

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	1 de 24
		VIGENTE DESDE	04/10/2022



**POLÍTICAS DE COPIA DE SEGURIDAD,
RESGUARDO Y RECUPERACIÓN DE
INFORMACIÓN DIGITAL**

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	2 de 24
		VIGENTE DESDE	04/10/2022

TABLA DE CONTENIDO

1. INTRODUCCIÓN4

2. OBJETIVO.....4

2.1 OBJETIVOS ESPECÍFICOS.....4

3. DEFINICIONES ¡Error! Marcador no definido.

4. CONDICIONES GENERALES5

5. POLÍTICAS DE COPIAS DE RESPALDO DE LA INFORMACIÓN5

5.1 RESPONSABILIDAD DE APLICACIÓN6

6. INVENTARIO DE INFORMACIÓN A RESPALDAR.....6

7. ARQUITECTURA DE SOLUCIÓN DE BACKUP9

8. HERRAMIENTAS DE TOMA DE BACKUP9

9. PROCESO TOMA DE COPIA DE RESPALDO 10

10. PROCESO DE RESTAURACIÓN..... 18

11. PRUEBAS DE RESTAURACIÓN..... 22

12. ENVÍO DE CINTA A CUSTODIA..... 22

13. ETIQUETADO DE LA CINTA 22

14. PLAN DE COPIAS DE LA INFORMACIÓN 23

15. . CONTROL DE CAMBIOS 23

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	3 de 24
		VIGENTE DESDE	04/10/2022

INDICE DE CUADROS

Cuadro No. 1. Inventario de Información a Respalidar8

Cuadro No. 2. Etiquetado de la cinta26

INDICE DE FIGURAS

Figura No. 1: Arquitectura de Backup Actual10

Figura No. 2: Herramientas para toma de backup actual.....11

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	4 de 24
		VIGENTE DESDE	04/10/2022

1. INTRODUCCIÓN

El presente documento define las políticas de copias de respaldo de información del IDIPRON, así mismo establece los esquemas y las herramientas que cuenta la Entidad para proteger y garantizar que la información esté disponible ante cualquier suceso o eventualidad por fallas humanas, desastres naturales y que sea recuperable en un tiempo de respuesta mínimo en el momento de activar un plan de continuidad ante desastres.

2. OBJETIVO


Establecer las políticas y esquemas de copias de seguridad de los servidores, servicios y bases de datos que posee el IDIPRON con el fin de garantizar la continuidad de la información y del software necesario ante una eventualidad y la recuperación ante un incidente.

2.1 OBJETIVOS ESPECÍFICOS

- Definir las Políticas de backup.
- Establecer el plan de copias de la información.
- Definir el inventario de la información a resguardar.
- Definir el esquema de etiquetado de cinta.
- Establecer procedimientos y esquema de restauración de la información.

3. GLOSARIO

TÉRMINO	DEFINICIÓN
Backup (copia de respaldo o copia de seguridad)	Es una copia de la información, datos, base de datos, archivos, aplicaciones, software o imágenes en un medio de almacenamiento externo, con la finalidad de poder recuperar la información en caso de un incidente, como, por ejemplo: daño, borrado accidental, desastre natural.
Cell manager	Servidor donde está instalado el software para realizar los respaldos programas.
DataProtector	Software encargado de la ejecución de copias de respaldo a múltiples máquinas de una misma red.
Drive	Es la unidad donde se pueden leer y escribir las cintas del Dataprotector.
Host	Computador conectado a una red, el cual es administrado por recursos de la misma.
IP	Internet Protocol: es el número que identifica un dispositivo en una red.
Librería de cintas	Dispositivo donde guarda en magazín cintas para poder realizar respaldos y restore por medio de la ejecución de un drive el cual también complementa la librería
Log	Registro de actividades.
Pool de Cintas	Conjunto de cintas empleadas como medio de almacenamiento.

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	5 de 24
		VIGENTE DESDE	04/10/2022

TÉRMINO	DEFINICIÓN
Restore	Restauración de un sistema a un estado determinado utilizando una cinta de backup, en la que se ha respaldado previamente la información.
Usuario	Persona quien reporta una solicitud de servicio, puede ser de un cliente externo o interno.
UPI	Unidad de Protección Integral

4. CONDICIONES GENERALES

Las solicitudes de requerimientos deben realizarse a través del software de mesa de ayuda como primera opción y canal oficial con la finalidad de poder garantizar que el caso quede debidamente registrado. En caso de no poder registrar el requerimiento a través de la mesa de ayuda, este se realizará mediante correo electrónico o memorando.

Cada dependencia debe establecer la información que requiere ser resguardadas de acuerdo con su tabla de retención documental o propósito.

La Oficina de Tecnologías de la Información y las Comunicaciones Realizará y garantizará pruebas periódicas a los medios que fueron generados con la finalidad de contar con mecanismos que garanticen la adecuada recuperación de la información ante una eventualidad.

Aplicar los controles necesarios de acuerdo al Modelo de Seguridad y Privacidad de la información en especial a lo estipulado en los controles del Numeral 12.1.1, 12.3.1 Respaldo de la Información de la NTC-ISO/IEC 27001.

5. POLÍTICAS DE COPIAS DE RESPALDO DE LA INFORMACIÓN

- La Oficina de Tecnologías de la Información y las Comunicaciones realiza backups a las carpetas compartidas que contienen archivos e información de todas las áreas que así lo requieren, de las bases de datos Oracle, de las aplicaciones y sistemas de información, backup de políticas y configuración firewall, de las imágenes de los servidores virtuales y físicos, backup de correos, además intranet y/o portal web, backup políticas del antivirus, backup de configuración de los Switch.
- Las pruebas de restauración se harán cada seis meses y de forma aleatoria se seleccionará una cinta con los backups realizados, y se hará su respectiva restauración en conjunto con el administrador o responsable de ese sistema.
- En caso de que se cuente con el servicio de alojamiento del portal web institucional contratado con un tercero, este debe responder por el backup de dicho portal y es responsabilidad de webmaster monitorear la generación de los backups que se generen.
- El backup de la intranet existente es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones.
- Cada vez que un funcionario se retira de la institución, la Oficina de Tecnologías de la Información y las Comunicaciones verificará la desactivación de los permisos (correo, accesos a carpetas compartidas, y perfiles de usuario de los diferentes sistemas de información). En caso de los contratistas deberá diligenciar el certificado de entrega a cargo del contratista.

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	6 de 24
		VIGENTE DESDE	04/10/2022


- La Oficina de Tecnologías de la Información y las Comunicaciones no se hace cargo de la información que el funcionario entrega al líder del proceso, jefe de área o unidad y/o supervisor.
 - El administrador del Sistema de Información o plataforma tecnológica deberá informar a través de la plataforma de mesa de ayuda o correo Institucional al administrador de la plataforma de backup a qué carpetas o subcarpetas se le debe realizar backup y con qué periodicidad.
 - Cuando se cuente con proveedores, se les debe exigir a los mismos la realización de los backups de la información del servicio contratado (ejemplo hosting portal web), deben responder por los backup de la información.
 - En las sedes o Unidades de Protección Integral (UPI) que no cuentan con un equipo de cómputo servidor, la Oficina de Tecnologías de la Información y las Comunicaciones, instalará en un equipo de cómputo del área administrativa el agente del software de backup. De igual manera designará una ruta o carpeta, la cual deberá contener la información institucional que requiera ser resguardada de acuerdo con la naturaleza de la misionalidad o tabla de retención documental de dicha UPI. La información va a ser copiada al final de cada mes, y se borrará posteriormente. Cabe acotar que el responsable de la UPI designará la(s) persona(s) encargada(s) de alojar la información de esa sede en el equipo asignado para tal fin. La carpeta debe nombrarse con el nombre de dicha sede (ejemplo: UPI Servita).
- Nota: se recomienda que los nombres de los archivos contenidos en esa carpeta no sean extensos, ya que, al momento de ser trasladados, los nombres de los archivos que sean demasiados largos generarán problemas de copiado.
- En las sedes o Unidades de Protección Integral (UPI) que cuentan con un equipo de cómputo servidor, la Oficina de Tecnologías de la Información y las Comunicaciones instalará el agente del software de backup. De igual manera designará una ruta o carpeta, el cual deberá contener la información institucional que requiera ser resguardada de acuerdo con la naturaleza de la misionalidad o tabla de retención documental de dicha UPI. La información va a ser copiada al final de cada mes, y se borrará posteriormente. Cabe acotar que el responsable de la UPI designará la(s) persona(s) encargada(s) de alojar la información de esa sede en la ruta asignado para tal fin. La carpeta debe nombrarse con el nombre de dicha sede (ejemplo: UPI Arcadia).
 - Cuando exista un servicio contratado con un tercero que maneja información del IDIPRON, este proveedor garantizar y responder por el backup de la información de acuerdo con los servicios contratados.

5.1 RESPONSABILIDAD DE APLICACIÓN

Profesionales y técnicos de la Oficina de Tecnologías de la Información y las Comunicaciones del IDIPRON.

6. INVENTARIO DE INFORMACIÓN A RESPALDAR

PLATAFORMA TECNOLÓGICA O SISTEMA DE INFORMACIÓN	TIPO	DESCRIPCIÓN	PERIODICIDAD
File System interdemilan.idipron.local)	Archivos (carpeta compartida)	Repositorio archivos áreas o dependencias sede calle 63	Full: Primer día hábil del mes incrementales: en forma diaria de lunes a sábado, hasta fin de mes. El último día hábil del mes se envía a custodia.

	GESTION DE TICS		CÓDIGO	E-GTIC-MA-03
			VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL		PÁGINA	7 de 24
			VIGENTE DESDE	04/10/2022
File System (liverpool.idipron.local)	Archivos (carpeta compartida)	Repositorio archivos áreas o dependencias sede calle 61	Full: último día del mes. Incrementales: en forma diaria de lunes a viernes, hasta el fin de mes. El último día del mes se envía a custodia.	
Bases de Datos Oracle	/arch_sicap /arch_simi /arch_sysman /back_sicap /back_simi /back_sysman /export_db	Backup de las 3 instancias de la base de datos de producción de oracle: que incluye la base de datos financiera, administrativa y misional. Incluye logs de transacciones.	Full: Primer día hábil del mes y los días domingo. incrementales: en forma diaria de lunes a sábado. A fin de mes se envía a custodia.	
Servidor Simi	C:/misApps/logs C:/ProgramFiles(x86)/Tomcat7.0/webapps G:/Archivos subidos G:/bk_logs G:/WinDirStat	Backup del registro de errores y movimientos del sistema de base de datos SIMI. Despliegue del empaquetado del SIMI. Archivos adjuntos de lo NNAJ y backup de los logs - SIMI.	Full: último día del mes. A fin de mes se envía a cinta. En otra cinta se tiene programado Full el domingo y de lunes a sábado se realiza incrementales, esta cinta se envía a custodia cuando este completa.	
Imágenes servidores virtuales	AL-AHLY ARGEL ATENAS BERLIN CASABLANCA HELSINKI KABULI LISBOA LONDRES MANCHESTER-CITY ORACLE_CLOUD_CONTROL PARIS SOFIA SRVIDIPRONAPL01 VeeamConfigBackup_porto VMWARE_VCENTER AL-NASR APOLLON BARCELONA BEITAR Estambul EVERTON FLAMENGO FORTIANALYZER-VM64 JERUSALEN JUVENTUS MACCABI OAKLANDRAIDERS PARISSG PORTAL_INSTITUCION SRVAPLMISIONAL SRVIDIPRONOAS XAMAX	Backup de imágenes de servidores virtualizados (entre Windows server y Linux)	Full último día del mes. A fin de mes se envía a custodia	

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	8 de 24
		VIGENTE DESDE	04/10/2022

Configuración y políticas del Firewall	Políticas del Firewall	Backup configuración, reglas y políticas del Firewall	Full último día del mes. A fin de mes se envía a custodia.
Imágenes servidores físicos	LIVERPOOL SHAMROCK SHELSEA ADELAIDE EUPEN	Backup de imágenes servidores físicos	Full último día del mes. A fin de mes se envía a custodia.
Configuración de Switches	Configuración de Switches	Backup de plantillas de configuración de switches del centro de cómputo sede principal calle 63.	Full cada seis meses, posterior a este periodo se envía a custodia en la cinta respectiva.
Intranet	Intranet portal institucional	Copia del servidor de aplicaciones y base de datos de la intranet.	Full todos los días (portal_idipron.sql y portal_idipron.zip), a fin de mes se envía a custodia.
Fuentes de desarrollos propios	Carpeta compartida sistemas\Backup_app_i dipron	Contiene copia de las fuentes de desarrollo de idocument.	Full último día del mes. A fin de mes se envía a custodia.
Backup de equipos y medios extraíbles	N/A	Backup que se toma en cinta a solicitud del responsable de la Secretaría General, Subdirección, Gerencia, Área o dependencia y el cual es ocasional.	N/A

Cuadro No. 1. Inventario de Información a Respaldar

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	9 de 24
		VIGENTE DESDE	04/10/2022

7. ARQUITECTURA DE SOLUCIÓN DE BACKUP

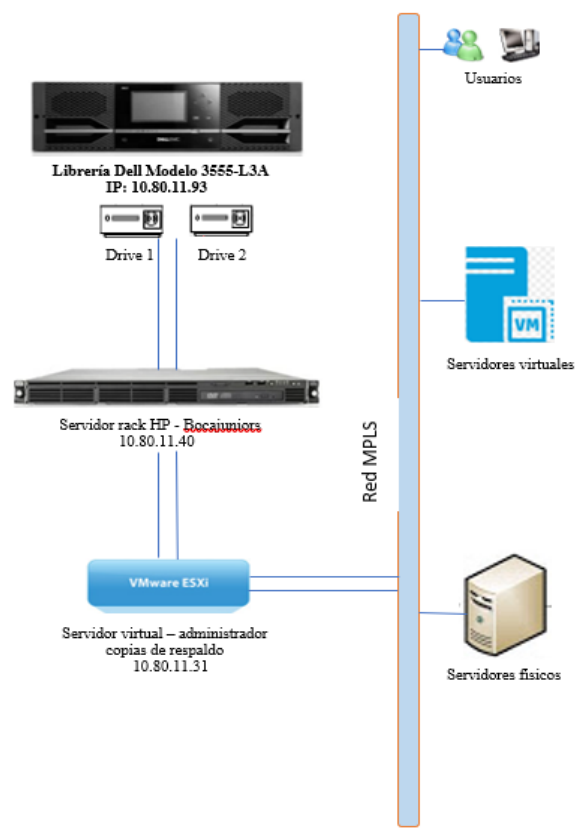


Figura No. 1: Arquitectura de Backup Actual

8. HERRAMIENTAS DE TOMA DE BACKUP

La Entidad cuenta con los siguientes programas para realizar tomas de backup de información: software dataprotector y veeambackup.

El software dataprotector es el programa que administra el envío de la toma del backup de información a la librería de cintas; y el programa veeambackup se emplea para toma de imágenes de máquinas virtuales o físicas, a su vez también se puede emplear para toma de datos de información.

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	10 de 24
		VIGENTE DESDE	04/10/2022

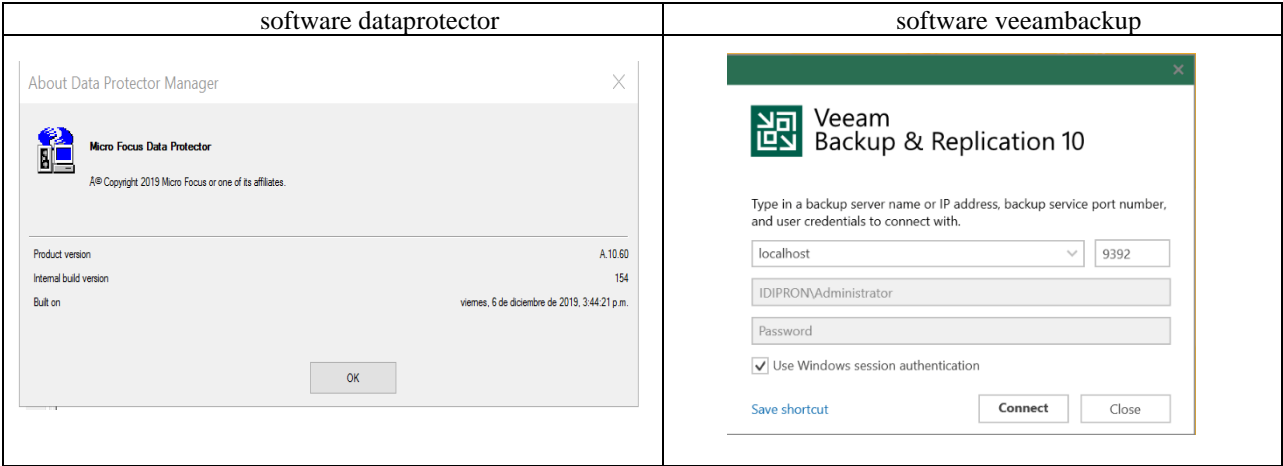


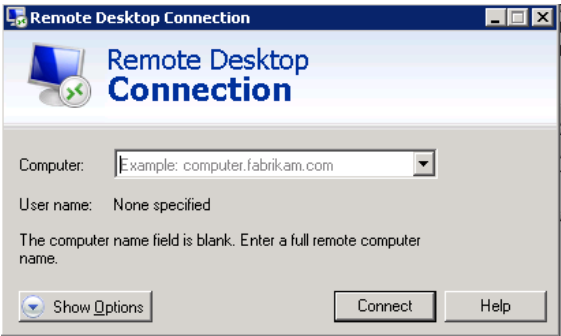
Figura No. 2: Herramientas para toma de backup actual

9. PROCESO TOMA DE COPIA DE RESPALDO

Para llevar a cabo la toma de copias de respaldo en las cintas LTO con el software de administración de copias de respaldo, se deben seguir las siguientes etapas de acuerdo con el sistema operativo en el cual va a ser instalado el agente.

Instalación en Sistema Operativo Windows

- Para instalar el agente del dataprotector, se debe dirigir al host, equipo PC o server, se puede por el terminal para comenzar a realizar la instalación de dataprotector.



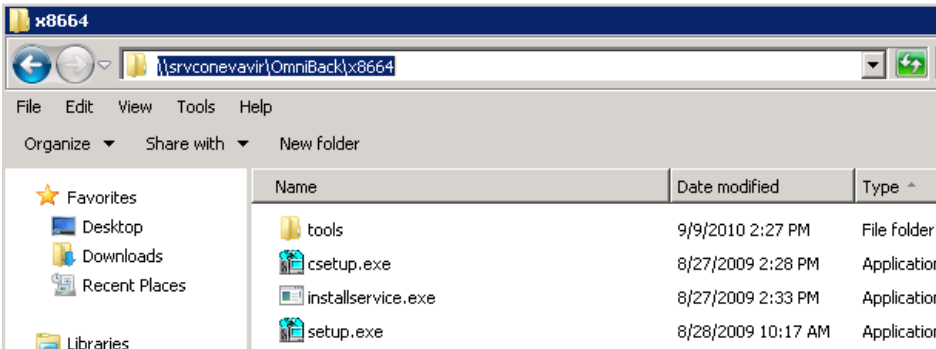
- Se debe asegurar que el host pueda tener comunicación con el Cell manager, esto se puede comprobar por medio de un ping, si no lo realiza se puede adicionar por el archivo host de sistema operativo en este caso Windows.



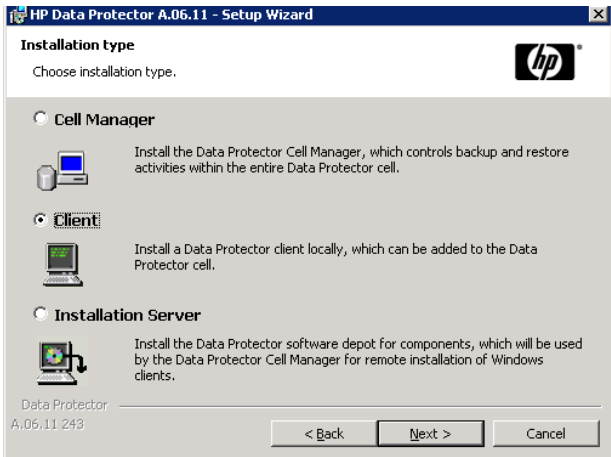
- Se debe ingresar la IP del Cell manager y el nombre para que pueda conectarse.
- Se debe mapear el nombre del Cell manager en ejecutar y buscamos la siguiente ruta:

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	11 de 24
		VIGENTE DESDE	04/10/2022

\\srvconeavir\OmniBak\x8664

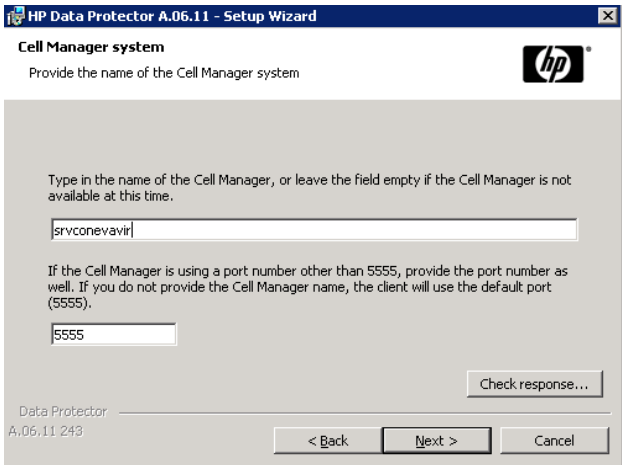


- En esta carpeta se encuentra el instalador del Dataprotector para el sistema operativo de 64bits, se debe dar doble clic sobre él y nos mostrará el asistente del paquete de instalación.
- Luego se debe indicar el tipo de instalación “Cliente”.



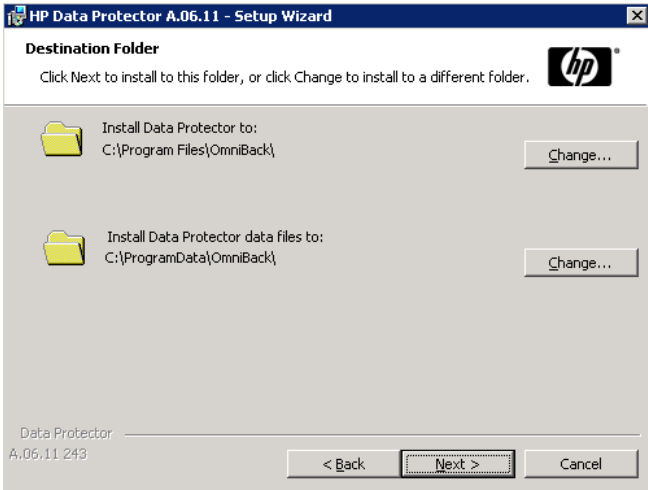
- Posteriormente se muestra un campo para poder colocar el nombre del Cell manager donde quedará configurado el host que se está instalando.

NOTA: *se debe colocar el nombre correcto o la IP del Cell manager para que pueda después importarse el host sin ningún inconveniente, de lo contrario se debe reinstalar el producto.*

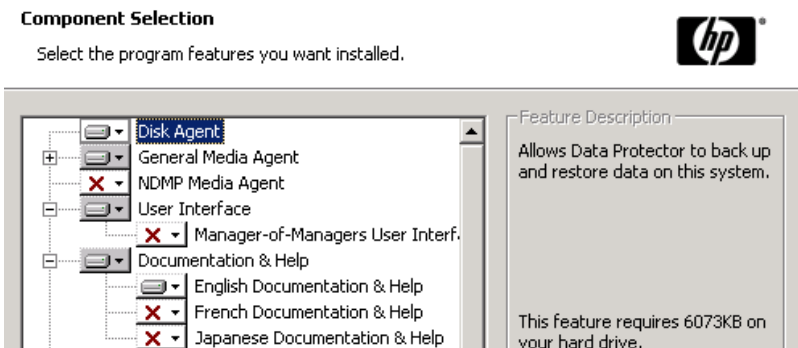


	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	12 de 24
		VIGENTE DESDE	04/10/2022

- Luego se muestra la ubicación de donde quedará la carpeta del Data protector

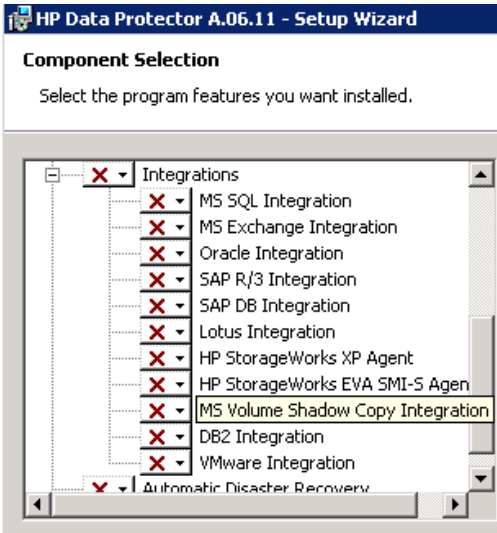


- En la siguiente imagen indica las características a instalar.



NOTA: Por defecto siempre se va a instalar disk agent y media agent que son los dos primordiales para que pueda realizar sin inconvenientes la integración.

- La siguiente imagen muestra las diferentes opciones de integración a base de datos para poder realizar la instalación en cualquiera de ellas.



Por último, se realiza la instalación y se completa el asistente.

Instalación en Sistema Operativo Linux

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	13 de 24
		VIGENTE DESDE	04/10/2022

- Se debe colocar en el host, PC o servidor el instalador correspondiente y se ubica en una carpeta vacía

```
[root@jbolli20 DP]# ls -lrt
total 1660804
-rwxrwxrwx 1 root root 1698992469 Jan 15 15:44 HP_DP_7.00_for_Linux_TD586-15005.tar.gz
[root@jbolli20 DP]#
```

- Se realiza la descompresión

```
-rwxrwxrwx 1 root root 1698992469 Jan 15 15:44 HP_DP_7.00_for_Linux_TD586-15005.tar.gz
[root@jbolli20 DP]# gunzip HP_DP_7.00_for_Linux_TD586-15005.tar.gz
[root@jbolli20 DP]#
```

- Se ejecuta la descompresión de la extensión .tar

```
-rwxrwxrwx 1 root root 1738752000 Jan 15 15:44 HP_DP_7.00_for_Linux_TD586-15005.tar
[root@jbolli20 DP]# tar -xvf HP_DP_7.00_for_Linux_TD586-15005.tar
DOCS/
DOCS/C/
DOCS/C/DP_help.tar.gz
DOCS/C/pdf/
DOCS/C/pdf/AutonomyIDOLServerIntegration.pdf
DOCS/C/pdf/IntegrationMS.pdf
DOCS/C/pdf/ZDBAdmin.pdf
DOCS/C/pdf/ProductAnnouncements.pdf
DOCS/C/pdf/IntegrationORASAP.pdf
DOCS/C/pdf/GRExtensionMSSHAREPOINT.pdf
DOCS/C/pdf/AutonomyLiveVaultIntegration.pdf
DOCS/C/pdf/Installation.pdf
DOCS/C/pdf/StoreOnceSoftwareDeduplication.pdf
DOCS/C/pdf/GRExtensionVMWARE.pdf
DOCS/C/pdf/support_matrices/
DOCS/C/pdf/support_matrices/NAS_Support_Matrix.pdf
DOCS/C/pdf/support_matrices/MO_SptMtx.pdf
DOCS/C/pdf/support_matrices/EMC_SupportMatrix.pdf
DOCS/C/pdf/support_matrices/Device_Support_Matrix.pdf
DOCS/C/pdf/support_matrices/HPEVA_SMIS_SupportMatrix.pdf
DOCS/C/pdf/support_matrices/HPDR_SupportMatrix.pdf
DOCS/C/pdf/support_matrices/Platform_Integrtn_SptMtx.pdf
DOCS/C/pdf/support_matrices/HPXP_SupportMatrix.pdf
DOCS/C/pdf/support_matrices/Virtualization_Support_Matrix.pdf
DOCS/C/pdf/support_matrices/VSS_SupportMatrix.pdf
```

- Se deben dar permisos del puerto 755 a la carpeta donde se deja el producto

```
[root@jbolli20 home]# chmod -R 755 DP
[root@jbolli20 home]#
```

- Con el paquete descomprimido se debe ingresar a la carpeta LOCAL_INSTALL

```
[root@jbolli20 DP]# ls -lrt
total 1699696
drwxr-xr-x 2 root root      4096 Aug 24  2009 Xen_sup
drwxr-xr-x 5 root root      4096 Feb 16  2011 HPSW_Integrations
drwxr-xr-x 6 root root      4096 Feb 28  2011 DOCS
drwxr-xr-x 2 root root      4096 Mar 11  2011 LICENSE
-rwxr-xr-x 1 root root     6667 Mar 12  2012 Readme.txt
drwxr-xr-x 5 root sys       4096 Mar 26  2012 linux_x86_64
drwxr-xr-x 2 root root      4096 Mar 26  2012 LOCAL_INSTALL
-rwxr-xr-x 1 root root 1738752000 Jan 15 15:44 HP_DP_7.00_for_Linux_TD586-15005.tar
[root@jbolli20 DP]# cd LOCAL_INSTALL
[root@jbolli20 LOCAL_INSTALL]# ls -lrt
total 72
-rwxr-xr-x 1 root root 68425 Mar 26  2012 omnisetup.sh
```

- Se debe ejecutar la Shell omnisetup.sh. Se debe colocar de esta manera para instalar el disk agent, el media agent y la integración, en este caso con Oracle

```
-rwxr-xr-x 1 root root 68425 Mar 26  2012 omnisetup.sh
[root@jbolli20 LOCAL_INSTALL]# ./omnisetup.sh -install da,ma,oracle8
```

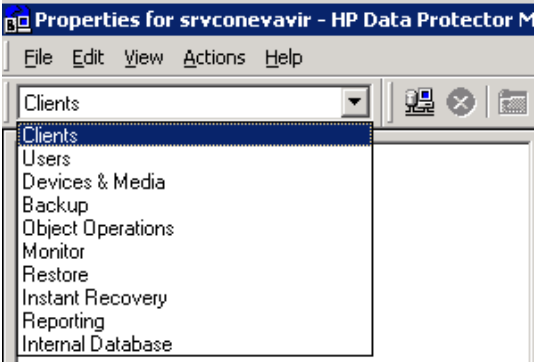
	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	14 de 24
		VIGENTE DESDE	04/10/2022

Integración del agente en el cell manager

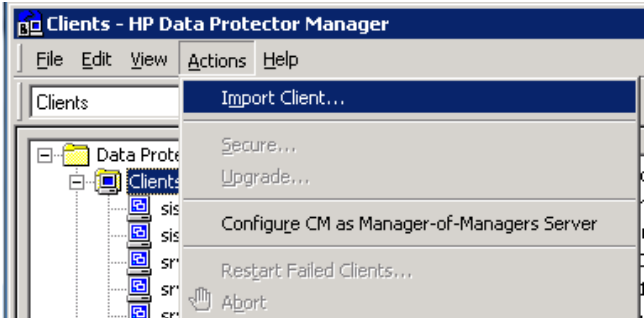
- Después de tener la instalación del agente de dataprotector en el host en el cual se va a realizar los respaldos de información, se debe dirigir al administrador Cell manager, y dar doble clic al icono de Data protector.



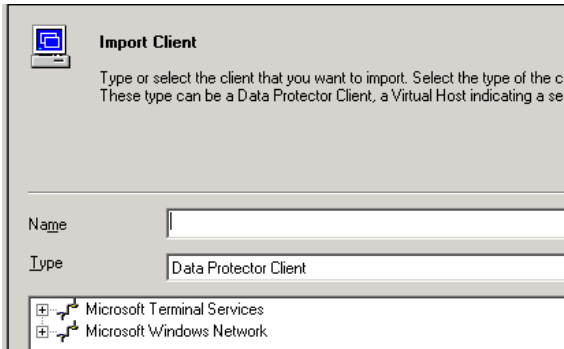
- Se debe ingresar a la opción “Clients”.



- Se debe después seleccionar la opción de Action- Import Client

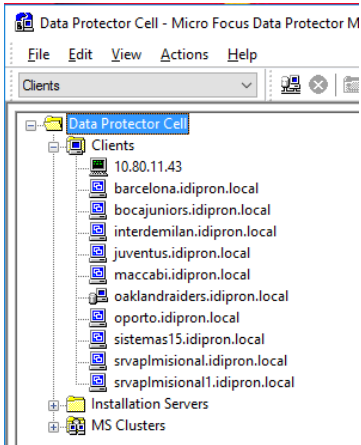


- Luego se muestra una opción para poder colocar el nombre del host en el que realizamos la instalación del agente dataprotector.

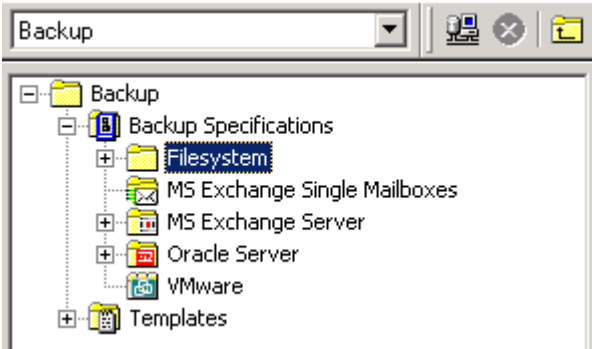


- Por último, se debe dar clic en finalizar.
- Al finalizar la importación del host, éste aparecerá en la lista con los demás host configurados en Data protector.

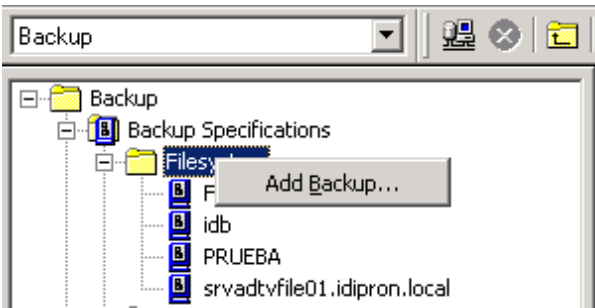
	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	15 de 24
		VIGENTE DESDE	04/10/2022



- Posteriormente en data protector se debe buscar la opción llamada Backup-Filesystem



- Se debe dar clic derecho, para seleccionar una opción llamada Add Backup



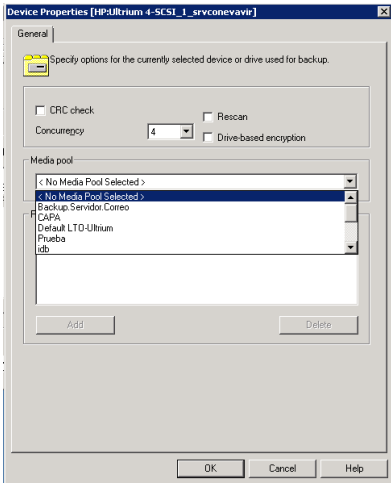
- En la siguiente imagen se muestra las diferentes plantillas para creación de un backup, para filesystem se debe seleccionar la primera, después clic en OK.

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	17 de 24
		VIGENTE DESDE	04/10/2022

- Luego se debe seleccionar la librería y el drive al cual va a utilizar el backup nuevo.



- Después se habilitará una opción que está al otro costado llamada PROPERTIES esta nos indicará en qué pool de cintas va asignado este backup, ya que, si no se selecciona ninguno, el backup cuando se vaya a ejecutar quedará en “mount request” solicitando cinta.

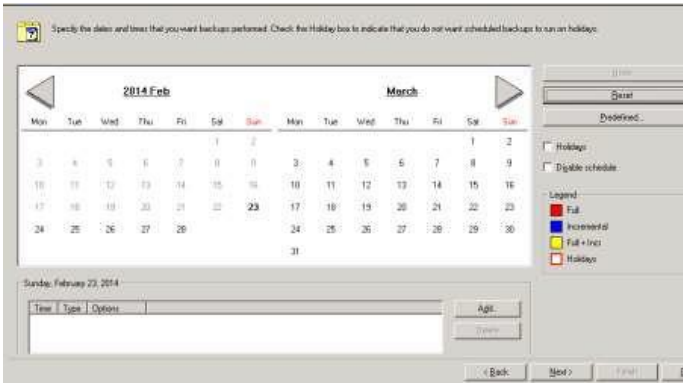


- Luego de dar clic en NEXT mostrará otra ventana para poder cambiar configuraciones avanzadas, se selecciona la opción NEXT.

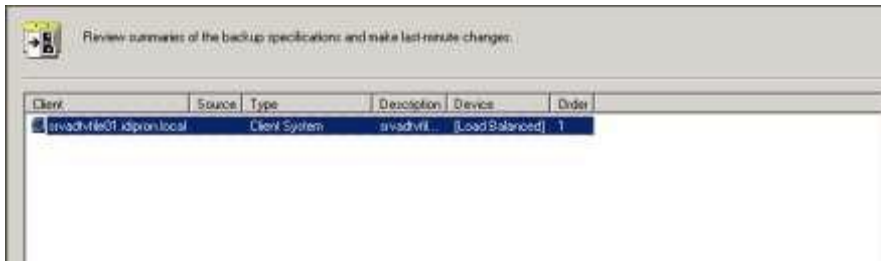


- Por último, se muestra la ventana en donde ingresaremos la calendarización de backup; hora, fecha, días.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. INTEGRACIÓN SOCIAL Instituto Oriental para la Protección de la Niñez y la Juventud	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	18 de 24
		VIGENTE DESDE	04/10/2022



- Para adicionar un horario al backup nuevo, se debe dirigir a la opción que dice Add, acá aparecerá un recuadro donde se debe suministrar el horario que se desee.
- Por último, se mostrará un resumen de los parámetros indicados previamente.



- Luego se debe asignar un nombre al backup nuevo.



10. PROCESO DE RESTAURACIÓN

Los jefes o los responsables de la Secretaria General, Subdirecciones, las oficinas, áreas o dependencias son los únicos autorizados para solicitar la recuperación de la información ante un incidente, pérdida total o parcial siempre y cuando este en el inventario de copia respaldo o haya solicitado una copia previa.

La solicitud para restauración de copias de respaldo debe hacerse a través del software de mesa de ayuda que dispone la Entidad. La cual se atenderá de acuerdo con los acuerdos de nivel de servicio establecidos en la mesa de ayuda, con la finalidad de dar trámite para solicitar los medios magnéticos o cintas al custodio de los mismos.

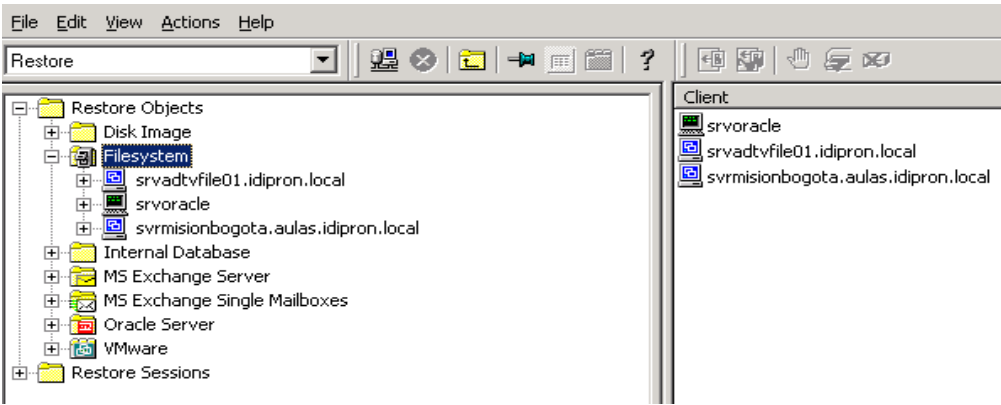
Al finalizar el procedimiento, el administrador de copias de respaldo debe devolver el medio magnético o la cinta al custodio.

Para llevar a cabo la restauración de la información almacenada en una cinta LTO, se deben realizar los siguientes pasos:

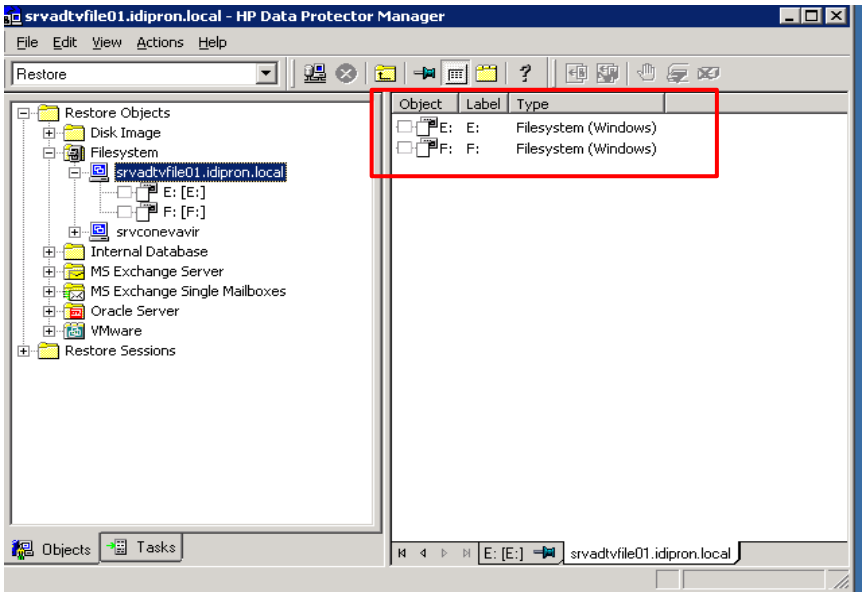
- Para restaurar la información alojada en una cinta, se debe colocar la cinta en el hardware de la librería de cintas, y abrir el software administrador de backup, elegir la opción “Device & Media”, seleccionar “Slots” ubicar un slot libre o disponible, dar clic derecho y seleccionar la opción “Enter”.

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	19 de 24
		VIGENTE DESDE	04/10/2022

- Posteriormente se debe seleccionar la cinta, en el slot indicado aparecerá con un signo de interrogación y luego se debe dar clic derecho y seleccionar la opción “Import Catalog...”
- Para poder restaurar un archivo o una carpeta en específico, se ingresa primero a la opción que se llama RESTORE.

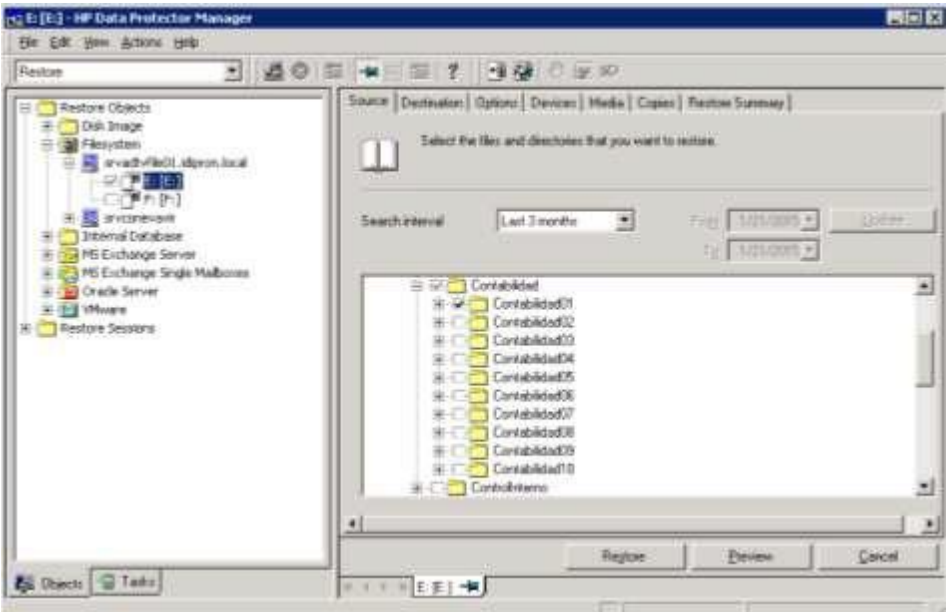


- Luego se debe seleccionar el servidor donde está almacenado el Archivo o la carpeta que se va a recuperar, se selecciona la opción señalada como se muestra en la siguiente imagen. En la parte derecha de la ventana se pueden ver los servidores que cuentan con el backup, luego se selecciona el host de origen de la información y se da doble clic.

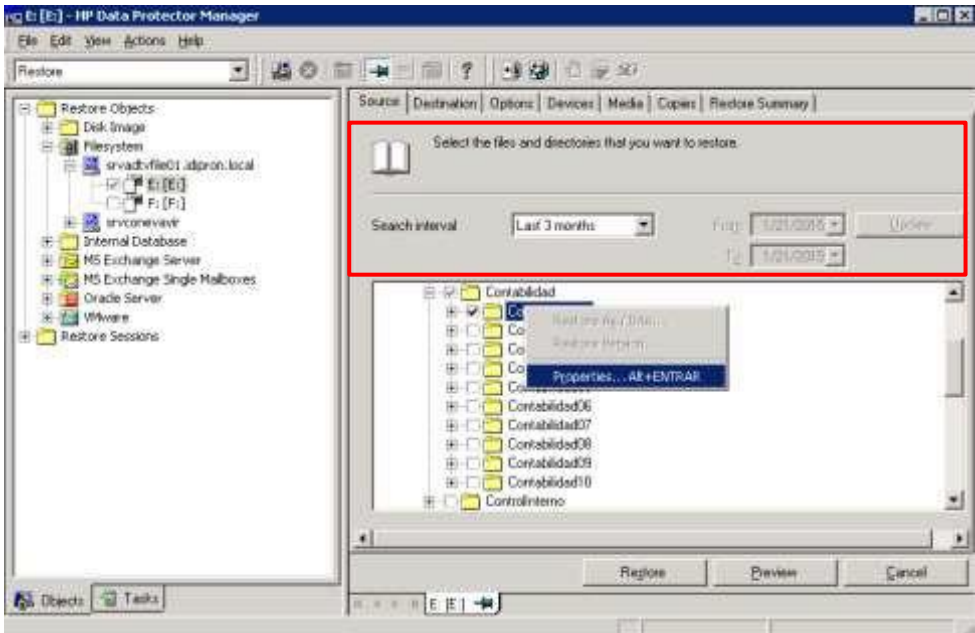


- Aparecen las unidades a las cuales se realizó la copia, es decir están habilitadas las unidades “E” y “F”, se debe seleccionar la unidad que posee la información que queremos restaurar.
- En la siguiente imagen se muestra la carpeta de la unidad E y la subcarpeta llamada Contabilidad01.

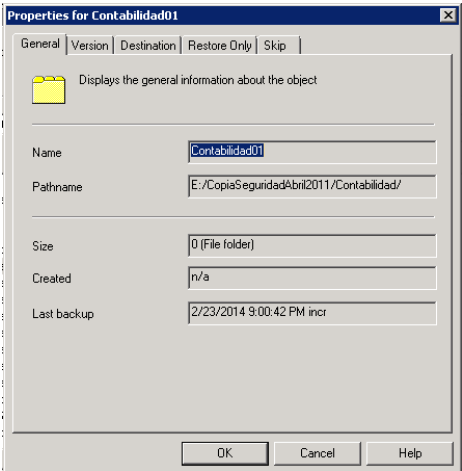
	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	20 de 24
		VIGENTE DESDE	04/10/2022



- En la siguiente imagen en el recuadro en rojo, se puede seleccionar el intervalo de tiempo para realizar la restauración (en este caso los últimos 3 meses), o también especificando un intervalo desde una fecha inicial a una fecha final.

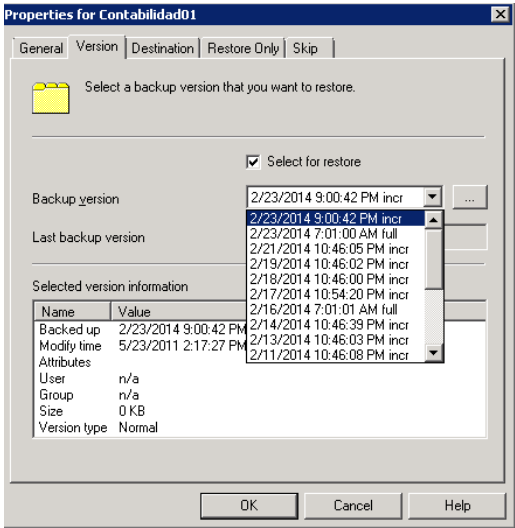


- Se debe dar clic derecho a la carpeta indicada y vamos a la opción llamada PROPERTIES.

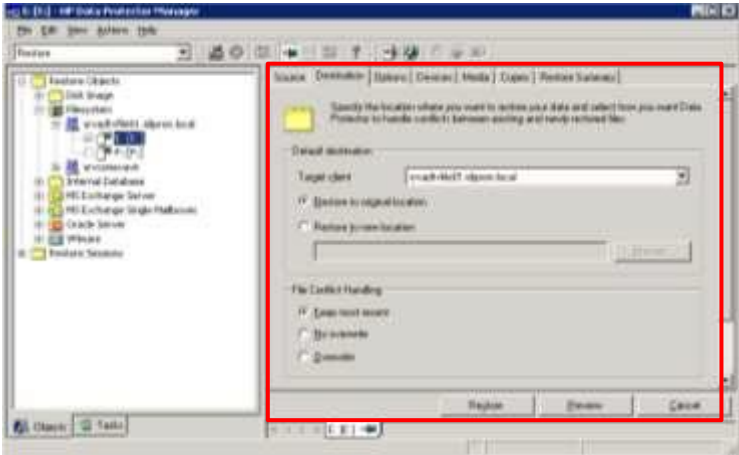


	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	21 de 24
		VIGENTE DESDE	04/10/2022

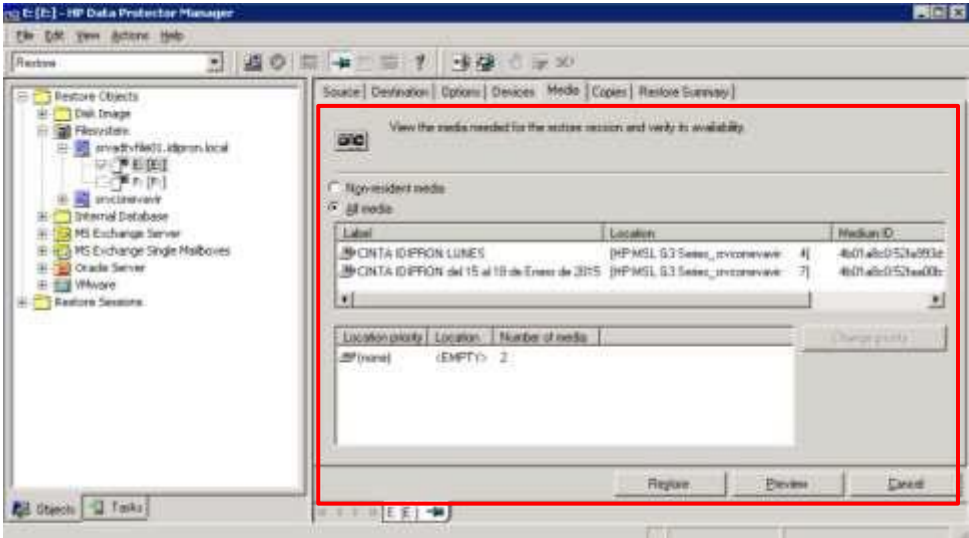
- Luego se debe seleccionar una de las siguientes opciones del menú desplegable, donde se elige el tipo de “Version del Backup” – seleccionando la fecha de restauración y el tipo del backup, bien sea si se realizó en forma incremental o full.



- Luego de Indicada la fecha que quiere restaurar, se debe dar clic en la pestaña DESTINATION en el menú desplegable de la opción Target client, allí se debe seleccionar la ubicación a donde se quiere restaurar la información. Existen dos opciones más: “Restore to original location” la cual sirve para que el backup quede en la misma ubicación y “Restore to new location” permite seleccionar una ubicación diferente para realizar la restauración de la copia.
- También se puede seleccionar que se sobrescriba en una ubicación existente o dejar una copia más reciente para no afectar si existe una con el mismo nombre.

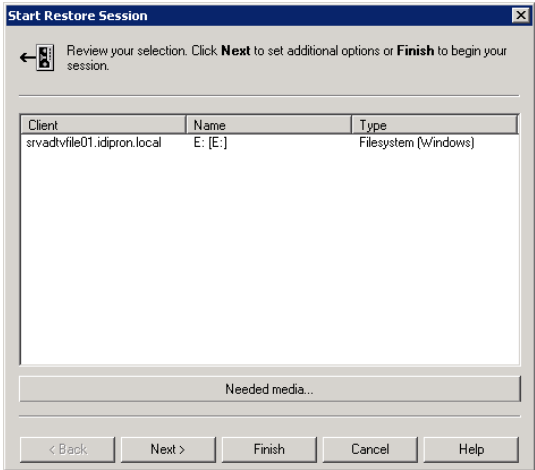


- En la pestaña “Media” se debe asegurar que las cintas se encuentren dentro de la librería para poder realizar el respaldo sin ningún inconveniente. Allí se muestra las cintas que contiene el backup para restaurar.



	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	22 de 24
		VIGENTE DESDE	04/10/2022

- Luego se debe seleccionar la opción restore ubicada en la parte de inferior de la ventana y posteriormente se debe dar clic en la opción Finish.



- Por último, se debe constatar que la restauración se haya realizado satisfactoriamente, en la ruta seleccionada para su restauración.

Nota: en caso de que la información a ser restaurada, no se encuentre en las cintas dentro de la librería del Dataprotector, se debe solicitar la cinta donde se encuentre custodiada para su posterior revisión.

11. PRUEBAS DE RESTAURACIÓN

La Oficina de Tecnologías de la Información y las Comunicaciones realizará pruebas de restauración de las cintas cada seis (6) meses, con la finalidad de dar cumplimiento a la etapa del plan de recuperación de desastres. Para dichas pruebas se tomarán cintas en forma aleatoria.

Nota: las pruebas de restauración se harán a las cintas que han cumplido la periodicidad estipulada y/o por designación específica del área.

12. ENVÍO DE CINTA A CUSTODIA

El administrador de copias de respaldo envía la(s) Cinta(s) generada (s) a custodia dentro de los de los 7 primeros días hábiles del mes siguiente. Este procedimiento se hace de acuerdo al proceso con que cuenta la Entidad para custodia de medios.

13. ETIQUETADO DE LA CINTA

Una vez la cinta se va a enviar a custodia, se debe etiquetar de la siguiente manera:

IDENTIFICADOR CINTA (Ejemplo)	DESCRIPCIÓN
012020_IDI_BD	Los 2 primeros dígitos especifican el mes. Los 4 siguientes dígitos especifican el año. Los caracteres IDI especifican las 3 iniciales de Idipron. Los últimos caracteres especifican el origen de la información, en este caso BD = Base de Datos
012020_IDI_MVF	Los 2 primeros dígitos especifican el mes. Los 4 siguientes dígitos especifican el año. Los caracteres IDI especifican las 3 iniciales de Idipron. Los últimos caracteres especifican el origen de la información, en este caso MVF = Máquinas virtuales y físicas.

Cuadro No. 2. Etiquetado de la cinta

	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	23 de 24
		VIGENTE DESDE	04/10/2022

Nota: En el formato de bitácora de backup se describe el contenido de la cinta.

14. PLAN DE COPIAS DE LA INFORMACIÓN

Se contará con un plan de copias de seguridad, de acuerdo con el siguiente esquema:

Backup Full: es un backup de la información que contiene la totalidad de los archivos seleccionados.

Backup Incremental: es una copia de respaldo de la información creada o modificada después de la última copia full (completa); en caso de ser necesaria una restauración de dicha información, se debe tener el última backup full y todas las copias incrementales, tomadas hasta la fecha.

15. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA (DD/MM/AAAA)	ELABORÓ
01	Se crea el Manual para Manejo de la Aplicación de Respaldos Data Protector y Políticas de Resguardo.	23/02/2015	Carlos Alberto Celis Técnico Operativo Luis Albeiro Cortés Profesional Universitario Geovanny Melgarejo Profesional Universitario
02	<ul style="list-style-type: none">- Se modifica el paso N° 2 del numeral 3.6, adicionando los servidores de Oracle y Misión Bogotá, para el monitoreo de backup y operación de backup diario. Se complementa la explicación de diferencial y full en la toma de backups en el servidor de archivos. Se adiciona la operación de backups bajo el pool “Pool_BD_Oracle_Fin_Semana”.- Se modifica el numeral 3.7 por “Restauración de Archivos”.- Se adiciona dentro del numeral 3.7 la nota que hace referencia a la restauración de la información.- Se adiciona el numeral 3.8 en cuanto a Pruebas de Restauración con sus respectivas gráficas y pasos explicativos.- Se modifica el numeral 3.11, en cuanto a Políticas de Respaldo, adicionando los servidores de Oracle y Misión Bogotá	08/03/2016	Carlos Alberto Celis Técnico Operativo Geovanny Melgarejo Profesional Universitario
03	Para la presente versión el manual se actualizó a la plantilla vigente de manual	22/04/2019	Sandra Lucia Badlissi Tajan Profesional Área de Sistemas

 ALCALDÍA MAYOR DE BOGOTÁ D.C. INTEGRACIÓN SOCIAL Instituto Distrital para la Protección de la Niñez y la Juventud	GESTION DE TICS	CÓDIGO	E-GTIC-MA-03
		VERSIÓN	05
	POLÍTICAS DE COPIA DE SEGURIDAD, RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN DIGITAL	PÁGINA	24 de 24
		VIGENTE DESDE	04/10/2022

04	<p>Se modifica el documento de acuerdo con los siguiente:</p> <ul style="list-style-type: none">- Se migra el documento al formato documento interno.- Se modifica el nombre del documento.- Se incluyen objetivos específicos.- Se incluye la información de la arquitectura con que cuenta la Entidad para realizar el proceso de copia de respaldo de información.- Se incluye el inventario de la información a la que se le realiza backup y su periodicidad.- Se incluye la descripción del etiquetado de la cinta de backup.	16/11/2021	<p>Carlos Alberto Celis Profesional Universitario</p> <p>Oralia Franco Góez Profesional – Contratista</p>
05	<ol style="list-style-type: none">1. Se realiza la actualización de las áreas / dependencias y cargos mencionados en el documento con el fin de dar cumplimiento a lo establecido en el Acuerdo “Por el cual se modifica la Estructura Organizacional del INSTITUTO DISTRITAL PARA LA PROTECCIÓN DE LA NIÑEZ Y LA JUVENTUD IDIPRON, se establecen las funciones de sus dependencias y se dictan otras disposiciones”2. Se realiza el ajuste de la codificación de los formatos y documentos mencionados en el procedimiento (manual, documento interno o instructivo), de acuerdo con los ajustes realizados a los códigos de los documentos del Sistema Integrado de Gestión producto del rediseño institucional.3. Se realiza cambio de código del documento del A-TIC-MA-005 al código E-GTIC-MA-003	04/10/2022	<p>MARISOL MONSALVE USME PROFESIONAL OFICINA ASESORA DE PLANEACIÓN</p>

16. REVISIÓN Y APROBACIÓN

	NOMBRE	CARGO	FECHA (DD/MM/AAAA)
REVISÓ	VIVIANA ANDREA SANCHEZ MORALES	PROFESIONAL OFICINA ASESORA DE PLANEACIÓN	04/10/2022
APROBACIÓN LÍDER DE PROCESO	FABIAN ANDRÉS CORREA ÁLVAREZ	JEFE OFICINA ASESORA DE PLANEACIÓN	04/10/2022