INSTRUCTIVO: Gestión de Copias de Seguridad			
FECHA DE APLICACIÓN: 2024-09-10	**CÓDIGO:** IN.0720.04	**VERSIÓN:** 002	
ELABORADO POR: FABIAN EDUARDO ROJAS GALLEGO PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION CAROLA DUQUE JIMENEZ TECNICO ADMINISTRATIVO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	**REVISADO POR:** PAMELA KATHERINE ENRIQUEZ PAZ PERSONAL DE APOYO GRUPO GESTIÓN AMBIENTAL Y DE CALIDAD EDWIN RUANO GAMBOA PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	**APROBADO POR:** DIEGO ALEXANDER MILLAN LONDOÑO JEFE DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	CVC Corporación Autónoma Regional del Valle del Cauca

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 ejecutarse completa y almacenarla de forma comprimida y cifrada.
c. La OTI debe incorporar 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 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 seguridadde las bases de datos de los sistemas de información de la CVC y su correcto funcionamiento como mínimouna (1) vez 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 con los responsables de los activos de información. 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. Cuando se requiera el apagado o reinicio de un servidor, el responsable del activo de información deberá informar al responsable de copias de seguridad para ejecutar previamente una copia de forma manual, en caso que se considere ser necesario.
m. 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 facilitará herramientas que puede usarse para tal fin.
n. Todos los funcionarios que almacenen y actualicen en recursos compartidos, como unidades de red, OneDrive y SharedPoint deberán generar una copia de seguridad de la mismacomo mínimo cada tres (3) meses.
o. 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.
p. Cuando se presenten fallas en los discos duros, se deberá realizar procesos de restauración y recuperación de la información cuando sea posible, utilizando herramientas y mecanismos técnicos y tecnológicos para intentar recuperar la información almacenada en el dispositivo averiado. Los responsables de la información validarán la integridad de la misma.
q. 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.
r. Se debe 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.

Cuando se presenten cambios en los activos de información, se deberán informar para actualizar las políticas de copias de seguridad.

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: * SABS * SIGEC * SIPA * LIMS * SFI * 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	Servidor virtual DEPLOYMENT - JD Edwards (Windows)	JDEDEP	Servidor virtual DEPLOYMENT (Windows) - JD Edwards	Servidor virtual
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
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	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 a la fecha

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 que permite parametrizar la copia y réplica de activos de información, a través de políticas que 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.

El responsable del activo de información debe informar al responsable de las copias de seguridad, los cambios que afecten la normal ejecución de las copias de seguridad.

En los equipos sujetos a copia de seguridad, se deberá instalar la utilidad que permita 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, para facilitar la revisión de su ejecución.

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

Para el caso de un servidor virtual:

- Dirección IP de la máquina virtual
- Nombre de la máquina virtual
- Nombre del equipo (host)
- 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.

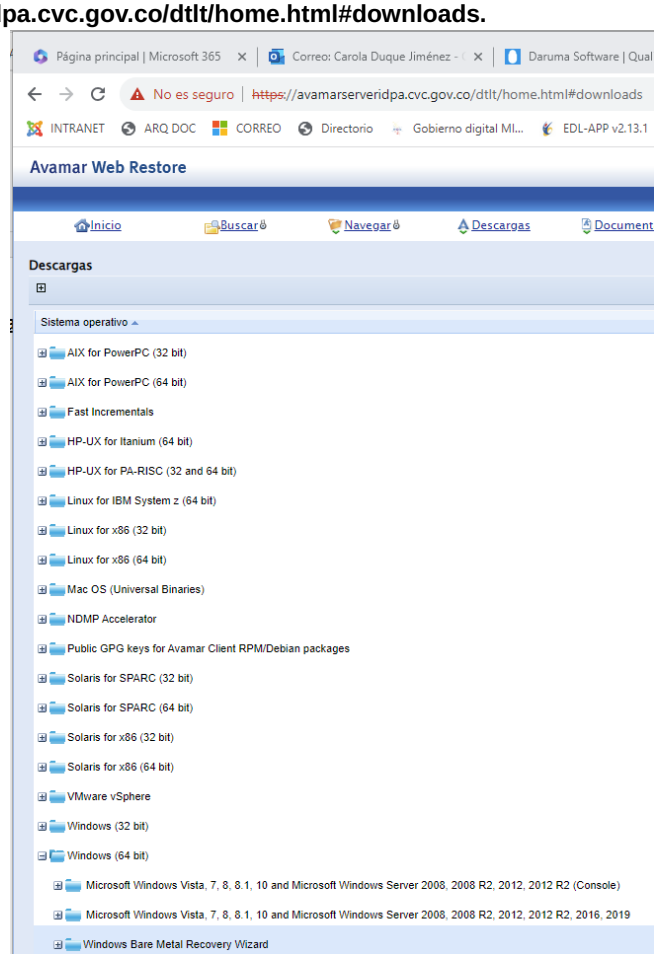
Para el caso de carpetas/archivos en repositorios específicos:

- Nombre del equipo (host)
- Dirección IP

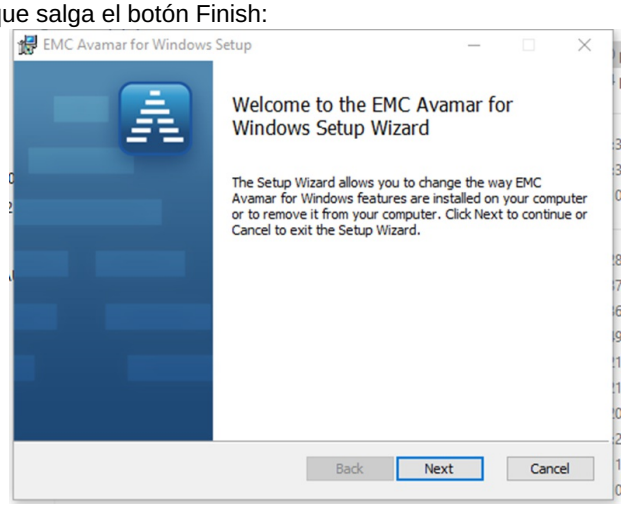
- Sistema operativo y versión
- Usuario y contraseña con permisos de ejecución (la instalación del agente la puede realizar el responsable del servidor en cuestión si así se desea)
- Ruta de las carpetas para hacer la copia
- Frecuencia y horario (especificar en el caso que se requiera aplicar más de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

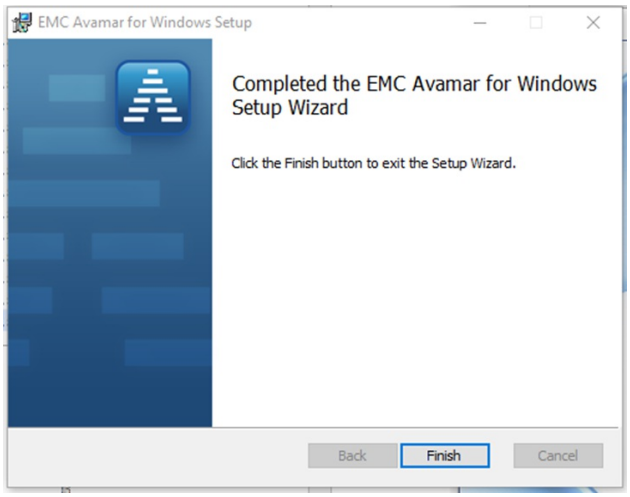
Pasos para la instalación del agente de copias de seguridad AVAMAR:

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.**

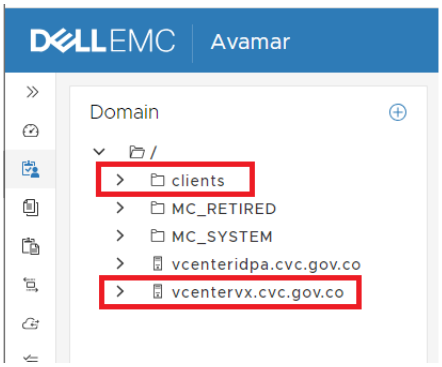


2. Se ejecuta el instalador hasta que salga el botón Finish:





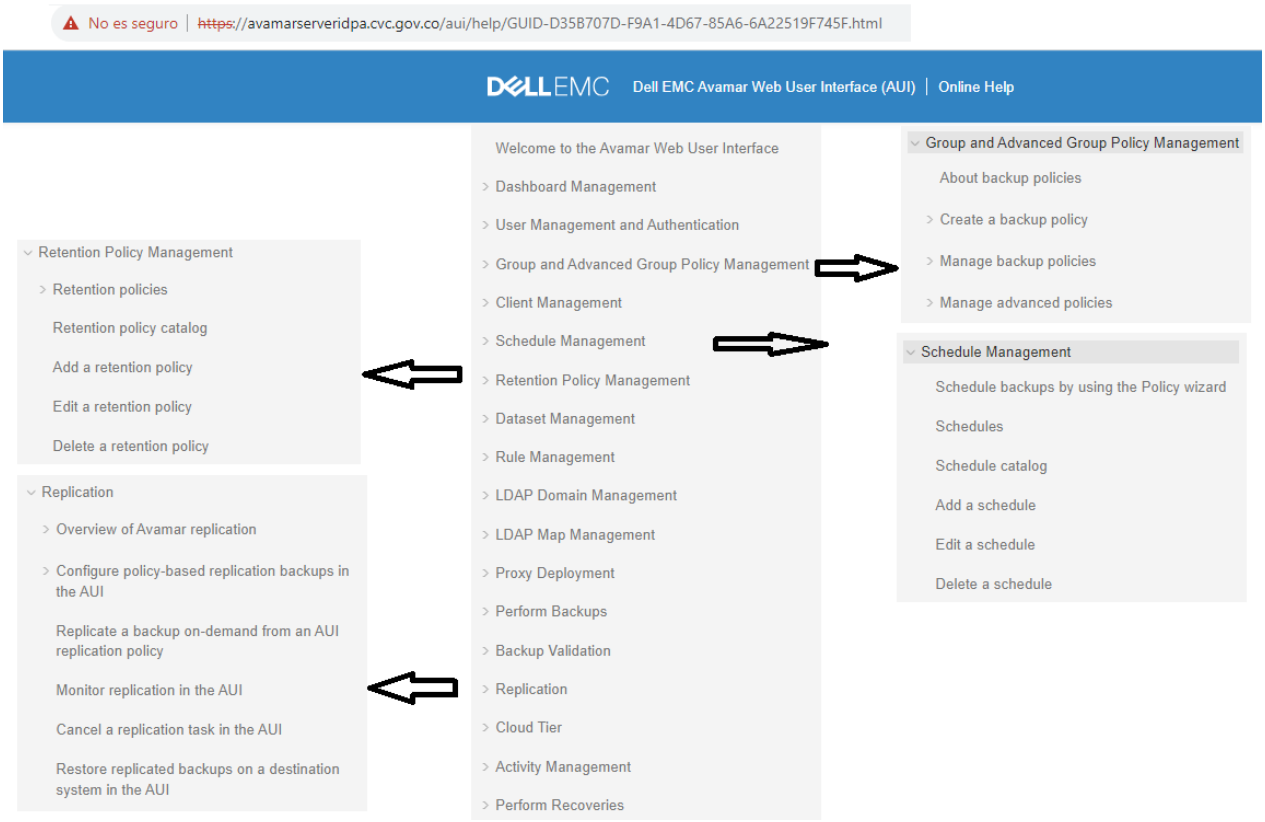
3. Luego de instalado el agente en el activo de información, se procede a realizar su activación con el fin de poder gestionarlo desde la herramienta de copias de seguridad.
    - Se ingresa a la carpeta donde se está instalado el agente de AVAMAR y se ejecuta.
    - Al ejecutar el agente, solicita la 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 utilizado actualmente en la CVC (AVAMAR), consulte la página del fabricante. **https://www.dell.com/support/contents/es-co/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 la herramienta de copias de seguridad.



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. Copia de seguridad diaria con tiempo retención mínima de 30 días.
2. Copia de seguridad semanal con tiempo de retención mínima de 30 días. Aplica solo para casos particulares a petición del responsable del activo de información.
3. Copia de seguridad mensual con tiempo mínimo de retención de 12 meses.
4. Copia de seguridad anual sin período de retención establecido, máximo los primeros quince (15) díasdel año siguiente.
5. Réplica de la copia de seguridad como mínimo tres (3) veces por semana, de las últimas cinco (5) copias de seguridad de cada uno de los activos de información con un período de retención de treinta (30) días.
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:** Los días lunes, miércoles y viernes, se deben enviar las últimas cinco (5) copias padre generadas, a un sistema especializado de copias de seguridad diferente al ubicado en 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	DIARIA - 30 días SEMANAL - 30 días MENSUAL - 12 meses	SI
9	JD EDWARDS ENTERPRISE ONE	Servidor virtual DEPLOYMENT - JD Edwards (Windows)	JDEJDEP	DIARIA MENSUAL	DIARIA - 30 días MENSUAL - 12 meses	SI
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	SEMANAL MENSUAL	SEMANAL - 30 días MENSUAL - 12 meses	SI

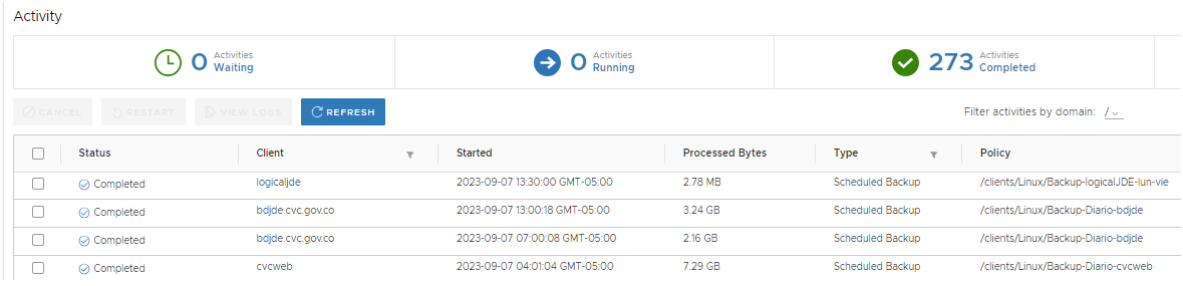
14	GEOCVC	Sistema de Información de consulta y análisis de información cartográfica básica y temática, fruto del levantamiento y actualización constante de la información físico-biótica y social que bajo un enfoque ecosistémico se viene adelantando sobre todo el Departamento del Valle del Cauca	geocvc19c	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 a la fecha.

3.2.3. EJECUTAR LA POLÍTICA DE COPIAS DE SEGURIDAD.

La herramienta de copias de seguridad, permite la configuración de políticas para que se ejecuten de forma automática según los parámetros establecidos. Cuando sea necesario ejecutar alguna política de forma manual, se debe identificar el activo de información y la política que será ejecutada.

Cuando se ejecuta una política de forma automática o manual en la herramienta, se genera un registro de actividades que permite evidenciar el estado, la fecha y hora de ejecución, entre otros, como se muestra a continuación:



NOTA 3: En caso de identificar una falla en el proceso de ejecución, esta actividad se debe ejecutar de forma manual.

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 ejecutadas. 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.

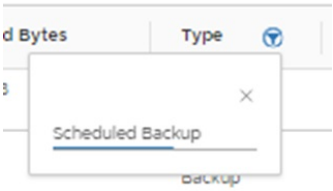
Antes de entrar a validar detalladamente, se debe verificar en la herramienta de copias de seguridad, la opción de **Activities Failed** 

, donde se muestran las copias que generaron error.

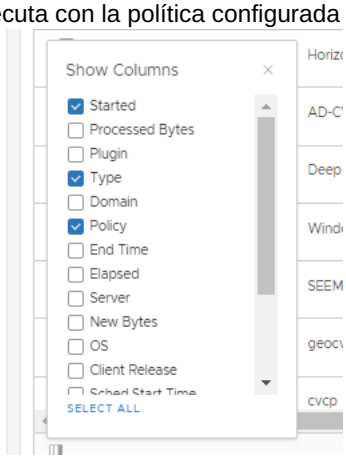
Se debe verificar el registro de actividades en la herramienta de copias de seguridad, ingresando a la opción **Monitor/Activity.**

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.
     - **Time Out - End**: Tardó en finalizar, 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 el siguiente día laboral 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.

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.

Las réplicas a las copias de seguridad están parametrizadas para ejecutarse de forma automática los días lunes, miércoles y viernes. Se replican las últimas cinco (5) copias generadas a un sistema especializado de copias de seguridad ubicado en un datacenter alterno, con un período de retención de treinta (30) días. Se pueden aplicar excepciones de acuerdo a la transaccionalidad de la información por requerimiento del responsable del activo de información.

Atendiendo las mejores prácticas y lo recomendado por la Norma ISO 27002:2013, numeral 12.3.1 Respaldo de la Información, literal c), "Las copias de respaldo se deberían almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal.", la CVC dispone de un datacenter principal y uno alterno al cual se realizan las réplicas.

NOTA 5: En caso de identificar una falla en el proceso de esta actividad se debe ejecutar de forma manual, preferiblemente en horarios que no afecten el rendimiento y disponibilidad de los recursos.

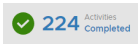
3.2.7. VERIFICAR EL RESULTADO DE LA EJECUCIÓN DE LA POLÍTICA DE RÉPLICA DE COPIAS DE SEGURIDAD.

La herramienta de copias de seguridad utilizada por la CVC, almacena un registro de actividades a corto plazo de las políticas ejecutadas. 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.

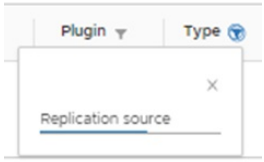
Antes de entrar a validar detalladamente, se debe verificar en la herramienta de copias de seguridad, la opción de **Activities Failed** 

, donde se muestran las copias que generaron error.

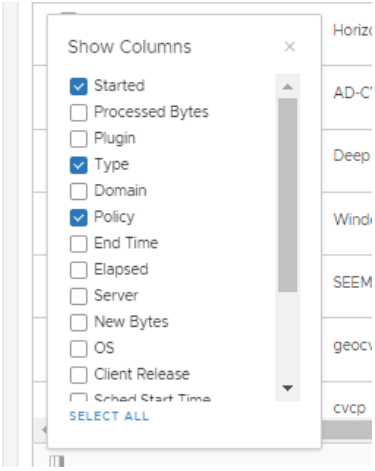
Se debe verificar el registro de actividades en la herramienta de copias de seguridad, ingresando a la opción **Monitor**/**Activity**.

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.
     - **Time Out - End**: Tardó en finalizar, 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 siguiente día laboral 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 del activo de información solicitado. Si la solicitud no está completa se debe rechazar. El requerimiento debe contener:

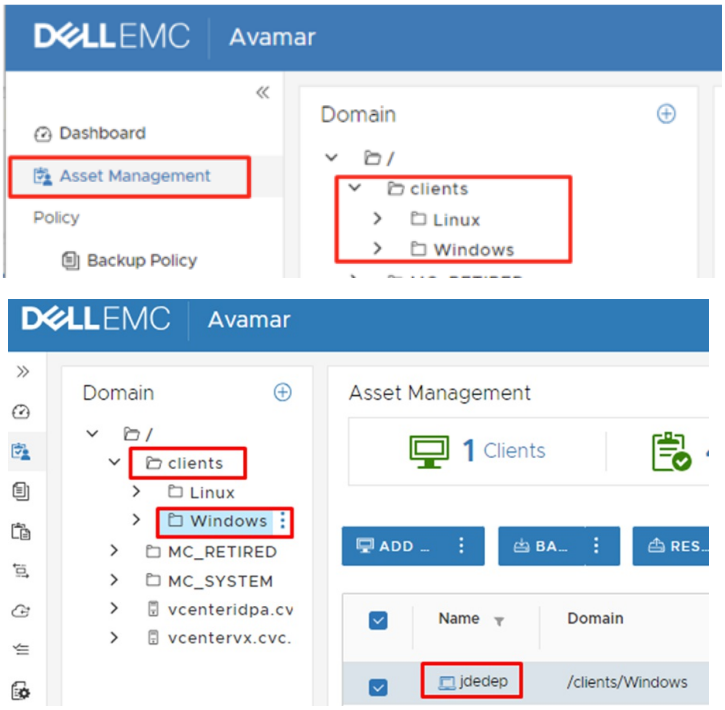
- Quien lo autoriza (Personal autorizado o responsable del activo de información)
- Nombre del activo de información
- Nombre del equipo (host)
- Dirección IP
- Tipo o clasificación (Archivo o servidor virtual)
- Fecha de la copia a restaurar

Con los parámetros de la solicitud se debe ubicar la copia y se debe ejecutar el proceso de restauración a la ruta deseada. En el equipo destino debe estar instalado el agente de la herramienta de copias de seguridad.

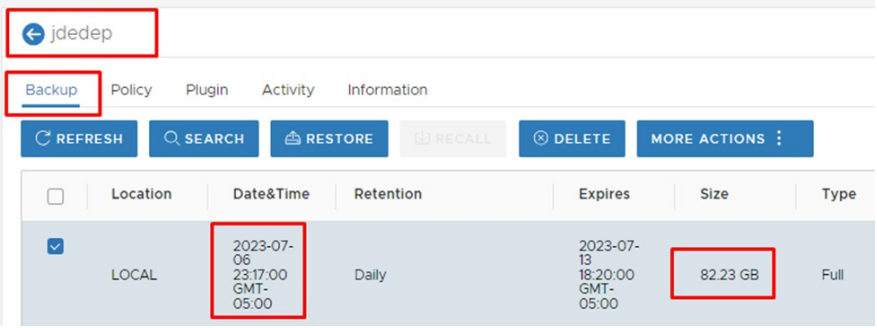
El proceso de restauración se realiza de la siguiente manera según el tipo:

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:



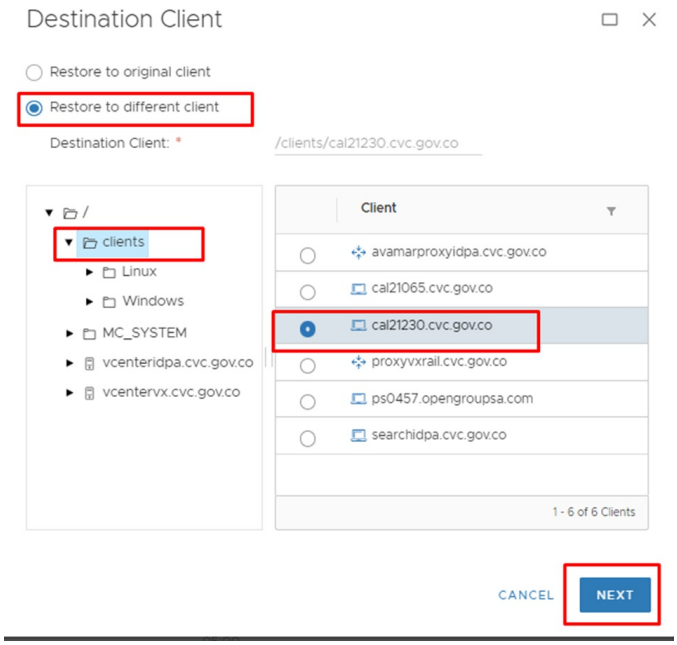
2. Cuando se ha identificado el activo que se desea restaurar, se debe ubicar la copia de seguridad a partir de la cual se va a realizar el proceso de restauración. Se debe seleccionar la opción **VIEW MORE** y en la pestaña **Backup** seleccionar la copia de seguridad deseada.



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.

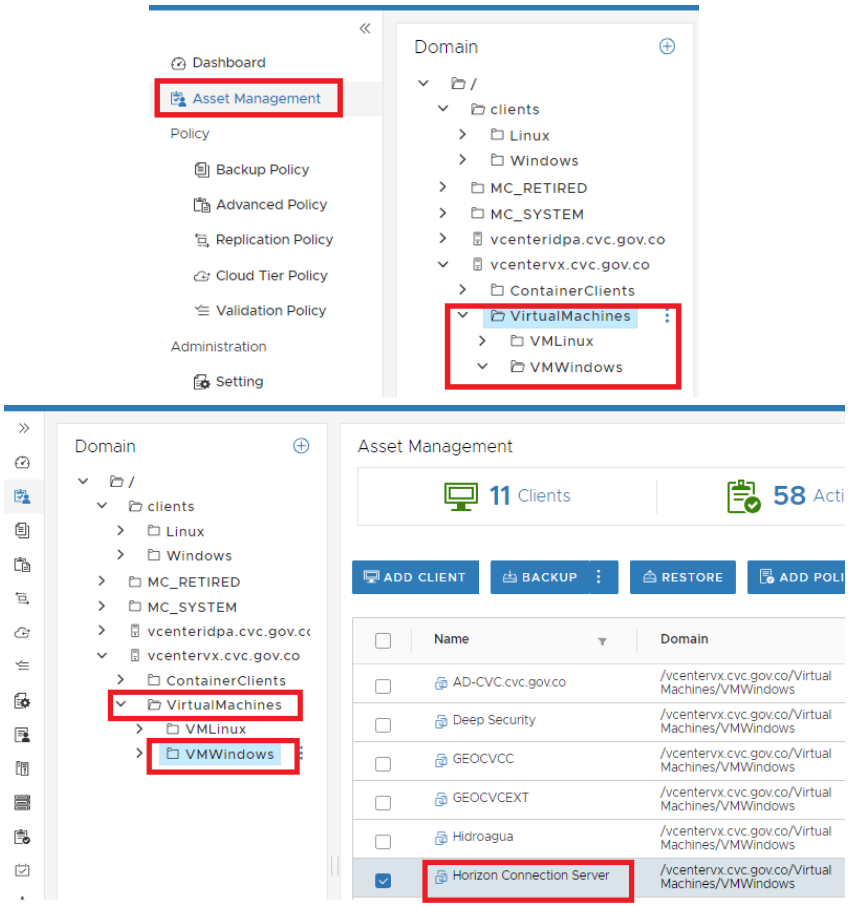
Se debe determinar la ruta donde se va a restaurar la copia de seguridad. En la opción **Destination Location** se debe seleccionar **Restore everything to a different location** y se selecciona la carpeta destino en la opción **CHOOSE**.

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**.

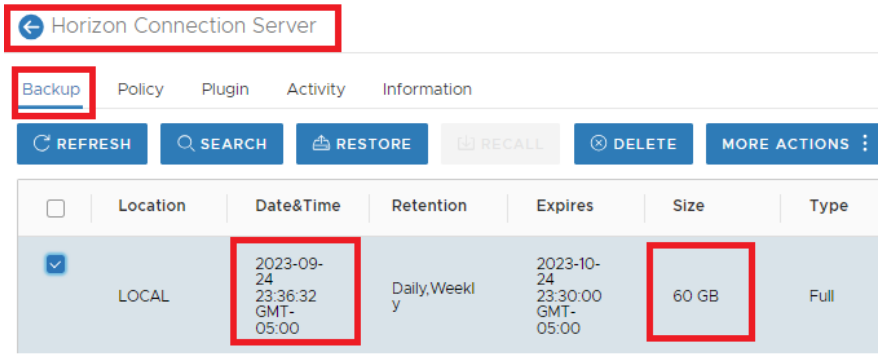
Para confirmar el proceso de restauración, se debe validar que en la ruta destino haya sido restaurada la información solicitada.

<u>Restauración de servidor virtual:</u>

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 7: Para continuar con el proceso de restauración se debe contar con un entorno de virtualización, el cual se debe sincronizar con la herramienta de copias de seguridad.

NOTA 8: Para mayor información acerca de la restauración de un servidor virtual, consulte la ayuda del Centro de Administración de la herramienta de copias de seguridad (AVAMAR).

NOTA 9: Si la restauración de la copia de seguridad no fue exitoso, se debe repetir 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 la integridad de la copia de seguridad restaurada e informar el resultado.

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**