RESPALDO	Cada aplicación Web que haga manejo de activos de información, debe tener definido el (los) volúmenes donde se encuentra la información que se genera en la aplicación como resultado de una interacción con el usuario o por creación propia de la aplicación. **Esquema 1** • La oficina TIC definió, que el proceso de Backup se realice de forma automática con una periodicidad diaria. • Seleccionar los volúmenes sobre los cuales se va a realizar la copia de seguridad. • Realizar un tar.gz sobre el volumen respectivo t*ar -zcvf my-{$nombreApp){$fecha}.tar.gz /ruta/a/dir1/ /ruta/a/dir2/* • Para realizar la prueba que el archivo quedó creado correctamente *tar -tzf my_tar.tar.gz >/dev/null* • Una vez creado el archivo se puede definir la periodicidad de cargue del mismo a la nube **Esquema 2** La entidad puede hacer uso de la herramienta restic. Esta herramienta permite realizar un esquema de backups sobre activos de información con un esquema incremental, el

	cual emula un proceso como el esquema de versionamiento de los repositorios de información basados en GIT. Las ventajas de este esquema son varias. Sobre este esquema corresponde a un backup incremental que permite restaurar versiones específicas o incluso archivos particulares que pudieran verse comprometidos en caso de vulnerabilidades de seguridad. Se pueden hacer comparaciones entre diferentes momentos para ver inyección de archivos o simplemente para tener las diferencias de los documentos incluidos. ✓ *restic init --repo {$nombre_repositorio}* ✓ *restic -r {$directorio_del_repositorio} [--verbose] backup --tag <tag> {$archivo_o_directorio} [--exclude-file=excludes.txt]* ✓ Para validar la consistencia del repositorio restic -r *{$directorio_del_repositorio} check [--read-data]* ✓ En caso de querer restaurar el repositorio restic *-r {$directorio_del_repositorio} restore latest --target {$directorio_destino}* ✓ restic *-r {$directorio_del_repositorio} restore {$snapshot_id} --target {$directorio_destino}* ✓ *Imprimir el contenido de un directorio restic -r {$directorio_del_repositorio} dump {$directorio_en_restic} {$snapshot_id} > restore.tar*
RESPONSABLE	Equipo de Infraestructura Minambiente

DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DIRECTORIO ACTIVO	
ACTIVIDADES ESENCIALES	Generar una réplica de seguridad del directorio activo a través de la VPN con la nube de AWS
TIPO	DIRECTORIO ACTIVO (replica en nube)
UBICACIÓN	Directorio Activo de la entidad
PASO A PASO PARA GENERAR LA COPIA DE RESPALDO	Esquema que permite tener una copia de lectura en la nube del directorio activo como esquema de contingencia ante alguna eventualidad sobre la infraestructura tecnológica de la entidad. Precondición para su respectivo funcionamiento: • Definición de la VPN con el esquema en Nube • Esquema redundante de la VPN en caso de fallo • Aprovisionamiento de la instancia en nube correspondiente que permite una copia del directorio activo para el caso de Amazon Web Services (t2.medium) • Instalación del directorio activo • Monitoreo del esquema de funcionamiento Las acciones para tener una copia activa se describen a continuación: • Crear el Servicio RODC en el servidor de AWS

	• En el Servidor Local de Dominio Configurar el servicio de Lectura para RODC en Nube • Promover a DC el servidor en AWS • https://console.aws.amazon.com/ • Seleccionar el servidor del directorio activo • Definir un task para tener un snapshot del servidor de acuerdo a las definiciones del usuario de acuerdo a la temporalidad **Consideraciones:** se debe contar con una cuenta activa en la nube
RESPONSABLE	Equipo de Infraestructura Minambiente

DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS ARCHIVOS DE CONFIGURACIÓN DISPOSITIVOS DE RED	
ACTIVIDADES ESENCIALES	Generar copias de respaldo de los archivos de configuración de los dispositivos de red.
TIPO	ARCHIVOS DE CONFIGURACIÓN
UBICACIÓN	Datacenter Minambiente
PASO A PASO PARA GENERAR LA COPIA DE RESPALDO	Descripción de actividades: • Configurar el protocolo SNMPv2c o v3 en el equipo activo. • Configurar la dirección IP del equipo Colector de información asociado al protocolo SNMP establecido. • Habilitar credenciales de acceso mediante protocolo (SSH) en el equipo activo. • Configurar las plantillas SNMP y de autenticación en la aplicación IMC. • Efectuar el descubrimiento del equipo activo mediante la aplicación IMC empleando las plantillas del numeral anterior. • Vincular el equipo activo al plan automático de backups. **Consideraciones:** La copia de seguridad ocurre durante un período diario de 30 minutos configurable por el usuario conocido como la ventana de copia de seguridad. Las copias de seguridad automatizadas se guardan durante un número configurable de 30 días (denominado período de retención de la copia de seguridad). Su período de retención de respaldo automático se puede configurar hasta treinta y cinco días. • Efectuar la configuración en el orden indicado • Depurar la carpeta de backups según los lineamientos documentales del Ministerio de Ambiente y Desarrollo Sostenible. • De presentarse fallas de hardware y software en el servidor, los backups se podrán generar manualmente y almacenarse en el drive corporativo con los permisos respectivos. • Puertos lógicos de comunicación abiertos en forma bidireccional entre el servidor y la red de gestión de equipos activos.
RESPONSABLE	Equipo de Infraestructura Minambiente (Redes de datos)

7 BIBLIOGRAFIA

Backup System S.F. Backup Systems receives ISO 27001 Certification. Obtenido de: http://www.backup-systems.co.uk/blog/backup-systems-receives-iso-27001-certification

ICONTEC 2016. Controles de Seguridad y Privacidad de la Información. Obtenido de: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Mineducacion 2018. Política de Seguridad y Privacidad de la Información. Obtenido de: https://www.mineducacion.gov.co/1759/articles-349495_recurso_105.pdf

Mintic S.F. Respaldo y recuperación de los Servicios tecnológicos. Obtenido de: https://www.mintic.gov.co/arquitecturati/630/w3-article-8862.html