| INSTRUCTIVO: Gestión de Copias de Seguridad | | | |
|---|---|---|---|
| **FECHA DE APLICACIÓN:**<br>2023-10-20 | **CÓDIGO:**<br>IN.0720.04 | **VERSIÓN:**<br>001 | |
| **ELABORADO POR:**<br>FABIAN EDUARDO ROJAS GALLEGO<br>PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION<br>CAROLA DUQUE JIMENEZ<br>TECNICO ADMINISTRATIVO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION<br>JUAN CARLOS CAMACHO CASTILLO<br>PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION | **REVISADO POR:**<br>PAMELA KATHERINE ENRIQUEZ PAZ<br>PROFESIONAL DE APOYO GRUPO GESTIÓN AMBIENTAL Y DE CALIDAD<br>EDWIN RUANO GAMBOA<br>PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION | **APROBADO POR:**<br>DIEGO ALEXANDER MILLAN LONDOÑO<br>JEFE DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION | |

## 1. OBJETIVO

Describir en detalle las actividades que se deben realizar en el procedimiento de Gestión de Copias de Seguridad - Backups Gestión de Copias de Seguridad PT.0720.27.

## 2. DEFINICIONES

Las definiciones que aplican a este procedimiento pueden ser consultadas en el siguiente enlace **GLOSARIO DE TÉRMINOS Y DEFINICIONES OTI**.

## 3. DESARROLLO

### 3.1. POLÍTICAS OPERACIONALES Y CONDICIONES GENERALES

a. La OTI, debe realizar el respaldo de los activos de información clasificados en el Inventario de Activos de Información con nivel de **criticidad alta** y **media**, que a su vez se consideren sujetos a copia de seguridad como son las bases de datos de los aplicativos institucionales, servidores virtuales, archivos específicos en repositorios de información que se consideren críticos o de otros servicios que se encuentren virtualizados, mediante la utilización de herramientas tecnológicas y procedimientos estandarizados.
b. La información respaldada por la OTI de los activos de información clasificados con nivel de **criticidad alta** y **media,** debe almacenarse comprimida y cifrada.
c. La OTI debe contar con los recursos tecnológicos especializados para la gestión de copias de seguridad.
d. La OTI debe implementar estrategias de respaldo alterno para las copias de seguridad realizadas.
e. Se podrá realizar la contratación de una empresa especializada en la custodia de copias de seguridad, que brinde la confianza necesaria en el almacenamiento de las copias de seguridad alternas.
f. Toda copia configurada en la herramienta de copias de seguridad debe tener:
    - Origen de datos (Servidor virtual o archivo)
    - Periodicidad de la copia de seguridad
    - Periodo de retención de la copia de seguridad
g. La herramienta de copias de seguridad debe conservar el histórico de las copias generadas y conservarlo de acuerdo a la retención configurada.
h. Se debe tener una evidencia de la revisión de la ejecución de las copias y las réplicas configuradas en la herramienta de copias de seguridad. Ese registro debe contener como mínimo:
    - Medio en el que se realiza
    - Si se realizó automática o manualmente
    - Fecha de la copia o réplica
    - Si se finalizó con éxito o con errores
    - Observaciones, si se realizó alguna acción
    - Quien revisó
i. La información de los archivos contenidos en las copias de seguridad debe ser exclusivamente de uso de la CVC y no de uso personal.
j. Se debe realizar una prueba de restauración de copias de seguridad y su correcto funcionamiento como mínimo dos (2) veces al año, o el tiempo que el personal de la OTI considere prudente, de acuerdo a la criticidad de la información.
k. Las actividades que se llevan a cabo para la gestión de copias de seguridad y su resultado, deben ser validadas mínimo una (1) vez al año. En esta evaluación se deberá verificar que se esté haciendo la copia de los activos de

información sujetos a copia de seguridad, además de la valoración de los riesgos o nuevos riesgos en caso de falla de los sistemas.

l. Todos los funcionarios de la CVC que tienen a cargo equipos de cómputo y que manejen información sensible y crítica, deben realizar copia de la información periódicamente como mínimo cada tres (3) meses, para ello la OTI dispondrá de herramientas que puede usarse para tal fin.
m. Todos los funcionarios que tengan información que sea actualizada en recursos compartidos como unidades de red, OneDrive y SharedPoint debe ser respaldada como mínimo cada tres (3) meses.
n. Se debe realizar una copia de seguridad de la información almacenada en los equipos de cómputo, cuando se requiera formatear y reinstalar el sistema operativo.
o. Cuando se presenten fallas en los discos duros, se deberán realizar procesos de restauración y recuperación de la información contenida en los mismos, utilizando herramientas y mecanismos técnicos y tecnológicos para buscar salvar la información almacenada en el dispositivo averiado. Los responsables de la información validarán la integridad de la misma.
p. Se debe realizar copia de seguridad de la información contenida en las estaciones de trabajo cuando hay retiro de un funcionario de la CVC, previa autorización del jefe inmediato.
q. Realizar copias de seguridad periódicas de los activos de información que almacenen cuentas de usuario de los recursos o servicios tecnológicos como directorio activo y bases de datos de aplicativos institucionales.

### 3.2. GESTIÓN DE COPIAS DE SEGURIDAD

#### 3.2.1. IDENTIFICAR LOS ACTIVOS DE INFORMACIÓN QUE SON SUJETOS A COPIA DE SEGURIDAD.

La identificación de los activos de información sujetos a copia de seguridad en la Corporación, se lleva a cabo de acuerdo a la criticidad definida en el Inventario de Activos de Información o por un requerimiento específico.

Teniendo en cuenta el Inventario de Activos de Información, los sujetos a copia de seguridad son los de criticidad:

- **Alta:** Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
- **Media:** Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio.

Para la Corporación, entre los activos de información sujetos a copia de seguridad se encuentran:

- **Bases de datos:** Previamente el responsable del sistema de información o quien hace las veces de DBA, debe generar una copia de seguridad de la base de datos e informar la ruta del archivo generado para su posterior parametrización en la herramienta de copias de seguridad.
- **Carpetas y archivos:** Almacenados en rutas o repositorios específicos.
- **Servidores virtuales y físicos:** Se identifican las carpetas y archivos a los cuales se requiera generar copia de seguridad.

| No. | NOMBRE DEL ACTIVO DE INFORMACIÓN | DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN | NOMBRE ACTIVO DE INFORMACIÓN EN LA HERRRAMIENTA DE COPIAS DE SEGURIDAD | DESCRIPCIÓN DE LO QUE SE LE HACE COPIA EN LA HERRAMIENTA DE COPIAS DE SEGURIDAD | TIPO ACTIVO DE INFORMACIÓN |
|---|---|---|---|---|---|
| 1 | Oracle Virtualization Manager | Servidor virtual (Linux) administrador de las máquinas virtuales de Oracle. KVM | Oracle OVM Manager | Al servidor virtual | Servidor virtual |
| 2 | VxRail Manager | Virtualizador de gestión de clúster de hiperconvergencia (VxRail) | VxRail Manager | Al servido virtual | Servidor virtual |
| 3 | Directorio Activo | Máquina Virtual para administrar el directorio activo de la Corporación. | AD-CVC.cvc.gov.co | Servidor Virtual para administrar el directorio activo de la Corporación. | Servidor virtual |
| 4 | CVCP | Esquema agrupado de base de datos | cvcp | A la base de datos Oracle de:<br>* SABS<br>* SIGEC<br>* SIPA<br>* LIMS<br>* SFI<br>* Queryx (Nómina) V7 | Carpeta/Archivo |

| | | | | | |
|---|---|---|---|---|---|
| 5 | JD EDWARDS ENTERPRISE ONE - Base de datos producción | Sistema de información tipo ERP, para el cual actualmente las funcionalidades financieras de Contabilidad, Cuentas por pagar y Presupuesto. | bdjde.cvc.gov.co | A la base de datos de PRODUCCIÓN Oracle de JD EDWARDS PRODUCCIÓN | Carpeta/Archivo |
| 6 | JD EDWARDS ENTERPRISE ONE - Base de datos prueba | Sistema de información tipo ERP, para el cual actualmente las funcionalidades financieras de Contabilidad, Cuentas por pagar y Presupuesto. | jdeprueba | A la base de datos de PRUEBAS ORACLE de JD EDWARDS. (Del servidor virtual) | Carpeta/Archivo |
| 7 | JD EDWARDS ENTERPRISE ONE - Carpetas lógica | BD - Servidor físico de Lógicas (Linux) - Logicalde - de JD EDWARDS | logicaljde | A archivos específicos de: Servidor físico de Lógicas (Linux) de JD EDWARDS | Carpeta/Archivo |
| 8 | JD EDWARDS ENTERPRISE ONE - Carpetas Weblogic | Servidor físico WebLogic (Linux) de JD EDWARDS. Capa media, servidor físico WebLogic.cvc.gov.co | weblogic | A archivos específicos de: Servidor físico WebLogic (Linux) de JD EDWARDS. Capa media, servidor físico WebLogic.cvc.gov.co | Carpeta/Archivo |
| 9 | JD EDWARDS ENTERPRISE ONE - Carpetas Deployment | BD - Servidor físico DEPLOYMENT - JD Edwards (Windows) | jdedep | A archivos específicos de: Servidor físico DEPLOYMENT (Windows) - JD Edwards | Carpeta/Archivo |
| 10 | JD EDWARDS ENTERPRISE ONE - Servidor virtual pruebas | Sistema de información tipo ERP, para el cual actualmente las funcionalidades financieras de Contabilidad, Cuentas por pagar y Presupuesto. | jdeprueba | Servidor virtual Linux del aplicativo JD EDWARDS | Servidor virtual |
| 11 | Sistema de Información para Gestión de Calidad - DARUMA Software | Sistema de Información que permite la gestión de la calidad, el control y el mejoramiento continuo de acuerdo a lo definido por el Modelo Integrado de Planeación y Gestión (MIPG) y la administración de riesgos de gestión, corrupción y seguridad de la información definidos por el Departamento Administrativo de la Función Pública (DAFP) | cvcpad19c.cvc.gov | A la base de datos DARUMA | Carpeta/Archivo |
| | | Sistema de Información que permite la gestión | | | |

| | | | | | |
|---|---|---|---|---|---|
| 12 | Sistema de Información para Gestión de Calidad - DARUMA Software | de la calidad, el control y el mejoramiento continuo de acuerdo a lo definido por el Modelo Integrado de Planeación y Gestión (MIPG) y la administración de riesgos de gestión, corrupción y seguridad de la información definidos por el Departamento Administrativo de la Función Pública (DAFP) | DARUMA | Al servidor virtual | Servidor virtual |
| 13 | GEOCVCEXT | Sistema de Información de consulta y análisis de información cartográfica básica y temática, fruto del levantamiento y actualización constante de la información físico-biótica y social que bajo un enfoque ecosistémico se viene adelantando sobre todo el Departamento del Valle del Cauca | GEOCVCEXT | Al servidor virtual de aplicaciones del portal geo.cvc.gov.co GEOCVCEXT | Servidor virtual |
| 14 | GEOCVC | Sistema de Información de consulta y análisis de información cartográfica básica y temática, fruto del levantamiento y actualización constante de la información físico-biótica y social que bajo un enfoque ecosistémico se viene adelantando sobre todo el Departamento del Valle del Cauca | geocvc19c | A la base de datos de GEOCVC del portal geo.cvc.gov.co y de la Geodatabase de trabajo del Grupo sistema de información ambiental - versión 19C | Carpeta/Archivo |
| 15 | QUERYX SRH | Sistema de Información de Recursos Humanos (Nómina) | Queryx | Al servidor virtual - En desarrollo de Queryx 7 | Servidor virtual |
| 16 | Suite VISION GCI | Archivos específicos: Servidor virtual. CAPA MEDIA. Suite VISION GCI | cvcweb | A archivos específicos: Servidor virtual. CAPA MEDIA. Suite VISION GCI | Carpeta/Archivo |
| 17 | Intranet | Intranet PRODUCCIÓN | Intranet | Al servidor virtual | Servidor virtual |

**TABLA No. 1:** Muestra de activos de información

### 3.2.2. PARAMETRIZAR EN LA HERRAMIENTA ESPECIALIZADA LA POLÍTICA DE COPIAS DE SEGURIDAD.

La CVC cuenta con un sistema especializado para la gestión y almacenamiento de copias de seguridad comprimidas y cifradas, ubicado en el Datacenter central de la CVC.

La herramienta de gestión de copias de seguridad permite parametrizar la copia y réplica de activos de información, a través de políticas donde se establecen la periodicidad, retención y los parámetros de sincronización del sitio alterno para la gestión de réplicas.

Cada activo de información sujeto a copia de seguridad, debe ser creado, parametrizado y sincronizado en la herramienta de copias de seguridad. O cuando se trate de un activo de información que no sea nuevo, se realizan los ajustes requeridos en la herramienta.

El activo de información debe tener instalado el agente AVAMAR, el cual permite la sincronización automática con la herramienta de copias de seguridad.

Para la asignación de nombres a las políticas de seguridad, se deben considerar nombres nemotécnicos que describan el activo de información y la frecuencia de la política, esto con el fin de facilitar la revisión de su ejecución.

Para parametrizar las copias de seguridad de los activos de información, el responsable del activo de información debe suministrar la siguiente información para poder configurar la política:

**Para el caso de un servidor virtual:** Nombre de la máquina virtual

- Dirección IP de la máquina virtual
- Tamaño de la máquina virtual
- Frecuencia y horario (especificar en el caso que se requiera aplicar más de una política, ej. copia diaria, semanal y mensual)
- Retención (esta retención también debe ir ligada a la frecuencia de la copia de seguridad)

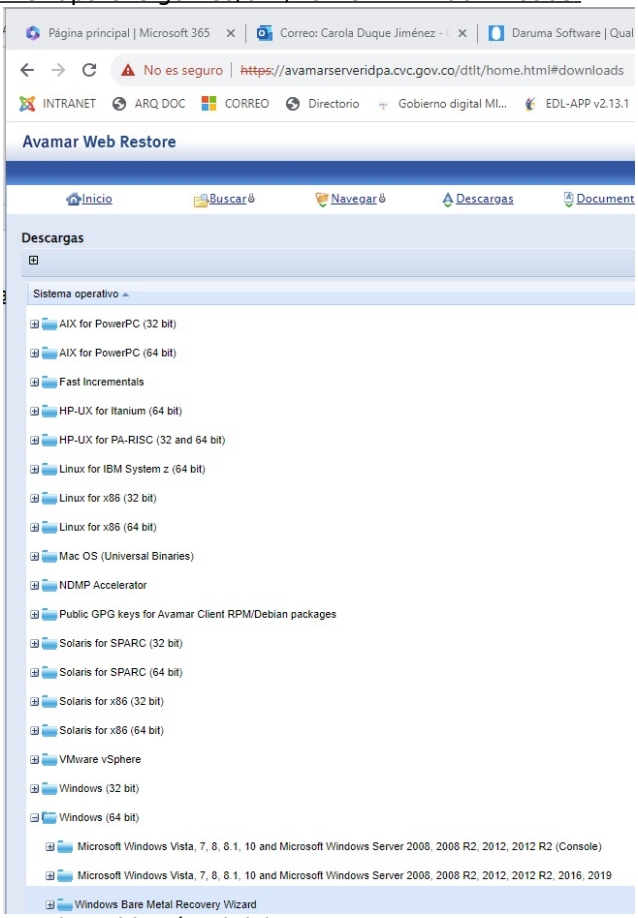
En caso de implementar un nuevo entorno de virtualización, se debe solicitar un proceso de configuración adicional para ser integrado con la herramienta de gestión de copias de seguridad.

**Para el caso de carpetas/archivos en repositorios específicos:**

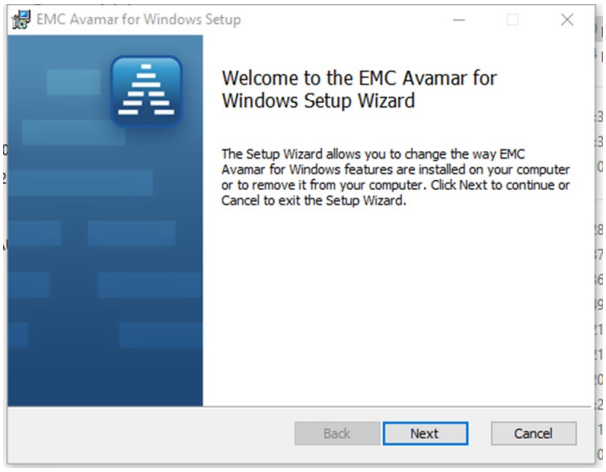
- Sistema operativo y versión
- Dirección IP
- Usuario y contraseña con permisos de ejecución (la instalación del agente la puede realizar el responsable del servidor en cuestión si así se desea)
- Ruta de las carpetas para hacer la copia
- Frecuencia y horario (especificar en el caso que se requiera aplicar más de una política, ej. copia diaria y mensual)
- Retención (esta retención también debe ir ligada a la frecuencia de la copia de seguridad)

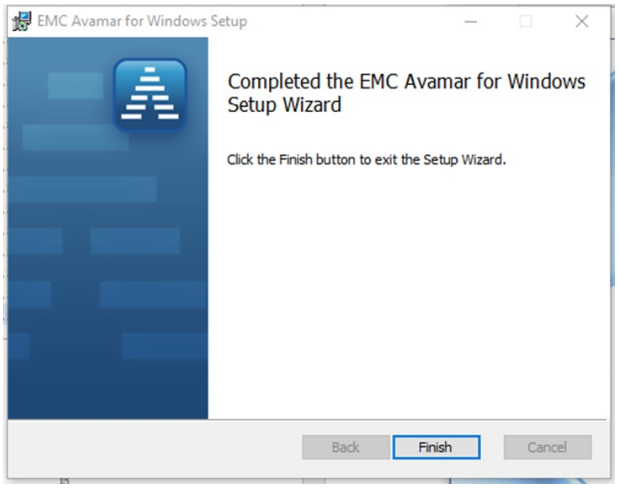
**Pasos para la instalación del agente AVAMAR:**

1. Dependiendo de la versión del sistema operativo de debe descargar el instalados para Windows y Linux de la siguiente URL: https://avamarserveridpa.cvc.gov.co/dtlt/home.html#downloads.



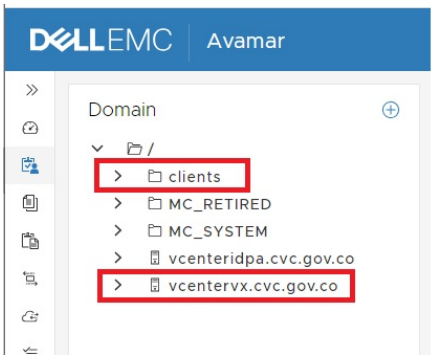

2. Se ejecuta el instalador hasta que salga el botón Finish:





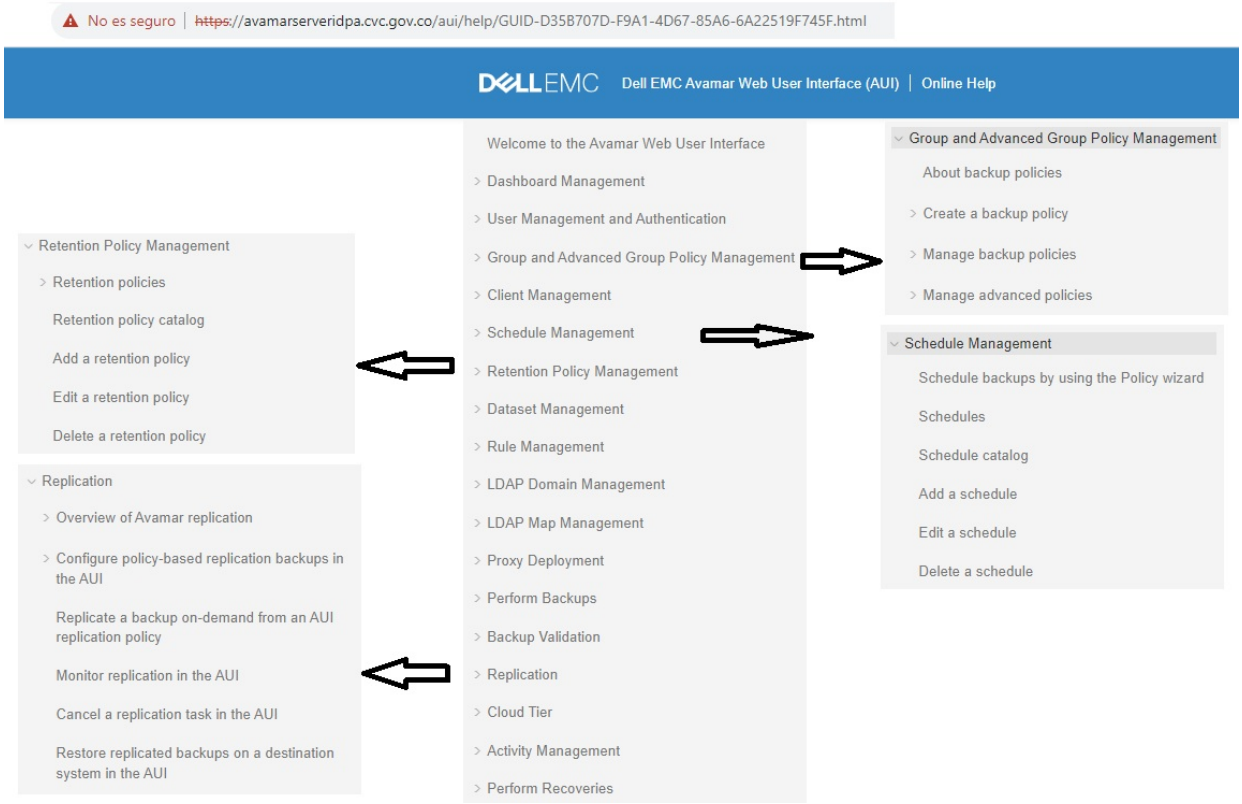
3. Luego de instalado el agente en el activo de información, se procede a realizar su activación con el fin de poder gestionarlo desde la herramienta de copias de seguridad.
    - Se ingresa a la carpeta donde se está instalado el agente de AVAMAR y se ejecuta.
    - Al ejecutar el agente, solicita la siguiente información para su sincronización con la herramienta de copias de seguridad:
        - **Dirección del servidor administrador:** avamarserveridpa.cvc.gov.co / 192.168.78.10
        - **Puerto del servidor administrador**: 28001
        - **Dominio del cliente:** /clients o /vcentervx.cvc.gov.co
        - Para Windows, se presiona el botón **Activar** y debe generarse el mensaje de información de activación exitosa "**Se activó el cliente de manera satisfactoria con mcs avamarserveridpa.cvc.gov.co:28001**.
        - El la herramienta de copias de seguridad se debería visualizar el activo de información en el dominio que se haya seleccionado.




**NOTA 1:** Para mayor información acerca de la instalación y activación del agente, consultar la página del fabricante del sistema especializado en la ruta de videos de asistencia: https://www.dell.com/support/contents/es-es/videos.

Con el activo de información creado y sincronizado en la herramienta de copias de seguridad, se procede a parametrizar las políticas de copias de seguridad y de réplicas, teniendo en cuenta la periodicidad y el tiempo de retención.

**NOTA 2:** Para mayor información acerca de la parametrización de las políticas en la herramienta de copias, consultar la ayuda del Centro de Administración de AVAMAR.




Configurada la política, se procede ejecutar una prueba de forma manual.

Los parámetros generales mínimos de periodicidad y tiempo de retención para las copias de seguridad de cada activo de información son:

1. Configurar una copia de seguridad diaria con tiempo retención mínima de 30 días. Lo que permite conservar una copia de 30 días atrás, ya que, al día siguiente al tiempo de retención, es decir, al día 31 se sobrescribe la copia de seguridad.
2. Para casos particulares solicitados, configurar una copia de seguridad semanal con tiempo de retención de mínima d e 30 días. La copia de seguridad semanal se conservará por 4 semanas, es decir, a la cuarta semana se sobrescribe la copia de seguridad.
3. Configurar el primer día del mes una copia de seguridad mensual con tiempo mínimo de retención de 12 meses. Lo que permite conservar una copia de seguridad de cada mes por un año.
4. Generar una copia de seguridad anual el primer día hábil del año. Esta copia de seguridad se debe ejecutar de forma manual de cada uno de los activos configurados en la herramienta de copias de seguridad, sin periodo de retención establecido. Se realiza de forma manual porque la herramienta de copias de seguridad no permite configurar una política de copia automática sino se le establece un período de retención.
5. Configurar una réplica de la copia de seguridad de cada uno de los activos de información, como mínimo tres (3) veces por semana.
6. Por requerimiento del responsable del activo de información, es posible contar con una parametrización diferente a lo anterior.
7. Para la generación de copias de seguridad de los activos que correspondan a carpetas/bases de datos, se aplica el principio abuelo-padre-hijo, de la siguiente manera:
    a. **Copia de seguridad Abuelo**: Consiste en realizar diariamente la primer copia de la base de datos o la carpeta, en una unidad de almacenamiento que determine el administrador de la información. Este lo realiza el DBA o quien haga sus veces.

b. **Copia de seguridad Padre**: Consiste en realizar diariamente una copia de la copia de seguridad abuelo a un equipo especializado y dedicado para almacenar las copias de forma comprimida y cifrada de acuerdo a una política establecida.
c. **Copia de seguridad Hijo:** Cada día de por medio (Lunes-Miércoles-Viernes) una de las copias generadas, deberá ser enviada a un sistema especializado para la gestión y almacenamiento diferente al que está ubicado en el Data Center principal de la CVC.

| No. | NOMBRE DEL ACTIVO DE INFORMACIÓN | DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN | NOMBRE ACTIVO DE INFORMACIÓN EN LA HERRRAMIENTA DE COPIAS DE SEGURIDAD | PERIODICIDAD COPIA DE SEGURIDAD | RETENCIÓN | RÉPLICA |
|---|---|---|---|---|---|---|
| 1 | Oracle Virtualization Manager | Servidor virtual (Linux) administrador de las máquinas virtuales de Oracle. KVM | Oracle OVM Manager | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |
| 2 | VxRail Manager | Virtualizador de gestión de cluster de hiperconvergencia (VxRail) | VxRail Manager | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |
| 3 | Directorio Activo | Máquina Virtual para administrar el directorio activo de la Corporación | AD-CVC.cvc.gov.co | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |
| 4 | CVCP | Esquema agrupado de base de datos | cvcp | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |
| 5 | JD EDWARDS ENTERPRISE ONE - Base de datos producción | Sistema de información tipo ERP, para el cual actualmente las funcionalidades financieras de Contabilidad, Cuentas por pagar y Presupuesto. | bdjde.cvc.gov.co | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |
| 6 | JD EDWARDS ENTERPRISE ONE - Base de datos prueba | Sistema de información tipo ERP, para el cual actualmente las funcionalidades financieras de Contabilidad, Cuentas por pagar y Presupuesto. | jdeprueba | SEMANAL | SEMANAL - 30 días | SI |
| 7 | JD EDWARDS ENTERPRISE ONE - Carpetas lógica | BD - Servidor físico de Lógicas (Linux) - Logicalde - de JD EDWARDS | logicaljde | DIARIA SEMANAL MENSUAL | DIARIA - 30 días SEMANAL - 30 días MENSUAL - 12 meses | SI |
| 8 | JD EDWARDS ENTERPRISE ONE - Carpetas Weblogic | Servidor físico WebLogic (Linux) de JD EDWARDS. Capa media, servidor físico WebLogic.cvc.gov.co | weblogic | DIARIA SEMANAL MENSUAL | | SI |
| 9 | JD EDWARDS ENTERPRISE ONE - Carpetas | BD - Servidor físico DEPLOYMENT - JD Edwards (Windows) | jdedep | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - | SI |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Deployment | | | | 12 meses | |
| 10 | JD EDWARDS ENTERPRISE ONE - Servidor virtual pruebas | Sistema de información tipo ERP, para el cual actualmente las funcionalidades financieras de Contabilidad, Cuentas por pagar y Presupuesto. | jdeprueba | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |
| 11 | Sistema de Información para Gestión de Calidad - DARUMA Software | Sistema de Información que permite la gestión de la calidad, el control y el mejoramiento continuo de acuerdo a lo definido por el Modelo Integrado de Planeación y Gestión (MIPG) y la administración de riesgos de gestión, corrupción y seguridad de la información definidos por el Departamento Administrativo de la Función Pública (DAFP) | cvcpad19c.cvc.gov | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |
| 12 | Sistema de Información para Gestión de Calidad - DARUMA Software | Sistema de Información que permite la gestión de la calidad, el control y el mejoramiento continuo de acuerdo a lo definido por el Modelo Integrado de Planeación y Gestión (MIPG) y la administración de riesgos de gestión, corrupción y seguridad de la información definidos por el Departamento Administrativo de la Función Pública (DAFP) | DARUMA | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |
| 13 | GEOCVCEXT | Sistema de Información de consulta y análisis de información cartográfica básica y temática, fruto del levantamiento y actualización constante de la información físico-biótica y social que bajo un enfoque ecosistémico se viene adelantando sobre todo el Departamento del Valle del Cauca | GEOCVCEXT | MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |
| | | Sistema de | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 14 | GEOCVC | Información de consulta y análisis de información cartográfica básica y temática, fruto del levantamiento y actualización constante de la información físico-biótica y social que bajo un enfoque ecosistémico se viene adelantando sobre todo el Departamento del Valle del Cauca | geocvc19c | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |
| 15 | QUERYX SRH | Sistema de Información de Recursos Humanos (Nómina) | Queryx | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |
| 16 | Suite VISION GCI | Archivos específicos: Servidor virtual. CAPA MEDIA. Suite VISION GCI | cvcweb | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |
| 17 | Intranet | Intranet PRODUCCIÓN | Intranet | DIARIA MENSUAL | DIARIA - 30 días MENSUAL - 12 meses | SI |

**TABLA No. 2:** Resumen de políticas de copias de seguridad implementadas.

### 3.2.3. EJECUTAR LA POLÍTICA DE COPIAS DE SEGURIDAD.

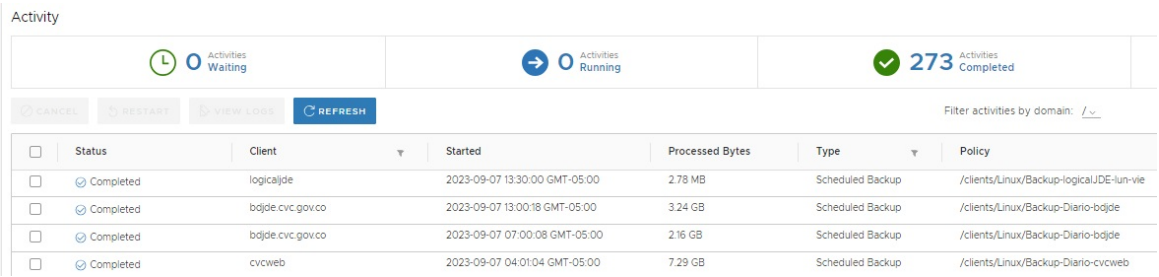
Cuando el activo de información tiene configurada la política de copia de seguridad en la herramienta, el proceso se ejecuta automáticamente.

Si por alguna razón se requiere ejecutar la política de forma manual en la herramienta de copias de seguridad, se identifica el activo de información y la política, y se ejecuta. Esta actividad se puede realizar por un requerimiento especial o por una falla en el proceso de la copia de seguridad.

**NOTA 3:** En caso de falla en el proceso, esta actividad se debe ejecutar finalizando la jornada laboral.

La copia de seguridad realizada es completa, cifrada, comprimida y almacenada.

La herramienta de copias de seguridad cuenta con registros de las actividades realizadas.




### 3.2.4. VERIFICAR EL RESULTADO DE LA EJECUCIÓN DE LA POLÍTICA DE COPIAS DE SEGURIDAD.

La herramienta de copias de seguridad utilizada por la CVC, almacena un registro de actividades a corto plazo de las políticas programadas. Para tener un registro histórico con información más completa, se debe llevar el registro en la Bitácora de Copias de Seguridad de las copias diarias y mensuales como se describe en los puntos siguientes de este instructivo.

Antes de entrar a validar detalladamente, se debe verificar en la herramienta de copias de seguridad, la opción de **Activities Failed** 

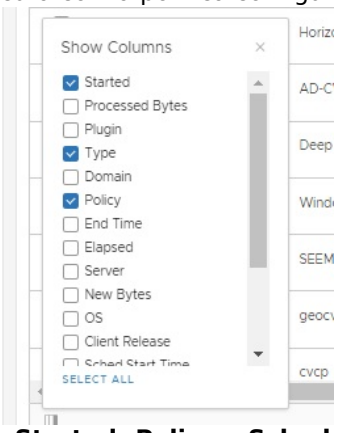
, donde se muestran las copias que generaron error.

Se debe verificar el registro de actividades en la herramienta de copias de seguridad, ingresando a la opción **Monitor/Activity.**

1. Se debe seleccionar la opción **Activities Completed** 

2. En el listado se debe filtrar en la columna **Type** las actividades con el parámetro **Scheduled Backup.**


3. Para facilitar la identificación del estado de las copias, se sugiere seleccionar las siguientes columnas:
   - **Started:** Fecha y hora de la copia
   - **Type:** Tipo de copia
   - **Policy:** Nombre de la política configurada
   - **Schedule:** Nombre de la tarea que se ejecuta con la política configurada




4. Se deben validar las columnas **Client**, **Status**, **Started**, **Policy** y **Scheduled** para determinar la acción a seguir y diligenciar la bitácora.
   - **Client:** Contiene el nombre del activo de información en la herramienta de copias de seguridad.
   - **Status:** Que indican si se realizaron con éxito o no. Para ello pueden salir los siguientes estados.
     - **Completed**: Realizada con éxito
     - **Completed w/Exception(s)**: Se completó pero tiene algunas excepciones.
     - **Failed:** Falló, para lo cual se debe ejecutar de forma manual.
     - **Timed Out - Start:** Tardó en iniciar, para lo cual se debe ejecutar de forma manual.
     - **Timed Out:** Tardó demasiado tiempo, para lo cual se debe ejecutar de forma manual.
     - **Running:** Aún se está ejecutando, para lo cual se debe dar un tiempo. Sino termina, se cancela y se vuelve a ejecutar de forma manual.
     - **No vm:** No existe el servidor virtual
5. Si el estado de alguna copia de seguridad fue fallida, se debe ejecutar la política de forma manual.
6. Se debe diligenciar la bitácora.

**NOTA 4:** La verificación de la ejecución de las políticas de copias de seguridad se debe realizar diariamente durante los días hábiles y para las copias mensuales, el día laboral siguiente a su ejecución.

### 3.2.5. REGISTRAR EN LA BITÁCORA DE COPIAS DE SEGURIDAD EL RESULTADO DE LA EJECUCIÓN DE LA POLÍTICA.

La Bitácora de Copias de Seguridad debe contener como mínimo los siguientes datos:

- **NOMBRE DEL ACTIVO DE INFORMACIÓN** (Como está en la herramienta de copias de seguridad)
- **DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN**
- **PERIODICIDAD**: Diaria, semanal, mensual o personalizada
- **MEDIO**: Destino de la copia
- **PROCESO DE COPIA**: Manual o automática
- **FECHA DE LA COPIA**: Corresponde a la columna Started
- **ESTADO DE LA COPIA**: Corresponde a la columna Status
- **OBSERVACIONES:** Información adicional de un evento especial
- **REVISÓ**: Persona que diligenció la bitácora

### 3.2.6. EJECUTAR LA POLÍTICA DE RÉPLICA DE COPIAS DE SEGURIDAD.

De acuerdo a las mejores prácticas y uno de los requisitos de la Norma ISO 27002:2023, numeral 12.3.1 respaldo de la información, literal c), acerca de que las copias de respaldo, se deberían almacenar en un lugar remoto y a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal. La CVC realiza réplicas a las copias de seguridad en un sitio remoto.

Los activos de información que tengan configurado la política de réplica en la herramienta de copias de seguridad, se ejecutarán de forma automática de acuerdo a la periodicidad programada. Se podrán ejecutar políticas de réplicas de forma manual cuando se considere necesario o se haya presentado falla en la ejecución de alguna de las políticas.

Las réplicas a las copias de seguridad están parametrizadas para ejecutarse de forma automática tres (3) veces por semana (lunes, miércoles y viernes). Se podrán aplicar excepciones de acuerdo a la transaccionalidad de la información por requerimiento del responsable del activo de información.

**NOTA 5:** Cuando se requiera ejecutar la réplica de forma manual se debe realizar finalizando la jornada laboral para evitar la saturación del canal de datos.

### 3.2.7. VERIFICAR EL RESULTADO DE LA EJECUCIÓN DE LA POLÍTICA DE RÉPLICA DE COPIAS DE SEGURIDAD.

La herramienta de copias de seguridad utilizada por la CVC, almacena un registro de actividades a corto plazo de las políticas programadas. Para tener un registro histórico con información más completa, se debe llevar el registro en la Bitácora de Réplicas de Copias de Seguridad de las réplicas realizadas como se describe en los puntos siguientes de este instructivo.

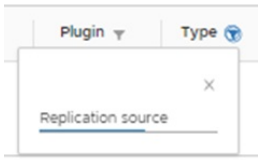
Antes de entrar a validar detalladamente, se debe verificar en la herramienta de copias de seguridad, la opción de **Activities Failed** 

, donde se muestran las copias que generaron error.

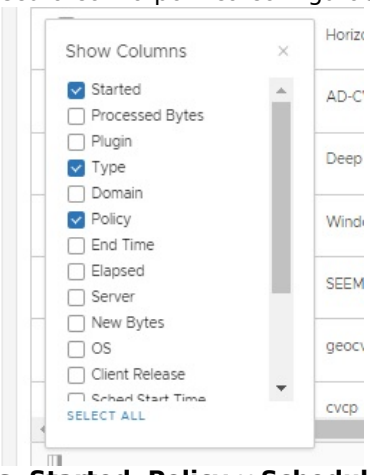
Se debe verificar el registro de actividades en la herramienta de copias de seguridad, ingresando a la opción **Monitor**/**Activity**.

1. Se debe seleccionar la opción **Activities Completed** 

2. En el listado se debe filtrar en la columna **Type** las actividades con el parámetro **Replication source**.




3. Para facilitar la identificación del estado de las réplicas, se sugiere seleccionar las siguientes columnas:
   - **Started:** Fecha y hora de la copia
   - **Type:** Tipo de copia
   - **Policy:** Nombre de la política configurada
   - **Schedule:** Nombre de la tarea que se ejecuta con la política configurada




4. Se deben validar las columnas **Client**, **Status**, **Started**, **Policy** y **Scheduled** para determinar la acción a seguir y diligenciar la bitácora.
   - **Client:** Contiene el nombre del activo de información en la herramienta de copias de seguridad.
   - **Status:** Que indican si se realizaron con éxito o no. Para ello pueden salir los siguientes estados.
     - **Completed**: Realizada con éxito
     - **Completed w/Exception(s)**: Se completó pero tiene algunas excepciones.
     - **Failed:** Falló, para lo cual se debe ejecutar de forma manual.
     - **Timed Out - Start:** Tardó en iniciar, para lo cual se debe ejecutar de forma manual.
     - **Timed Out:** Tardó demasiado tiempo, para lo cual se debe ejecutar de forma manual.
     - **Running:** Aún se está ejecutando, para lo cual se debe dar un tiempo. Sino termina, se cancela y se vuelve a ejecutar de forma manual.
     - **No vm:** No existe el servidor virtual
5. Si el estado de alguna réplica fue fallida, se debe ejecutar la política de forma manual.
6. Se debe diligenciar la bitácora.

**NOTA 6:** La verificación de la ejecución de las políticas de réplicas de copias de seguridad se debe realizar el día hábil siguiente a su ejecución.

### 3.2.8. REGISTRAR EN LA BITÁCORA DE RÉPLICAS DE COPIAS DE SEGURIDAD EL RESULTADO DE LA EJECUCIÓN DE LA POLÍTICA.

La Bitácora de Réplicas de Copias de Seguridad debe contener como mínimo los siguientes datos:

- **NOMBRE DEL ACTIVO DE INFORMACIÓN** (Como está en la herramienta de copias de seguridad)
- **DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN**
- **PERIODICIDAD**: Día de la semana de la ejecución de la réplica
- **MEDIO**: Destino de la réplica
- **PROCESO DE RÉPLICA**: Manual o automática
- **FECHA DE LA RÉPLICA:** Corresponde a la columna Started
- **ESTADO DE LA RÉPLICA:** Corresponde a la columna Status
- **OBSERVACIONES**: Información adicional de un evento especial
- **REVISÓ**: Persona que diligenció la bitácora

### 3.2.9. RESTAURAR LA COPIA DE SEGURIDAD DEL ACTIVO DE INFORMACIÓN.

Cuando exista un requerimiento específico, se deberá ejecutar la restauración de la copia de seguridad de un activo de información.

El requerimiento debe contener:

- Quien lo autoriza (Personal autorizado o responsable del activo de información)
- Nombre del activo de información
- Tipo o clasificación (Archivo o servidor virtual)
- Fecha de la copia a restaurar

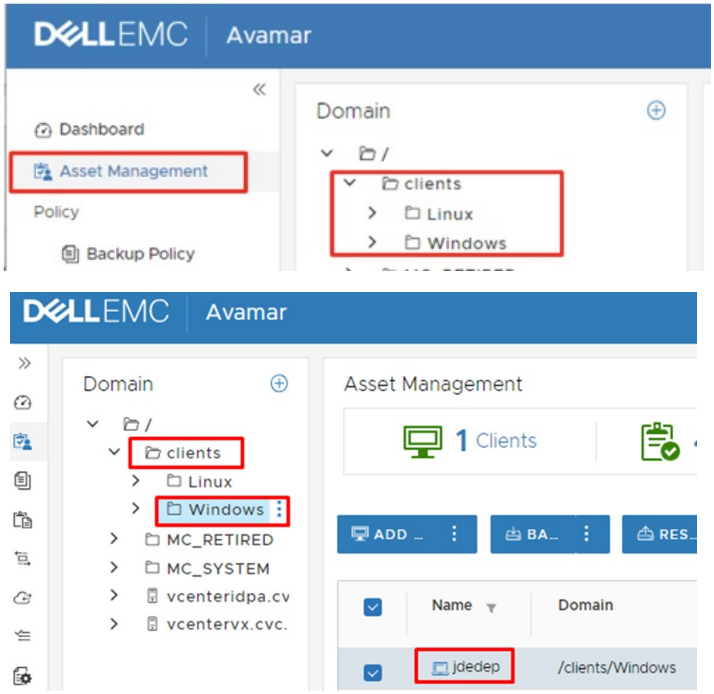
Si la solicitud no está completa se debe rechazar.

Con los parámetros de la solicitud se ubica la copia y se ejecuta el proceso de restauración a la ruta deseada. En dicho equipo deberá estar instalado el agente de la herramienta de copias de seguridad.

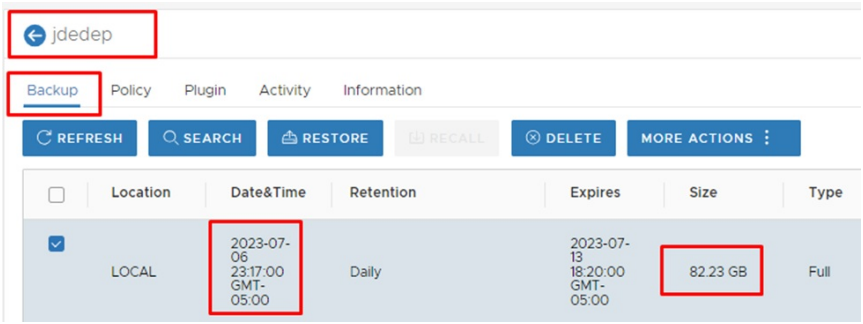
El proceso de restauración se realiza de la siguiente manera según el tipo:

**Restauración de carpetas o archivos específicos:**

1. Se debe identificar el activo de información en la herramienta de copias de seguridad. Para ello se ingresa en la opción **Asset Management** y se debe ubicar el activo en el árbol **Domain** en la opción **Clients,** como se muestra en las siguientes imágenes:



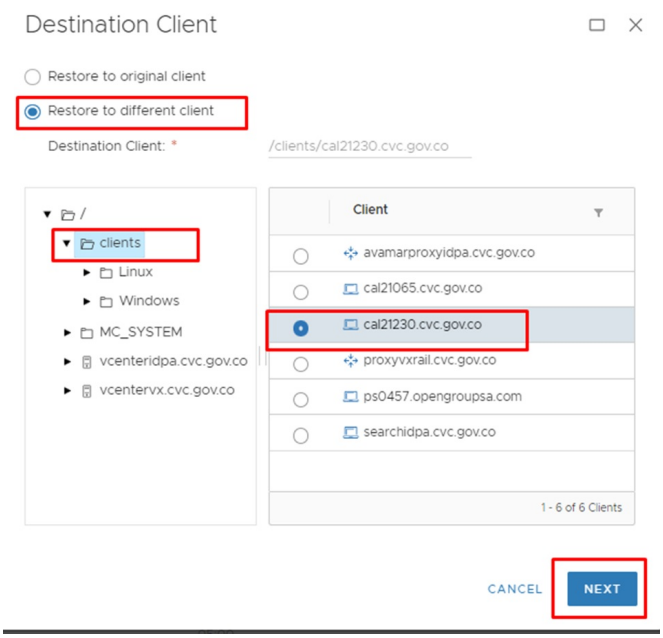

2. Cuando se ha identificado el activo que se desea restaurar, se debe ubicar la copia de seguridad a partir de la cual se va a realizar el proceso de restauración. Se debe seleccionar la opción **VIEW MORE** y en la pestaña **Backup** seleccionar la copia de seguridad deseada.




3. Se debe determinar el tipo y tamaño del medio de almacenamiento requerido para que se lleve a cabo satisfactoriamente el proceso de restauración. Se debe tener en cuenta el espacio disponible y el estado del medio destino.

4. Para iniciar el asistente de restauración se debe dar clic en el botón **RESTORE.**

El asistente solicitará que se determine el cliente destino de la copia. Se debe determinar si se desea restaurar en el cliente original o en un cliente de destino diferente.




Se debe determinar en la opción **Backup Content**, el contenido que es objeto de restauración.

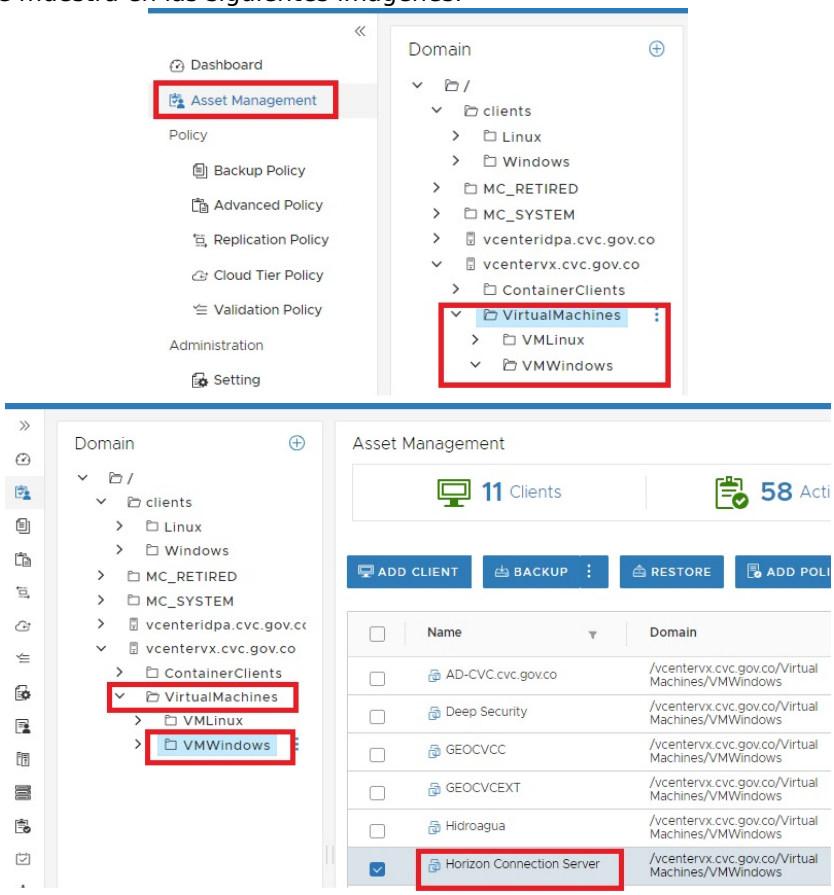
Se debe determinar la ruta donde se va a restaurar la copia de seguridad. En la opción **Destination Location** se debe seleccionar **Restore everything to a different location** y se selecciona la carpeta destino en la opción **CHOOSE**.

Con los parámetros ingresados se puede iniciar el proceso de restauración. Verifique que los parámetros son válidos e inicie el proceso de restauración dando clic en el botón **FINISH**.

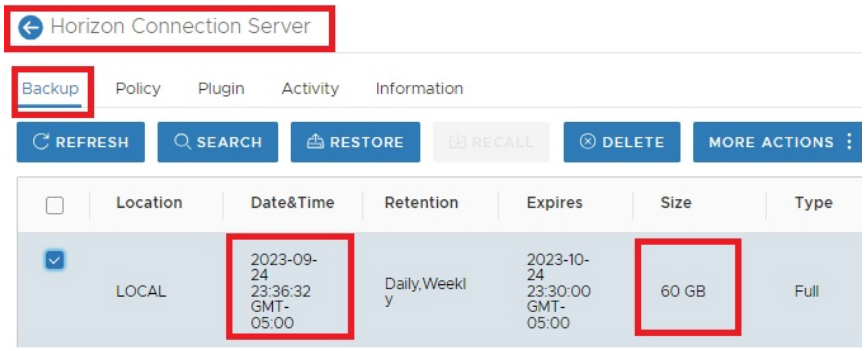
Para confirmar el proceso de restauración, se debe validar que en la ruta destino haya sido restaurada la información solicitada.

**Restauración de servidor virtual:**

1. Se debe identificar el servidor virtual en la herramienta de copias de seguridad. Para ello se ingresa en la opción **Asset Management** y se debe ubicar el servidor en el árbol **Domain** en la opción **vcentervx.cvc.gov.co, VirtualMachines** como se muestra en las siguientes imágenes:




2. Cuando se ha identificado el activo que se desea restaurar, se debe ubicar la copia de seguridad a partir de la cual se va a realizar el proceso de restauración. Se debe seleccionar **VIEW MORE** y en la pestaña **Backup** seleccionar la copia de seguridad deseada.




3. Para iniciar el asistente de restauración se debe dar clic en el botón **RESTORE.**

**NOTA 6**: Para continuar con el proceso de restauración se debe contar con un entorno de virtualización el cual se debe sincronizar con la plataforma Avamar.

**NOTA 7**: Para mayor información acerca de la restauración de un servidor virtual, consultar la ayuda del Centro de Administración de AVAMAR.

**NOTA 8:** Si la restauración de la copia de seguridad no fue exitoso se repite el proceso.

### 3.2.10. REGISTRAR EN LA BITÁCORA DE RESTAURACIÓN DE COPIAS DE SEGURIDAD EL RESULTADO DE LA RESTAURACIÓN.

La Bitácora de Restauración de Copias de Seguridad debe contener como mínimo los siguientes datos:

- **FECHA RESTAURACIÓN:** DIA-MES-AÑO
- **NOMBRE DEL ACTIVO DE INFORMACIÓN** (Como está en la herramienta de copias de seguridad)
- **TIPO**: Carpeta o servidor
- **FECHA DE LA COPIA DE SEGURIDAD A RESTAURAR**: DIA-MES-AÑO
- **MEDIO**: Destino de la restauración
- **ESTADO DEL PROCESO DE RESTAURACIÓN:** Normal o con errores
- **SOLICITADO POR**
- **TAMAÑO DE LA RESTAURACIÓN**
- **OBSERVACIONES**
- **QUIEN RESTAURÓ**

### 3.2.11. PROBAR EL ESTADO DE LA COPIA DE SEGURIDAD RESTAURADA.

El responsable del activo de información, deberá de acuerdo a su experticia validar con las pruebas necesarias la integridad de la copia de seguridad restaurada y generar un informe como evidencia.

## 4. ANEXOS

- **Anexo 1: PT.0720.27 Gestión de Copias de Seguridad**
- **Anexo 2:** Bitácora de Copias de Seguridad
- **Anexo 3:** Bitácora de Réplicas de Copias de Seguridad
- **Anexo 4:** Bitácora de Restauración de Copias de Seguridad