MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

Plan para la Generación de Copias de Respaldo (BACK-UP)

Proceso:
Gestión de Servicios de Información y Proyectos Tecnológicos
Versión 2
Vigencia: 20/10/2022

MADSIG
Sistema Integrado de Gestión

TABLA DE CONTENIDO

INTRODUCCIÓN 3

1 OBJETIVO 4

2 ALCANCE 4

3 ROLES Y RESPONSABILIDADES 5

4 DEFINICIONES 6

5 DESCRIPCIÓN DEL PLAN 7

6 PLAN DE GENERACIÓN DE COPIAS DE RESPALDO (INFRAESTRUCTURA) 8

7 BIBLIOGRAFIA 21

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 críticos 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 los lineamientos establecidos en la generación de las copias de respaldo de los activos críticos aquí descritos, se deben analizar detenidamente las políticas de operación que se encuentran definidas dentro del procedimiento copias de respaldo de la entidad, como premisa a la aplicación de las actividades relacionadas en este documento.

Su propósito principal es establecer e implementar estrategias que permitan generar, recuperar y mantener las copias exactas de la información crítica 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.
- Proporcionar un estándar para el etiquetado de los medios de copias de seguridad.
- Establecer un estándar para el almacenamiento y la recuperación de la información.

- Generar lineamientos para la generación de las copias de seguridad.

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, terminan con la verificación del Backup y posterior custodia de dichas copias de seguridad de acuerdo con los lineamientos establecidos por gestión documental.

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
Requerimiento Proveedor	R	R	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		C	R

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

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 las mismas 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 procedimientos de recuperación. Las acciones a contemplar aplican para Antes-Durante- Después con el fin de reducir las pérdidas de información generadas por eventos inesperados.

Plan de Contingencia: Procedimientos alternativos 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 restaura 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: volumen en donde se encuentran archivos que hacen parte integral de una aplicación (jpg, pdf, docx, pptx, xlsx)

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 documento de Plan de 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 Backup`s, mediante la ejecución de manera periódica de pruebas de restauración de algunas copias de backup para garantizar su correcto funcionamiento. En caso 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 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*
PROCEDIMIENTO	✓ Por medio de la herramienta generadora de copias de respaldo Veritas Net Backup y Veritas Backup Exec, se realiza la integración con la infraestructura Virtual correspondiente

a 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, entre otros que sean previamente solicitados.

- ✓ Mediante la herramienta generadora de copias de respaldo Veritas Net Backup y Veritas Backup Exec, 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: El tipo de operación de backup más básico y completo es el backup completo. Como su propio nombre indica, este tipo de respaldo, copia la totalidad de los datos en otro juego de soportes, que puede consistir en cintas o discos. 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 Backup debe ser ejecutado cada 15 días calendario, es decir, los primeros días de cada mes y a mediados del mismo. Este tipo de Backup solo guarda la diferencia de datos entre la copia full inicial y el servidor actualmente activo.

> *Backups incrementales: Una operación de respaldo incremental sólo copia los datos que han variado desde la última operación de backup de cualquier tipo. Se suele utilizar la hora y fecha de modificación estampada en 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 desde esas operaciones. Como un backup 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 un backup 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.*

	✓ Una vez realizada la tarea programada por el JOB, las copias de seguridad se encontrarán almacenadas 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 el backup quedó generado de forma correcta y su retención se hará de acuerdo a lo especificado por los lineamientos establecidos por gestión documental y las áreas involucradas. A continuación se describen las actividades que se deben realizar para la restauración de las copias de respaldo: ✓ 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 procedimiento del mismo, y probar nuevamente. En el caso del **SERVIDOR DE ARCHIVOS FILE SERVER** por medio de las herramientas de ejecución de Backups (herramienta generadora de copias de respaldo Veritas Net Backup y Veritas Backup Exec), es posible realizar una restauración Granular, es decir, es posible restaurar información parcial de los discos duros de almacenamiento, de la información contenida en estos. ***GRANULAR RESTORE (RESTAURACIÓN GRANULAR):*** *Una restauración de elementos individuales desde una copia de seguridad para la que se habilitó la opción de recuperación granular, a menudo se desea restaurar sólo una parte de los datos de una aplicación: un único mensaje de un buzón de correos o correo electrónico, una tabla de datos o registro en una base de datos o un archivo o carpeta de una imagen de máquina virtual. Cuando un sistema de copia de seguridad permite realizar estas pequeñas restauraciones, llamadas «restauración granular», los usuarios pueden conservar todos los datos de las aplicaciones más actualizadas hasta la fecha, en sustitución de pequeñas piezas de datos que hayan sido borrados o dañados accidentalmente.*
RESPONSABLE	Equipo de Infraestructura Minambiente
CONOCIMIENTOS	Aplicaciones y Bases de datos
RECURSOS ESENCIALES	Sistema de información, instructivos y equipos.

NORMATIVIDAD	NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. Ley 23 de 1982: Sobre Derechos de Autor Decretos y normatividad aplicable a la SNR

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 *ON PREMISE*
PROCEDIMIENTO	✓ Por medio de la herramienta de administración de Correo electrónico GSUIT, 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 01-01-2020.PST",** donde USUARIO corresponde al nombre de la cuenta y 01-01-2020 corresponde a la fecha de ejecución del backup. **PROCEDIMIENTO DE COPIA DE CORREO ELECTRÓNICO GMAIL EN GSUIT** **Paso 1 - Gmail extracción de datos** Antes de iniciar el proceso real de conversión de correo electrónico, es necesario extraer y descargar los datos de Gmail cuenta al ordenador. Para facilitar las cosas, Google ha desarrollado una herramienta especial llamada Google Takeout, que permite a los usuarios descargar sus datos de una serie de servicios de Google en la forma de un comprimido ZIP expediente. De acuerdo con lo anterior, a continuación se relacionan las actividades que se deben realizar para la generación de las copias del correo electrónico: ✓ Acceder a través del enlace: https://takeout.google.com/settings/takeout. En este se muestra una larga lista de servicios que se pueden exportar, sin embargo si solo se requiere el correo, se hace clic en el "*Select none*" botón superior de la lista para deseleccionar todos los servicios y luego se desplaza hacia abajo hasta encontrar y

	activar la opción *Mail import option*. Es importante tener en cuenta que debe estar conectado necesariamente a las cuentas de Google para utilizarTakeout. ✓ Google Takeout: Haga clic en "Next" para proceder al siguiente paso. Aquí puede seleccionar un formato de archivo de salida alternativo (ZIP se utiliza de forma predeterminada) y el método de entrega preferida (link de descarga enviada al correo electrónico o el archivo resultante se guarda en Google Drive). ✓ Haga clic en "*Create archive*"para iniciar la extracción de datos. Se debe tener en cuenta dependiendo del número de mensajes de correo electrónico el tamaño correspondiente, entre otros factores. Este proceso puede tardar hasta varias horas. Una vez hecho esto, para llevar el servicio se deberá guardar el contenido de los buzones de correo a un MBOX para su posterior procesamiento y se comprime en un archivo ZIP para facilitar la descarga. ✓ Para archivar los datos en Gmail, seleccione la opción de enlace de descarga. A continuación recibirá un correo electrónico con un enlace que genera un archivo ZIP. En caso de optar por subir el archivo a Google Drive, se encontrará allí una vez finalizada el servicio de extracción de datos. ✓ Descargar emails de Gmail: Una vez se tiene el archivo de correo electrónico, se procede con la descarga y descompresión en una carpeta del disco duro. Se cuenta con un esquema para realizar la revisión de restauración. Esta operación se debe realizar 1 vez al mes, y sobre algunas cuentas de correo PST de forma tal que se garantice que el backup quedó de forma correcta, y su retención se hará de acuerdo a lo especificado en los lineamientos de gestión documental y las áreas correspondientes. ✓ Seleccionar el backup que se quiere restaurar, uno por archivo PST ✓ Montar el archivo en un programa compatible para su lectura. ✓ Realizar la lectura correspondiente.
RESPONSABLE	Equipo de Infraestructura Min ambiente
CONOCIMIENTOS	Aplicaciones y Bases de datos
RECURSOS ESENCIALES	Sistema de información, instructivos y equipos.
NORMATIVIDAD	NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. Ley 23 de 1982: Sobre Derechos de Autor Decretos y normatividad aplicable a la SNR

DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE RESPALDO BASES DE DATOS

ACTIVIDADES ESENCIALES	Realizar el proceso de backup de las base 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 de base de datos.
TIPO	Bases de datos
UBICACIÓN	Infraestructura *ON PREMISE*
PROCEDIMIENTO	✓ Realizar un dump de la base de datos. El dump de la base de datos debe depender del tipo de base de datos respectivo a. Mysql: *mysqldump -u dbreader -h {$ip} -p {$nombreBd} > {$volumen respectivo/$nombrebd_fecha.sql}* b. Postgresql: *pg_dump -Fd {$nombreBd} -j 5 > {$volumnrespectivo/$nombrebd_fecha.sql}* c. SqlServer script T-SQL: *BACKUP DATABASE [$nombreBD] TO DISK = N '{$volumen respectivo\$nombreBD_fecha.bak}'*; ✓ Una vez se realiza la copia se debe comprimir en un formato tar.gz. La verificación se debe hacer de dos formas: a. Fecha de modificación o creación: Para verificar si el backup se realizó en la fecha estipulada, se debe ubicar en la carpeta *($nombre_servidor)*. Al abrirla 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) b. 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.** ✓ La verificación del backup en las cintas LTO Ultrium se hará de la siguiente forma:

	a. Doble clic en el icono que se encuentra en el escritorio de "backup". b. En la ventana que aparece seleccionamos "*always start in wizard mode*" y clic en el botón "*next*". c. Periodicidad: Definida de acuerdo con el área respectiva y de acuerdo a la definición del riesgo en caso de pérdida de información. d. Diligenciar en los formatos de control las copias realizadas con sus respectivas bases de datos, fecha de creación y tamaño utilizar el formato oficial "*Bitácora Backup Diario*" en formato Excel. 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 a. Seleccionar el backup que se quiere restaurar, uno por cada base de datos b. Descomprimir el backup c. 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
CONOCIMIENTOS	Aplicaciones y Bases de datos
RECURSOS ESENCIALES	Sistema de información, instructivos y equipos.
NORMATIVIDAD	NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. Ley 23 de 1982: Sobre Derechos de Autor Decretos y normatividad aplicable a la SNR

DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE RESPALDO BASES DE DATOS EN NUBE	
ACTIVIDADES ESENCIALES	Realizar copias de respaldo de las base 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)
PROCEDIMIENTO	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 procedimiento 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. El costo de Glacier a Abril 2020 estaba en 0.004 GB (https://aws.amazon.com/s3/pricing/) esquema sobre el cual se guardaría la información luego de los 30 días con el último shapshot de la base de datos
RESPONSABLE	Equipo de Infraestructura Minambiente
CONOCIMIENTOS	Aplicaciones y Bases de datos
RECURSOS ESENCIALES	Sistema de información, instructivos y equipos.
NORMATIVIDAD	NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. Ley 23 de 1982: Sobre Derechos de Autor Decretos y normatividad aplicable a la SNR

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. El 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
PROCEDIMIENTO	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, de acuerdo al documento de "*Guía para el manejo del 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
CONOCIMIENTOS	Aplicaciones y Bases de datos
RECURSOS ESENCIALES	Sistema de información, instructivos y equipos.
NORMATIVIDAD	NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. Ley 23 de 1982: Sobre Derechos de Autor Decretos y normatividad aplicable a la SNR

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
PROCEDIMIENTO	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 (*Ver cargue Glacier Amazon Web Services*) **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
CONOCIMIENTOS	Aplicaciones y Bases de datos
RECURSOS ESENCIALES	Sistema de información, instructivos y equipos.
NORMATIVIDAD	NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. Ley 23 de 1982: Sobre Derechos de Autor Decretos y normatividad aplicable a la SNR

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
PROCEDIMIENTO	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 *(Ver Guía para el manejo de la infraestructura de la entidad bajo Amazon Web Services)* 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 definición del usuario de acuerdo a la temporalidad **Consideraciones:** se debe contar con una cuenta activa en la nube
RESPONSABLE	Equipo de Infraestructura Minambiente
CONOCIMIENTOS	Aplicaciones y Bases de datos
RECURSOS ESENCIALES	Sistema de información, instructivos y equipos.
NORMATIVIDAD	NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. Ley 23 de 1982: Sobre Derechos de Autor Decretos y normatividad aplicable a la SNR

DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DEL ESQUEMA DE INFRAESTRUCTURA EN NUBE	
ACTIVIDADES ESENCIALES	Realizar una copia de seguridad sobre el esquema de infraestructura que se encuentra desplegado en la nube
TIPO	INFRAESTRUCTURA SOBRE AWS
UBICACIÓN	Nube
PROCEDIMIENTO	Construcción de un script que aprovisione toda la infraestructura de la nube basada en la generación de los scripts que permiten su construcción a través del uso de la versión 0.11 de Terraform (https://www.terraform.io/) El esquema de infraestructura de la entidad, de acuerdo al documento de "*Guía para el manejo de la infraestructura de la entidad bajo Amazon Web Services*" **Consideraciones:** se debe contar con una cuenta activa en la nube de Amazon
RESPONSABLE	Equipo de Infraestructura Minambiente
CONOCIMIENTOS	Aplicaciones y Bases de datos
RECURSOS ESENCIALES	Sistema de información, instructivos y equipos.
NORMATIVIDAD	NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. Ley 23 de 1982: Sobre Derechos de Autor Decretos y normatividad aplicable a la SNR

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
PROCEDIMIENTO	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
CONOCIMIENTOS	Redes de Datos
RECURSOS ESENCIALES	Conectividad IP, TFTP, HTTP al servidor, Credenciales de acceso, Permisos de escritura.
NORMATIVIDAD	NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. Ley 23 de 1982: Sobre Derechos de Autor Decretos y normatividad aplicable a la SNR

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