Ambiente

Instructivo para la Generación de Copias de Respaldo (Back-Up)

Proceso

Gestión de Servicios de Información y Proyectos Tecnológicos

Versión 3

6/3/2025

TABLA DE CONTENIDO

1. 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.

2. 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.

3. 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 TI:

RECUPERACIÓN	A DEMANDA
• Bases de datos en producción (programado) • Código fuente a través de GitLab • Configuración de infraestructura (archivos de configuración de host y almacenamiento, dispositivos networking y equipos de seguridad perimetral) • Servidores en Producción (on premise) - toda la máquina • File Server de sistemas de información • File Server de otros documentos (únicamente versiones finales de documentos) • Directorio activo - toda la máquina	• Bases de datos en producción (programado) • Código fuente a través de GitLab • Configuración de infraestructura (archivos de configuración de host y almacenamiento, dispositivos networking y equipos de seguridad perimetral) • Servidores en Producción (on premise) - toda la máquina • File Server de sistemas de información • File Server de otros documentos (únicamente versiones finales de documentos) • Directorio activo - toda la máquina

RETENCIÓN	NO SE LE HACE BACKUP
• Onedrive (retención por 93 días) • Correo Electrónico (retención por 10 años)	• Información alojada en los equipos de cómputo de los usuarios

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.

4. 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 Con 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.

5. CICLO PARA REALIZACIÓN DE COPIAS DE COPIAS DE RESPALDO

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.

Ciclo (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. ACTIVIDADES PARA LA GENERACIÓN DE COPIAS DE RESPALDO (INFRAESTRUCUTURA)

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.

6.1 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 (Servidores de Servicio, File Server, Base de Datos, Aplicaciones, etc.), de una manera óptima y práctica, para su posterior almacenamiento según la retención programada y disposición para restauraciones de emergencia según requerimiento. ▪ Es necesario realizar una copia de seguridad de las máquinas virtuales en producción y algunas de desarrollo (Según requerimiento), que contenga la configuración de Software en sistema operativo, servicios y aplicaciones configuradas además de estructura en hardware virtual, tales como Memoria, Procesamiento, Dispositivos de red, Discos duros virtuales, entre otros, compatible con la estructura de virtualización VMware ESXi, 7.0.3, 22348816 y vSphere Client versión 7.0.3.01700 actualmente en producción en el Ministerio. ▪ Realizar copias de respaldo de la información almacenada en los SERVIDORES DE ARCHIVOS FILE SERVER, enfocada a la Data contenida en los servidores de aplicación y en los recursos compartidos asignados a las áreas de trabajo en el Ministerio de Ambiente y Desarrollo Sostenible.

POLÍTICAS	▪ En el momento de la solicitud de creación toda máquina o servidor virtual de producción debe estar incorporado en una de las políticas de los grupos de copia de respaldo para garantizar el DRP plan de recuperación de desastres. ▪ Actualmente se aplican tres tipos de retenciones a los Backups Full de las máquinas virtuales ▪ Diario con retenciones de dos semanas ▪ Semanal con retención de dos meses ▪ Bajo demanda, con retención según requerimiento del solicitante. **Nota:** En los servidores de producción de la entidad deben reposar únicamente versiones definitivas o finales de los documentos emitidos por las diferentes áreas. Las restauraciones se realizan bajo demanda y por solicitud y/o autorización de los lideres de área según el caso.
EXCEPCIONES	▪ En los servidores de desarrollo y pruebas según por solicitud y teniendo en cuenta las capacidades es posible agregar esta máquina o servidor virtual en una de las políticas de los grupos de copia de respaldo.
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 plataforma VMware teniendo acceso a la infraestructura de los servidores virtuales, se seleccionan las máquinas virtuales requeridas, entre ellos: MV de Aplicaciones, MV de Base de Datos, SERVIDOR DE ARCHIVOS FILE SERVER y MV de servicio, entre otras, que correspondan al funcionamiento de la infraestructura tecnológica, además de los otros que sean previamente solicitados. Mediante la herramienta generadora de copias de seguridad se agregan las máquinas virtuales a una política de respaldo según la criticidad de esta (esta varía según su retención y número de copias incrementales) se denomina JOBs, y a su vez se ejecutarán periódicamente en dos tipos de Backups: • <u>Backup Tipo Full:</u> Realizado al inicio de la ejecución del JOBs. Este tipo de Backup contendrá una copia íntegra 100% de la Máquina virtual previamente seleccionada. • <u>Backups completos Tipo FULL:</u> 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. 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, hardware especializado para este trabajo) referenciados por tipo de Backup y fecha de creación, dispuestos por la herramienta de generación de Backup. Este hardware especializado se encarga de garantizar la integridad y calidad efectiva de las copias de respaldo realizadas por el mismo, lo cual se evidencia en los logs generados por el software de gestión de dicho hardware. 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. • Restaurar el Backup en un ambiente con los recursos necesarios. • 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. • Por medio de la herramienta de copias de respaldo HPE StoreOnce/Simplivity se generan automáticamente Logs de auditoria referente a los Backups realizados garantizando así su integridad, fiabilidad y congruencia al momento de crearse y restaurarse.
RESPONSABLE	Equipo de Infraestructura MinAmbiente (Infraestructura).

6.2 DESCRIPCIÓN TÉCNICA PROCESO DE RETENCIÓN DE CUENTAS DE 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.
POLÍTICAS	Todos los datos de uso diario se retendrán durante 10 años desde su creación o modificación, después de lo cual se eliminarán de forma segura. Se debe tener en cuenta que esta política de retención de datos se aplica únicamente a las cuentas de Microsoft 365.
EXCEPCIONES	Las siguientes excepciones se aplicarán en casos específicos: • Requisitos Legales o Regulatorios: Si existen leyes o regulaciones que requieran una retención de datos más larga que los días establecidos en esta política, se cumplirá con dichos requisitos legales o regulatorios. • Litigios Pendientes: Si la entidad se encuentra involucrada en un litigio o una investigación legal, se suspenderá la eliminación de datos relevantes hasta que se resuelva el caso y se cumplan todos los requisitos legales relacionados con la retención de datos en el contexto del litigio. • Auditorías Internas o Externas: Los datos necesarios para auditorías internas o externas se retendrán según las necesidades de estas, respetando los plazos establecidos por las regulaciones aplicables. • Políticas de Retención Específicas: Si se ha establecido una política de retención de datos específica para ciertos tipos de información o departamentos dentro de la entidad, se seguirán los plazos y las excepciones definidos en esa política específica. Estas políticas y excepciones se implementan para garantizar una gestión adecuada de los datos, cumplir con las regulaciones y adaptarse a las circunstancias cambiantes de la entidad en relación con la retención de datos, siempre con un enfoque en la seguridad y el cumplimiento.
TIPO	Cuenta de correo corporativo (completo).
UBICACIÓN	INFRAESTRUCTURA Nube Microsoft
PASO A PASO PARA GENERAR LA	Por medio de la herramienta de administración de Correo electrónico Microsoft 365, se realiza una copia completa de la información contenida en las cuentas corporativas

COPIA DE RESPALDO	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. Estas copias solo se generan bajo demanda. Dicha información debe ser almacenada en los recursos tecnológicos dispuestos por la oficina, 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. o "Los respaldos de correo electrónico se realizan únicamente bajo demanda y no como copias de seguridad, ya que solo se retiene el contenido de los buzones. Estos respaldos se llevan a cabo a petición del usuario o del coordinador de área a través de casos en GEMA, solicitando la retención de correos electrónicos." o El archivo del Backup se entregará en la ubicación que el usuario indique.
RESPONSABLE	Equipo de Infraestructura MinAmbiente (Nube)

Nota

En el **M-A-GTI-5** se especifica detalladamente los segmentos de información que componen los servicios de Microsoft 365 (Correo y One Drive) y los diferentes niveles de responsabilidad.

6.3 DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE RESPALDO BASES DE DATOS ON PREMISE	
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.
POLÍTICAS	Todas las copias de seguridad de las bases de datos se mantendrán hasta máximo dos (2) días anteriores, así mismo, se realizarán Backups full para los motores actualmente implementados en el Ministerio SQL Server, Postgres y MySQL. Los Backups se realizarán a las bases de datos producción (prod). Los backups del primer día de cada mes se debe subir a un almacenamiento frio como AWS S3 glacier.
EXCEPCIONES	Se realizarán Backups a solicitud de las áreas funcionales siempre y cuando estás se soliciten a través de un caso en el Sistema de Información GEMA.
TIPO	Bases de datos on premise
UBICACIÓN	Infraestructura ON PREMISE
	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 nombre BD_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.

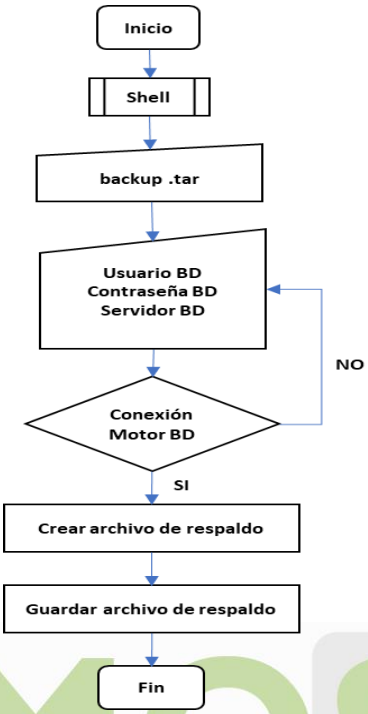
    Ejm: Back_DB “size” 826,102 KB.

  - 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.

La copia de seguridad de las bases de datos puede realizarse tanto de manera manual como semiautomatizada de acuerdo con el siguiente esquema básico:

semiautomatizado



Backups bases de datos SQL Server.

Para la realización de Backups en SQLServer se implementa un disco en el cual se generan tareas programadas a continuación se describe el proceso: A través del SQL Server Agent, en Jobs, se genera la siguiente acción con el fin de que se generen copias de todas las bases de datos a excepción de las bases de datos: master, model, msdb, tempdb.

```
--1. Se declaran las variables
DECLARE @path VARCHAR(500)
DECLARE @name VARCHAR(500)
DECLARE @filename VARCHAR(256)
DECLARE @time DATETIME
DECLARE @year VARCHAR(4)
DECLARE @month VARCHAR(2)
DECLARE @day VARCHAR(2)
DECLARE @hour VARCHAR(2)
DECLARE @minute VARCHAR(2)
DECLARE @second VARCHAR(2)
-- 2. Path donde estarán los backups
SET @path = 'B:\98\'
-- 3. Propiedades de tiempo para los backups
SELECT @time = GETDATE()
SELECT @year  = (SELECT CONVERT(VARCHAR(4), DATEPART(yy, @time)))
SELECT @month  = (SELECT CONVERT(VARCHAR(2), FORMAT(DATEPART(mm,@time),'00')))
SELECT @day   = (SELECT CONVERT(VARCHAR(2), FORMAT(DATEPART(dd,@time),'00')))
SELECT @hour  = (SELECT CONVERT(VARCHAR(2), FORMAT(DATEPART(hh,@time),'00')))
SELECT @minute = (SELECT CONVERT(VARCHAR(2), FORMAT(DATEPART(mi,@time),'00')))
SELECT @second = (SELECT CONVERT(VARCHAR(2), FORMAT(DATEPART(ss,@time),'00')))
WHERE name NOT IN ('master','model','msdb','tempdb') -- system databases are excluded
```

```
-- 4. Se definen las operaciones
DECLARE db_cursor CURSOR FOR
SELECT name
FROM master.dbo.sysdatabases
WHERE name NOT IN ('master','model','msdb','tempdb') -- system databases are excluded
--5. Se inicializan las operaciones
OPEN db_cursor
FETCH NEXT FROM db_cursor INTO @name
WHILE @@FETCH_STATUS = 0
BEGIN
-- 6. Se define el formato de los archivos
    SET @fileName = @path + @name + '_' + @year + @month + @day + @hour + @minute + @second +
'.BAK'
    BACKUP DATABASE @name TO DISK = @fileName
    FETCH NEXT FROM db_cursor INTO @name
END
CLOSE db_cursor
DEALLOCATE db_cursor
```

Después de definir este trabajo se procede a realizar el cronograma de la hora que se planea realizar cada respaldo tal como se muestra en la siguiente imagen, donde se correrá el JOB a la 1 am.

Backups bases de datos postgres

Para la realización de Backups en Postgrest se implementa con un procedimiento de Backups que esta implementado como crontab se envía como ejemplo el proceso que se tiene con SIFAME.

```
DIRBACKUPS=/backup/
FECHA=`date +%d%m%y`
DIR=${DIRBACKUPS}
export DIR


## Para cada base (en el caso de la PGN, cada base esta en una
## instancia particular), lo siguiente:
## SIFAME

PGPORT=6451
export PGPORT

BASE=bdsisfin5
export BASE

COPBASE=${BASE}_${FECHA}
export COPBASE

LOGFILE=logfile6451
export LOGFILE

DIRLOGFILE=/BASES/bases4/
export DIRLOGFILE

cd ${DIR}
##cp ${BASE}.gz ${BASE}.ant.gz
##cp ${LOGFILE}.gz ${LOGFILE}.ant.gz
##rm ${BASE}.gz
##rm ${LOGFILE}.gz
pg_dump ${BASE} | gzip > ${COPBASE}.gz
##cat ${DIRLOGFILE}/${LOGFILE} | gzip > ${LOGFILE}.gz
```

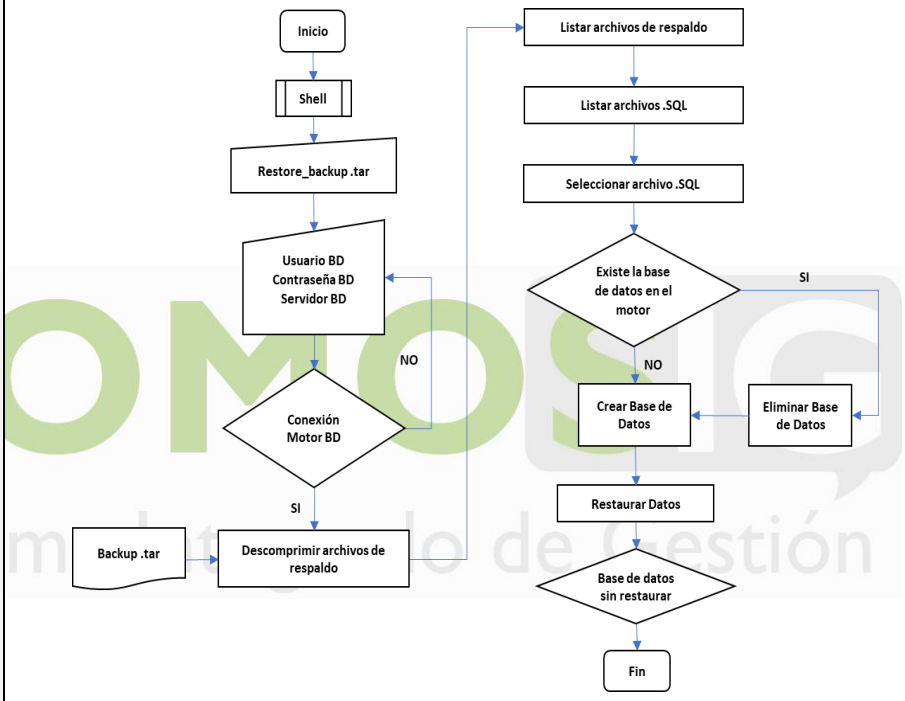
Restauración de bases de datos.

- 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}';

La restauración de las bases de datos puede realizarse tanto de manera manual como semiautomatizada de acuerdo con el siguiente esquema básico:

Restauración semiautomatizada



RESPONSABLE	Equipo de Infraestructura MinAmbiente (Infraestructura)

6.4 DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE RESPALDO BASES DE DATOS CLOUD	
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.
POLÍTICAS	Todas las copias de seguridad de las bases de datos se mantendrán hasta máximo dos (8) días anteriores, así mismo, se realizarán Backups full para los motores actualmente implementados en el Ministerio SQL Server, Postgres y MySQL. Los Backups se realizarán a las bases de datos producción (prod). Los Backups del primer día de cada mes deben descargar a un servidor on premise y se almacenara solo las 2 ultimas copias (2 meses).
EXCEPCIONES	Se realizarán Backups a solicitud de las áreas funcionales siempre y cuando estás se soliciten a través de un caso en el Sistema de Información GEMA.
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)

6.5 DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE RUTAS O DIRECTORIOS DE SERVIDORES, 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

6.6 DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS ARCHIVOS DE CONFIGURACIÓN DISPOSITIVOS DE RED	
ACTIVIDADES ESENCIALES	Generar copias de respaldo de los archivos de configuración a los dispositivos de red.
POLÍTICAS	Los switch y equipos de seguridad perimetrales serán sujeto de Backup de configuración, los cuales serán generados de forma periódica cada segundo (2) día de cada mes. Los Backups de configuración que no se puedan generar de forma automática por la herramienta de administración y monitoreo IMC, deberán ser obtenidos de forma manual y alojados en el repositorio del file server de redes y seguridad. Frente a actividades de mantenimiento sobre estos equipos, se hace necesario hacer una copia de respaldo o Backup por parte del proveedor como buena práctica previo a la rutina de mantenimiento. Los archivos de configuración se mantendrán exclusivamente en el repositorio del file server evitando duplicar información en otras unidades de almacenamiento. Se recomienda evitar configuraciones con protocolo SNMPv2 dado que este tiene características de poco seguro. Para evitar esto, debe implementarse protocolo SNMPv3 para los equipos que se encuentran en la herramienta de administración y monitoreo IMC. Dado que algunos equipos no dependen del protocolo SNMP para efectuar procesos de Backup, se relacionan el procedimiento en este documento para asegurar la obtención del archivo de configuración deseado. La retención de esta documentación se efectuará por dos años considerando que estos archivos son renovados constantemente 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.
EXCEPCIONES	Los demás componentes de red tales como access points, sistemas de videoconferencia, teléfonos IP, etc. No serán objeto de obtención de este proceso.
TIPO	ARCHIVOS DE CONFIGURACIÓN
UBICACIÓN	Datacenter MinAmbiente y cuartos de cableado

PASO A PASO PARA GENERAR LA COPIA DE RESPALDO	<u>Switch o Conmutador de Red</u> 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 para tener en cuenta • 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 file server con los permisos respectivos. • Puertos lógicos de comunicación deberán estar abiertos en forma bidireccional entre el servidor y la red de gestión de equipos activos. <u>Firewall FortiGate</u> • Ingresar al equipo Firewall Fortigate con privilegios de administrador • Ubicarse en el menú de la parte superior derecha donde se indica el usuario. • Se desplegará un menú, en el cual se deberá seleccionar la opción **Configuration** al hacer clic en esta opción de desplegar un nuevo menú para el que se elegirá la opción **Backup.** • Seguidamente, deberá elegir el medio en el cual se alojará el archivo deseado (local PC/USB Disk) • De forma opcional podrá elegir si se desea el Backup de forma encriptada. • Hacer clic en **OK** y el sistema generará el archivo de configuración. • Finalmente, mover el archivo obtenido con la extensión .conf al repositorio de file server Redes y Seguridad. <u>FortiAnalyzer</u> • Ingresar al equipo Firewall Fortigate con privilegios de administrador • Acceder al **ADOM** de **root** • Ingresar al ícono de **Ajustes del Sistema** • Una vez ubicado en el tablero diríjase a **Información del Sistema** y seleccionar la opción **Respaldo**

	• Allí se desplegará un recuadro que permitirá opcionalmente elegir cifrado y generación de credenciales para el archivo de configuración. • Si no se desea activar las opciones anteriores, desactivar la habilitación de cifrado y dar **OK**. • El sistema generará el archivo de respaldo requerido y lo alojará en la carpeta por default para descargas. • Finalmente, mover el archivo obtenido con la extensión .dat al repositorio de file server Redes y Seguridad. <u>FortiWeb</u> • Ingresar al equipo **FortiWeb** con privilegios de administrador • Acceder al menú **System** en la opción **Maintenance** y seleccionar **Backup & Restore**. • En esta pestaña asegurarse de elegir la opción **Backup** y **Backup entire configuration** • Allí se permitirá opcionalmente elegir **encriptación** e **inclusión de datos de Machine Learning** • Seleccionar la opción **Backup** de color verde. • El sistema generará el archivo de respaldo requerido y lo alojará en la carpeta por default para descargas. • Finalmente, mover el archivo obtenido con la extensión .zip al repositorio de file server Redes y Seguridad. <u>FortiDDoS</u> • Ingresar al equipo **FortiDDoS** con privilegios de administrador • Acceder al menú **System** en la opción **Maintenance** • En esta pestaña Backup & Restore elegir la opción **Backup** • Allí se permitirá opcionalmente activar la opción SPP, elegir la opción **Backup.** • El sistema generará el archivo de respaldo requerido y lo alojará en la carpeta por default para descargas. • Finalmente, mover el archivo obtenido con la extensión .zip al repositorio de file server Redes y Seguridad.
RESPONSABLE	Equipo de Infraestructura MinAmbiente (Redes y Seguridad Perimetral)

7. DEFINICIONES

Backup: 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.

8. 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

Ministerio de Educación 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.