



Resolución Directoral Regional

Nº 0990 -2023-DRELM

Lima, 20 Jul. 2023

VISTOS: El expediente N.º 0019942-2023-DRELM, el Informe N.º 0089-2023-MINEDU/VMGI-DRELM-OPP-ETI, el Informe N.º 0098-2023-MINEDU/VMGI-DRELM-OPP-ERMC, el Informe N.º 606-2023-MINEDU/VMGI-DRELM-OAJ-EGSA, y demás documentos que se adjuntan;

CONSIDERANDO:

Que, la Ley N.º 27658, Ley Marco de Modernización de la Gestión del Estado, declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano;

Que, el artículo 1 del Decreto Legislativo N.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, dispone que la referida ley tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como, el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la administración pública;

Que, el numeral 109.1 del artículo 109 del Decreto Supremo N.º 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N.º 1412, modificado por el Decreto Supremo N.º 075-2023-PCM¹, establece que: «El Sistema de Gestión de Seguridad de la Información (SGSI) comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación.»;

VISADO POR: LI QUISPE Juan
Carlos FAU 20330611023 hard
Motivo: Firma Digital
Fecha: 19/07/2023 14:09:17 -
0500

VISADO POR: FLORES PASTOR
Marcela Edith FAU 20330611023
soft
Motivo: Firma Digital
Fecha: 18/07/2023 17:01:50 -0500

¹ Decreto Supremo que modifica el Reglamento del Decreto Legislativo N.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, aprobado mediante el Decreto Supremo N.º 029-2021-PCM.

Código : 180723432
Clave : 2811



Que, mediante la Resolución Ministerial N° 004-2016-PCM se aprueba el uso obligatorio de la Norma Técnica Peruana «NTP 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.2ª Edición», en todas las entidades integrantes del Sistema Nacional de Informática, con el objeto de especificar los requisitos para establecer implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información; asimismo, incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información;

Que, mediante la Resolución de Secretaría General N° 148-2021-MINEDU, se aprueba la «Directiva para la Gestión de la Seguridad de la Información del Ministerio de Educación», la cual tiene como objetivo establecer lineamientos de seguridad de la información institucional para contribuir al logro de los objetivos estratégicos del Ministerio de Educación;

Que, a través de la Resolución Ministerial N° 180-2022-MINEDU se aprueba la «Política General de Seguridad de la Información en el Ministerio de Educación», la cual establece como uno de sus objetivos garantizar la confidencialidad, integridad y disponibilidad de la información para contribuir al logro de los objetivos estratégicos, mediante la implementación de controles de seguridad de la información;

Que, mediante Resolución de Secretaría General N.° 101-2022-MINEDU, de fecha 16 de junio de 2022, se resuelve derogar la Resolución de Secretaría General N.° 073-2019-MINEDU que aprueba la Directiva N° 005-2019-MINEDU/SPE-OPEP-UNOME denominada «Elaboración, aprobación y derogación de actos resolutiveos, así como elaboración y modificación de documentos de gestión, normativos y orientadores del Ministerio de Educación»; asimismo, derogar el artículo 1 de la Resolución de Secretaría General N.° 090-2020-MINEDU, que suspende la aplicación de la Directiva N.° 005-2019-MINEDU/SPE-OPEP-UNOME denominada «Elaboración, aprobación y derogación de actos resolutiveos, así como elaboración y modificación de documentos de gestión, normativos y orientadores del Ministerio de Educación»; y, aprobar la Directiva denominada «Elaboración, Aprobación y Tramitación de Actos Resolutiveos y Documentos Normativos del Ministerio de Educación»;

Que, el sub numeral 5.7 del numeral 5 de la mencionada Directiva establece que los órganos desconcentrados, programas o proyectos deben seguir las disposiciones emitidas en dicha Directiva, sin perjuicio que puedan establecer una ruta interna para la validación de sus propuestas de documentos normativos²;

Que, la precitada Directiva define a los Manuales como el documento que explica de forma ordenada y sistemática, una materia con relación a aspectos educativos o de gestión, a fin de aclarar, entender o verificar una actividad o procedimiento. Además,

² Numeral 7 de la Directiva

Son aquellos documentos que tienen por objeto regular el cumplimiento de las funciones y disposiciones normativas sobre aspectos operativos o administrativos en los órganos, unidades orgánicas, órganos desconcentrados, programas y proyectos del MINEDU, así como de las demás instancias de gestión educativa descentralizada, cuando corresponda. Los documentos normativos en el MINEDU se clasifican en:

- Lineamiento
- Norma Técnica
- Directiva
- **Manual**

Código : 180723432
Clave : 2811



estos pueden ser elaborados por todos los órganos, unidades orgánicas y programas del MINEDU y propuesto para su aprobación por los órganos competentes en la materia, siempre y cuando se sustente en una norma previamente aprobada. Su ámbito de aplicación es nacional o institucional y se aprueba, entre otros, con Resolución Directoral;

Que, asimismo, el sub numeral 11.3 del numeral 11 de la Directiva señala que el expediente deberá contar con la opinión favorable de la Oficina de Planeamiento y Organización y la Oficina de Asesoría Jurídica o las que hagan sus veces;

Que, en ese sentido, el Responsable del Equipo de Tecnologías de la Información mediante Informe N° 0078-2023-MINEDU-VMGI/DRELM-OPP-ETI, de fecha 22 de mayo de 2023, señala que el Equipo de Tecnologías de Información de la DRELM no cuenta con un manual sobre el estado situacional de las copias de seguridad (backups) de la DRELM, con la finalidad de que los datos estén protegidos y se puedan restaurar en caso de fallos o pérdidas de datos; por lo que, formula el proyecto de manual respectivo;

Que, la Oficina de Asesoría Jurídica a través del Memorándum N° 479-2023-MINEDU/VMGI-DRELM-OAJ-EGSA, de fecha 7 de junio de 2023, formuló observaciones al proyecto de manual, solicitando se subsane lo observado a fin de continuar con el trámite de aprobación de dicho manual;

Que, mediante Informe N° 0089-2023-MINEDU-VMGI/DRELM-OPP-ETI, de fecha 13 de junio de 2023, el Responsable del Equipo de Tecnologías de la Información, subsana las observaciones y formula el proyecto denominado «Manual de Generación de Copias de Seguridad (Backups) de la Dirección Regional de Educación de Lima Metropolitana», señalando que el manual garantizará que se sigan los procedimientos adecuados para respaldar los datos y prevenir la pérdida de información valiosa y aseguraría el cumplimiento de normativas y regulaciones relacionadas con la protección de datos y la gestión de la información; de otro lado, precisa que, las copias de seguridad son esenciales para garantizar la continuidad del servicio en caso de fallos técnicos, desastres naturales u otros incidentes imprevistos; asimismo, es una medida efectiva para proteger los datos de la DRELM contra ataques de ransomware, malware u otras formas de ciberataques;

Que, por medio de los Informes N.º 0092 y 098-2023-MINEDU/VMGI-DRELM-OPP-ERMC, de fechas 30 de mayo y 15 de junio de 2023, respectivamente, la Oficina de Planificación y Presupuesto emite opinión favorable al proyecto denominado «Manual de Generación de Copias de Seguridad (Backups) de la Dirección Regional de Educación de Lima Metropolitana»;

Que, mediante Informe N.º 606-2023-MINEDU/VMGI-DRELM-OAJ-EGSA, de fecha 6 de julio de 2023, la Oficina de Asesoría Jurídica concluye que se debe aprobar el «Manual de Generación de Copias de Seguridad (Backups) de la Dirección Regional de Educación de Lima Metropolitana»; conforme a la propuesta del órgano técnico;

Que, conforme a la facultad establecida en el literal k) del artículo 8 del Manual de Operaciones de la Dirección Regional de Educación de Lima Metropolitana, aprobado por Resolución Ministerial N.º 215-2015-MINEDU y su modificatoria, corresponde emitir el acto resolutivo correspondiente;

Código : 180723432
Clave : 2811



Contando con el visado de la Oficina de Planificación y Presupuesto y la Oficina de Asesoría Jurídica, y de conformidad con el Manual de Operaciones de la Dirección Regional de Educación de Lima Metropolitana, aprobado por Resolución Ministerial N.º 215-2015-MINEDU y su modificatoria;

SE RESUELVE:

ARTÍCULO 1.- APROBAR el «Manual de Generación de Copias de Seguridad (Backups) de la Dirección Regional de Educación de Lima Metropolitana», el mismo que como anexo forma parte integrante de la presente resolución.

ARTÍCULO 2.- DISPONER que el Equipo de Atención al Usuario y Gestión Documentaria de la Oficina de Atención al Usuario y Comunicaciones de esta sede regional notifique la presente resolución a todas las oficinas y unidades de la DRELM, conforme a ley.

ARTÍCULO 3.- DISPONER la publicación de la presente resolución en el Portal de la Dirección Regional de Educación de Lima Metropolitana: www.dreilm.gob.pe para su difusión correspondiente.

ARTÍCULO 4.- DISPONER que el Equipo de Archivo Documentario de la Oficina de Atención al Usuario y Comunicaciones de esta sede regional, archive los actuados adjuntos en el modo y forma de ley.

Regístrese y Comuníquese,

Documento firmado digitalmente

LUIS ALBERTO QUINTANILLA GUTIÉRREZ
Director Regional de Educación
de Lima Metropolitana

LAQG/D.DRELM
MEFP/J.OAJ
WJGM/C.OAJ
KJTG/Abg.OAJ

Código : 180723432
Clave : 2811



MANUAL DE GENERACIÓN DE COPIAS DE SEGURIDAD (BACKUPS) DE LA DIRECCION REGIONAL DE EDUCACION DE LIMA METROPOLITANA

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autoría de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

Resolución de Aprobación			
Resolución Directoral N°		-2023-DRELM	
Código	Versión	Páginas	Fecha de aprobación
MA-00X-02-DRELM	01		

Código : 110723145
Clave : 6289

VISADO POR: LI QUISPE Juan
Carlos FAU 20330611023 hard
Motivo: Firma Digital
Fecha: 11/07/2023 14:07:55 -
0500

FIRMADO POR: FLORES
PASTOR Marcela Edith FAU
20330611023 hard
Motivo: Firma Digital
Fecha: 11/07/2023 11:42:56 -0500





PERÚ

Ministerio de Educación

DOCUMENTO NORMATIVO

Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana

Código

MA-00X-02-DRELM


Control de Cambios

Versión	Sección / Ítem	Descripción del cambio:
01	----	Nuevo

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autografía de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

Código : 110723145
Clave : 6289



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
--	--	---------------------------

ESTADO FORMAL:

Nombre:	Elaborado por: (Cargo): Especialista en Sistemas e Informática - Gerry Ax'l Vera Suasnábar	Revisado por: (Cargo): Responsable del Equipo de Tecnologías de la Información - Julio Jesús Tello Barron
Fecha:	22/05/2023	22/05/2023

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autoría de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

Código : 110723145
Clave : 6289





PERÚ

Ministerio de Educación

DOCUMENTO NORMATIVO

Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana

Código

MA-00X-02-DRELM


ÍNDICE

1. Objetivo	4
2. Ámbito de Aplicación	4
3. Base Normativa	4
4. Definiciones	4
5. Contenido	
5.1 Estrategias de rotación de soportes de cinta	7
5.2 Configuración DRELM	10
5.3 Procedimientos para el cambio de cintas mediante panel y consola web	11
5.4 Interfaz de gestión remota (RMI)	12
5.5 Status Visualización de la información dinámica del dispositivo	13
5.6 Visualización de la información dinámica de la unidad	14
5.7 Cambio de la configuración del sistema	14
5.8 Cambio de la configuración de la unidad	16
5.9 Procedimientos para la limpieza de drive	16
5.10 Inventario de cintas	18
5.11 Protección contra escritura de los cartuchos de cinta	19
5.12 Compatibilidad con lectura retroactiva	21
5.13 Cargadores (autoloaders)	21
5.14 Traslado de soportes	22
5.15 Actualización del inventario actual de soportes	23
5.16 Liberación y sustitución de cargadores	23
5.17 Visualización del inventario del cartucho de cinta	24
5.18 Visualización del inventario del cartucho de cinta Panel LCD	25
5.19 Inventario actual de cintas Backup disponibles	26
5.20 Inventario de servidores y sistemas respaldados	26
5.21 Servidores virtuales respaldados diariamente con apoyo de la herramienta VMWARE	37
5.22 Formato de registro de reporte de sistemas de información con copias de respaldo	40
5.23 Pruebas de restauración de copias de seguridad	41

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autoría de la(s) firma(s) pueden ser verificadas en: <https://apps.firma.peru.gob.pe/web/validador.xhtml>.

Código : 110723145
Clave : 6289



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
--	--	---------------------------

1. Objetivo

El objetivo principal del manual es proporcionar información sobre el estado de las copias de seguridad de la Dirección Regional de Educación de Lima Metropolitana (DRELM) y los procedimientos adecuados para realizar copias de seguridad, supervisar su estado y garantizar su integridad. Tiene como propósito identificar los sistemas de información que están siendo respaldados y que estos estén protegidos; y que a su vez se puedan restaurar adecuadamente en caso de fallos o pérdidas de datos.

2. Ámbito de Aplicación


El presente manual es de observancia para la Dirección Regional de Educación de Lima Metropolitana.

3. Base Normativa

- Ley N° 29733, Ley de Protección de Datos Personales.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.
- Decreto Supremo N° 001-2015-MINEDU, que aprueba el Reglamento de Organización y Funciones del Ministerio de Educación.
- Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Decreto Supremo N° 075-2023-PCM, Decreto Supremo que modifica el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, aprobado mediante el Decreto Supremo N° 029-2021-PCM.
- Resolución Ministerial N.º 215-2015-MINEDU y su modificatoria, que aprueba el Manual de Operaciones de la Dirección Regional de Educación de Lima Metropolitana.
- Resolución Ministerial N° 180-2022-MINEDU que aprueba la “Política General de Seguridad de la Información en el Ministerio de Educación”.
- Resolución Ministerial N° 004-2016-PCM que aprueban el uso obligatorio de la Norma Técnica Peruana “NTP 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos”. 2ª. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática
- Resolución de Secretaría General N° 148-2021-MINEDU que aprueba la “Directiva para la Gestión de la Seguridad de la Información del Ministerio de Educación”.
- Resolución de Secretaría General N° 028-2019-MINEDU que aprueba la Directiva N° 003-2019-MINEDU/SPE-OTC denominada “VERIFICACIÓN Y VALIDACIÓN DE PRODUCTO SOFTWARE DE DESARROLLO EXTERNO”.
- Resolución de Secretaría General N.º 101-2022-MINEDU, de fecha 16 de junio de 2022, se resuelve derogar la Resolución de Secretaría General N.º 005-2019-MINEDU/SPE-

Código : 110723145
Clave : 6289



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
--	--	---------------------------

OPEP-UNOME denominada «Elaboración, aprobación y derogación de actos resolutiveos, así como elaboración y modificación de documentos de gestión, normativos y orientadores del Ministerio de Educación»; asimismo, derogar el artículo 1 de la Resolución de Secretaría General N.º 090-2020-MINEDU, que suspende la aplicación de la Directiva N.º 005-2019-MINEDU/SPE-OPEP-UNOME denominada “Elaboración, aprobación y derogación de actos resolutiveos, así como elaboración y modificación de documentos de gestión, normativos y orientadores del Ministerio de Educación”; y, aprobar la Directiva denominada “Elaboración, Aprobación y Tramitación de Actos Resolutiveos y Documentos Normativos del Ministerio de Educación”.


4. Definiciones

- **RMI (Remote Method Invocation):** es un mecanismo que permite realizar llamadas a métodos de objetos remotos situados en distintas (o la misma) máquinas virtuales Java.
- **Panel de control del operador (OCP):** esta interfaz permite utilizar el dispositivo desde el panel frontal.
- **Cinta/Cartucho magnética y/o soporte magnético:** es un medio de almacenamiento de información que utiliza una cinta recubierta de material magnético para registrar datos de forma secuencial.
- **Copia Completa / Full Backup:** es un tipo de respaldo de datos en el que se realiza una copia completa de todos los archivos y datos de un sistema o dispositivo. En este tipo de respaldo, se copian todos los archivos y carpetas seleccionados, sin importar si han cambiado desde la última copia de seguridad o no.
- **Copia Incremental:** es un tipo de copia de seguridad que solo guarda los archivos que han cambiado o han sido modificados desde el último respaldo realizado.
- **Copia diferencial:** es un tipo de copia de seguridad que guarda todos los archivos que han sido modificados o agregados desde el último respaldo completo. A diferencia de una copia incremental, que solo guarda los archivos modificados desde el último respaldo, una copia diferencial guarda todos los archivos modificados desde el último respaldo completo.
- **Autocargador:** es un dispositivo de almacenamiento diseñado para gestionar y automatizar el respaldo y la recuperación de datos en cintas magnéticas.
- **Cargadores:** son los mecanismos o compartimentos que albergan las cintas de respaldo en el dispositivo. Estos cargadores están diseñados para cargar y descargar automáticamente las cintas en las unidades de lectura/escritura del autocargador.
- **Soporte de medios:** medio físico utilizado para almacenar y proteger los datos respaldados por el software, como cintas magnéticas, discos duros u otros dispositivos de almacenamiento.
- **VMWARE:** es una tecnología que permite ejecutar múltiples sistemas operativos y aplicaciones en un solo servidor físico mediante el uso de máquinas virtuales.
- **SNAPSHOT:** es una función que permite capturar el estado y los datos de una máquina virtual (VM) en un momento específico. Un snapshot es una "foto" instantánea del estado de la VM, incluyendo la memoria, el almacenamiento y la configuración en ese momento.
- **Activo de Información:** Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autoría de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

Código : 110723145
Clave : 6289



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
--	--	---------------------------

- **Acceso:** En la lectura o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta una base de datos, los datos son primero accedidos y suministrados a la computadora y luego transmitidos a la pantalla del equipo.
- **Incidente:** Cuando se produce un ataque o se materializa una amenaza se tiene un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de eliminación de un archivo protegido.
- **Integridad:** Los valores consignados en los datos se han de mantener de tal manera que representen la realidad y su modificación debe ser registrada en bitácoras del sistema que permitan la auditoría de los acontecimientos. Las técnicas de integridad sirven para prevenir el ingreso de valores errados en los datos sea esta situación provocada por el software de la Base de Datos, por fallas de los programas, del sistema, el hardware o, simplemente, por errores humanos.
- **Privacidad:** Se define como el derecho que tiene la DRELM para determinar, a quién, cuándo y qué información de su propiedad podrá ser difundida o transmitida a terceros, en concordancia con la Ley N.º 27806, Ley de Transparencia y Acceso a la Información Pública, y demás normas conexas.
- **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o entidades no autorizados.
- **Datos Personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.
- **Sistemas de Información:** Conjunto de elementos relacionados entre sí con un objetivo en común, en el cual se almacenan datos y se genera información relacionada a un tema en particular, para ponerlos a disposición de sus usuarios. Pueden ser registros simples como archivos de Word/Excel, o pueden ser complejos como una aplicación de software con base de datos.
- **Datos:** En general se consideran datos a todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (base de datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colección de bits.
- **Centro de Datos:** El centro de datos, es un centro de procesamiento para obtener información, en el cual se albergan los sistemas de información, hardware, componentes asociados, como telecomunicaciones y sistemas de almacenamiento.
- **DRELM:** Dirección Regional de Educación de Lima Metropolitana

5. Contenido

Contenido General

La Dirección Regional de Educación de Lima Metropolitana (DRELM) actualmente cuenta con un sistema de respaldo de los sistemas de información, los cuales son almacenados en cintas magnéticas a través de un autocargador de cintas con su respectivo software de Backup.

Las copias de seguridad nos ayudarán a responder de manera rápida y eficaz ante un incidente de seguridad y a que podamos restablecer las actividades de la entidad lo antes posible, intentando reducir así el impacto. Ante la posibilidad de enfrentarnos a pérdidas de información, el presente documento describe el tipo de soporte utilizado, con qué

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autoría de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

Código : 110723145
Clave : 6289



periodicidad y en dónde se aloja la información, asimismo, describe las pruebas periódicas para verificar la integridad y la correcta recuperación de la información.

Revisión y actualización

El presente documento se revisará periódicamente para lograr la efectividad de los procedimientos establecidos, con la finalidad de actualizarlos y modernizarlos, ya que constituye un documento dinámico que puede ser modificado de manera total o parcial cada vez que sea necesario en los siguientes casos:

- Modificación de alguna tarea que signifique cambios en su estructura
- Modificación o derogación de la base legal, que sustenta su elaboración.
- Adecuar las modificatorias al manual si se considera procedente su contenido

Contenido Específico

5.1 Estrategias de rotación de soportes de cinta

Actualmente la DRELM cuenta con 46 cintas magnéticas que son utilizadas para el respaldo de la información, con un periodo de retención de 06 meses, para luego ser rotadas y reutilizadas.

La rotación de las cintas de respaldo de copias de seguridad (Backup) es un aspecto fundamental de todo buen plan de respaldo de datos. Existen varias estrategias de rotación de soportes de cinta que se pueden usar para hacer copias de seguridad de los datos.

Las estrategias de rotación de soportes de cinta más frecuentes son las siguientes:

- Hijo, que usa las mismas cintas cada día para ejecutar una copia de seguridad completa.
- Padre/Hijo, que usa varias cintas e incluye una combinación de copias de seguridad diferenciales o incrementales diarias y completas semanales para una programación de dos semanas. Esta estrategia proporciona las copias de seguridad para el almacenamiento en otra ubicación.
- Abuelo, que usa varias cintas e incluye una combinación de copias de seguridad incrementales o diferenciales diarias y completas semanales y mensuales. Esta estrategia también proporciona las copias de seguridad para el almacenamiento en otra ubicación.

a. Estrategia de rotación de soportes Hijo

La estrategia Hijo consiste en la ejecución de una copia de seguridad completa diaria.

La estrategia de rotación de soportes Hijo necesita lo siguiente:

Tabla: Estrategia de rotación de soportes Hijo

Elemento	Descripción
Número de soportes necesarios	1 (mínimo)





PERÚ

Ministerio de Educación

DOCUMENTO NORMATIVO

Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana

Código

MA-00X-02-DRELM

Período de protección de sobre escritura Última copia de seguridad



Figura 01: Estrategia de copias de seguridad Hijo

Si bien la administración de la estrategia Hijo es sencilla, el proceso de copia de seguridad usando un solo soporte no es un método de copia de seguridad eficaz. Los soportes magnéticos terminan desgastándose después de muchos usos, y los datos de los que se puede hacer copia de seguridad incluyen solo hasta la última copia de seguridad.

b. Estrategia de rotación de soportes Padre/Hijo

La estrategia de rotación de soportes Padre/Hijo necesita lo siguiente:

Tabla: Estrategia de rotación de soportes Padre/Hijo

Elemento	Descripción
Número de soportes necesarios	6 (mínimo)
Período de protección de sobre escritura	Dos semanas

La estrategia de rotación de soportes Padre/Hijo emplea una combinación de copias de seguridad completas y diferenciales o incrementales para una programación de dos semanas.

En este tipo de estrategia, se emplean como mínimo cuatro soportes de lunes a jueves para las copias de seguridad diferenciales o incrementales. Los otros dos soportes, que contienen copias de seguridad completas, se colocan fuera del ciclo y se almacenan en otra ubicación cada viernes.

La estrategia Padre/Hijo es fácil de administrar y le permite conservar los datos por más tiempo que la estrategia Hijo. La estrategia Padre/Hijo no es conveniente para las necesidades de protección rigurosa de datos de la mayoría de los entornos de red.

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autenticidad de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

Código : 110723145
Clave : 6289





PERÚ

Ministerio de Educación

DOCUMENTO NORMATIVO

Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana

Código

MA-00X-02-DRELM

La primera vez que ponga en práctica esta estrategia de copias de seguridad, deberá comenzar por realizar una copia de seguridad completa.

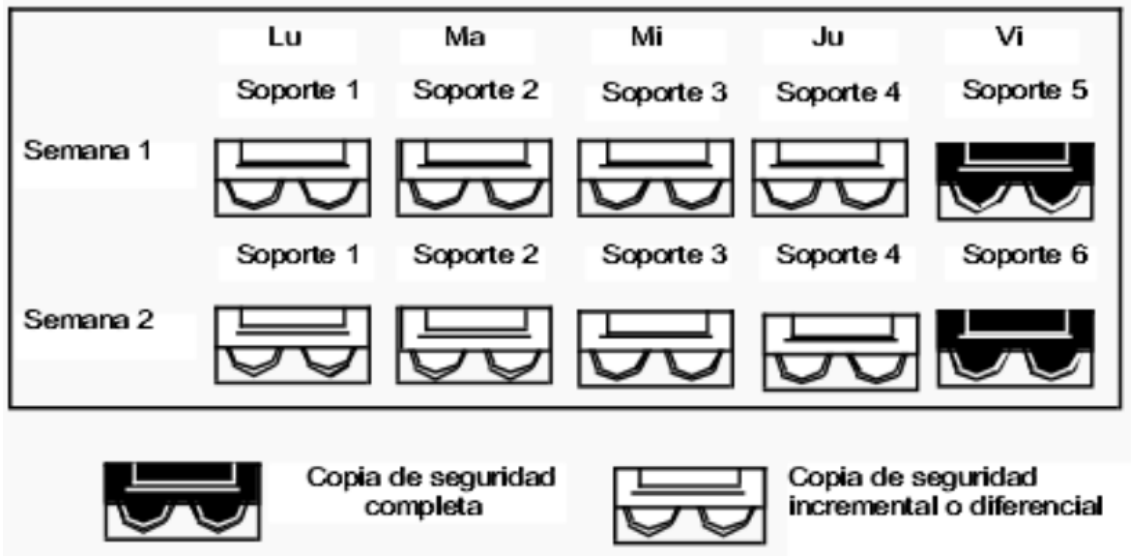


Figura 02: Estrategia de copias de seguridad Padre/Hijo

c. Estrategia de rotación de soportes Abuelo

La estrategia de rotación de soportes Abuelo necesita lo siguiente:

Tabla: Estrategia de rotación de soportes Abuelo

Elemento	Descripción
Número de soportes necesarios	19 (mínimo)
Período de protección de sobre escritura	Un año

El método Abuelo es una de las estrategias de rotación de soportes más comunes. El método Abuelo es fácil de administrar y lo suficientemente completo para permitir la fácil ubicación de archivos cuando se necesitan restaurar.

En este tipo de estrategia, se emplean cuatro cintas de lunes a jueves para copias de seguridad incrementales o diferenciales, y otras tres cintas para copias de seguridad completas cada viernes.

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autoría de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

Código : 110723145
Clave : 6289





PERÚ

Ministerio de Educación

DOCUMENTO NORMATIVO

Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana

Código

MA-00X-02-DRELM

Los 12 soportes restantes se emplean para realizar copias de seguridad completas mensuales y se almacenan en otra ubicación.

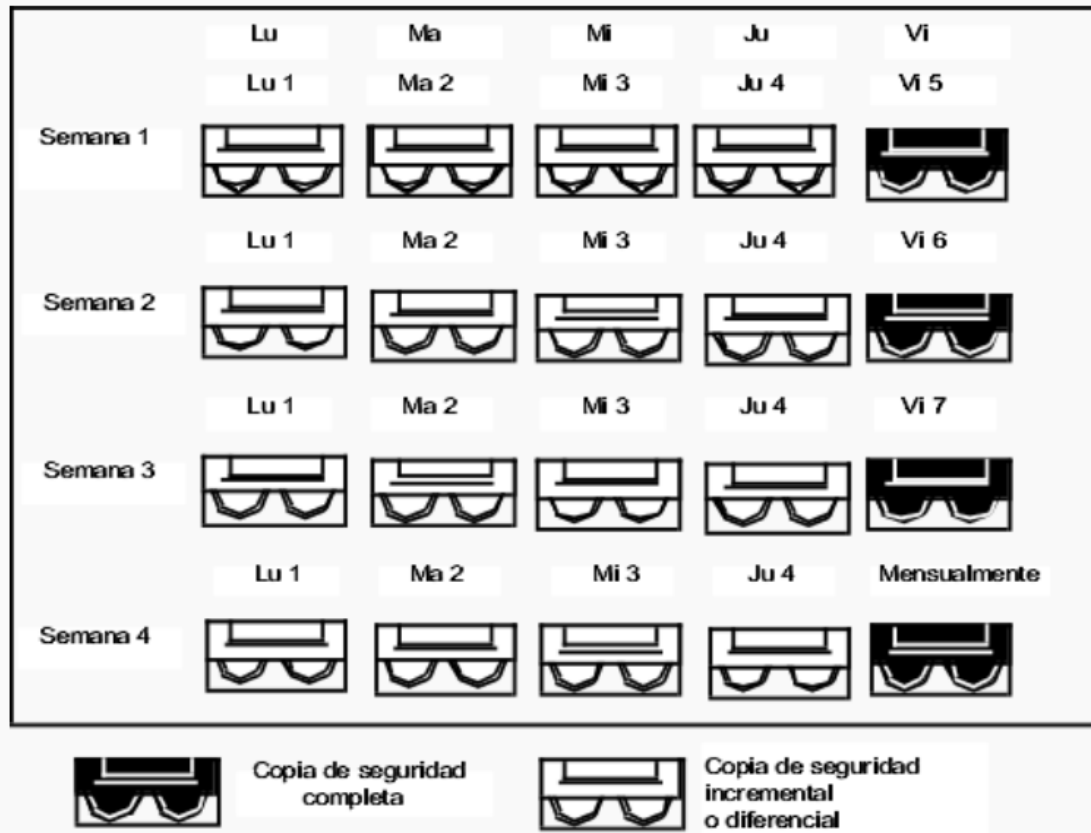


Figura 03: Estrategia de copias de seguridad Abuelo.

Esta estrategia se recomienda porque ofrece una relación óptima entre número de soportes y tiempo de almacenamiento (19 soportes/1 año). Es posible incorporar fácilmente más soportes. Por ejemplo, puede realizar una copia de seguridad completa el último sábado del mes para conservar permanentemente


5.2 Configuración DRELM

La configuración existente en la DRELM está basada en el software Veritas Back-up Exec Versión 21.0 con una configuración Padre/Hijo, con políticas de BackUp incrementales diarios y Full Back Diarios/Mensuales con intercambio de cintas desde un autocargador de cintas de marca HP.

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autoría de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

Código : 110723145
Clave : 6289



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
--	--	---------------------------

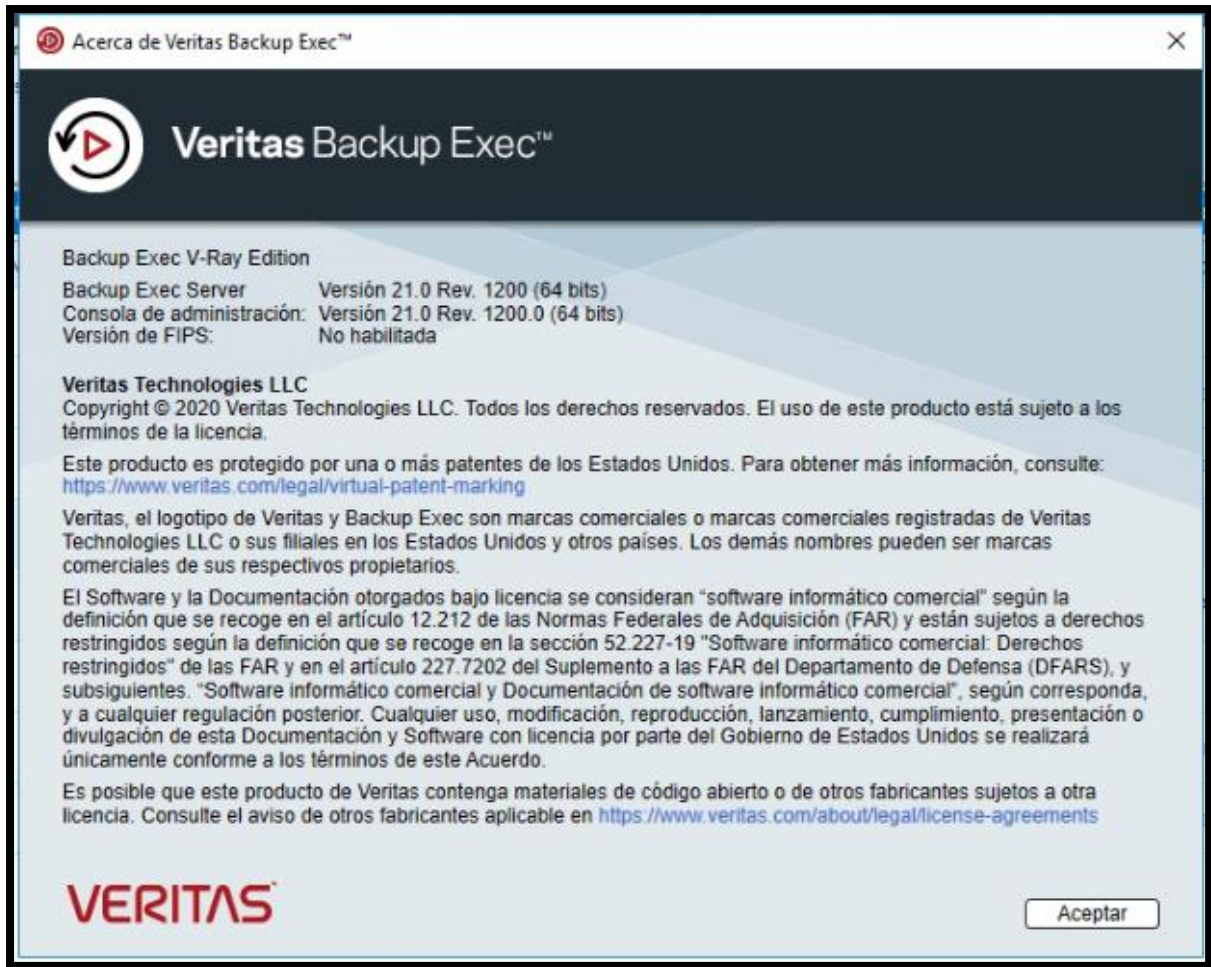


Figura 04: Software actualmente utilizado por la DRELM

Autoloader Information	
Serial Number	DEC0430936
Product ID	1x8 G2 AUTOLDR
Currently Installed Autoloader Firmware	6.00 / 2.90n
Bootcode Firmware Revision	0.82
Barcode Reader	SE625
Autoloader Mode	Automatic, Random
WWide Node Name	50014380272DFB8C
Autoloader Controller Version	LCM 1.1

Figura 05: Ventana informativa del autocargador de cintas

5.3 Procedimientos para el cambio de cintas mediante panel y consola web

El autocargador de cintas funciona con los siguientes métodos:

- Interfaz de gestión remota (RMI): esta interfaz permite supervisar y controlar el autocargador desde una página Web, en el cual se puede acceder a la mayoría de las funciones del autocargador.

Código : 110723145
Clave : 6289





PERÚ

Ministerio
de Educación

DOCUMENTO NORMATIVO

Manual de generación de copias de seguridad
(BACKUPS) de la Dirección Regional de
Educación de Lima Metropolitana

Código

MA-00X-02-DRELM

- Panel de control del operador (OCP): esta interfaz permite utilizar el dispositivo desde el panel frontal.
- Software de copia de seguridad del host: permite realizar algunas funciones básicas en el autocargador.

5.4 Interfaz de gestión remota (RMI)

5.4.1 Descripción general

La interfaz de gestión remota (RMI) permite supervisar y controlar el dispositivo desde un terminal conectado a la red o a través de internet. La RMI alberga un sitio de Internet dedicado y protegido que muestra una representación gráfica del dispositivo. Antes de utilizar la RMI, debe configurar las opciones de red del dispositivo y determinar la contraseña del administrador con el OCP. Para iniciar la RMI, abra un explorador HTML e introduzca la dirección IP del dispositivo en la barra de direcciones.

5.4.2 Inicio de sesión

Para iniciar sesión, seleccione Account Type, escriba la contraseña, si se la requiere, y haga clic en Log In.

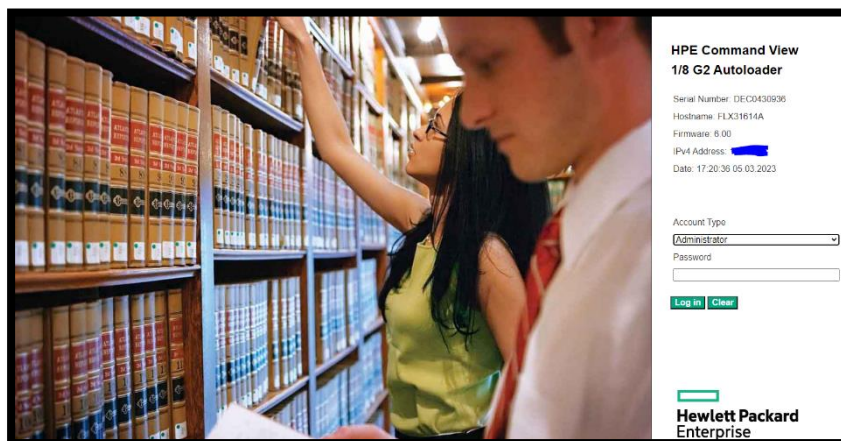


Figura 06: Ventana de inicio de sesión del autocargador de cintas

Los tipos de cuenta son:

- User: no requiere contraseña (deje el campo de contraseña en blanco).
- Administrator: requiere la contraseña del administrador. En el OCP y en la RMI se utiliza la misma contraseña de administrador. No existe una contraseña de administrador predeterminada.

El administrador debe configurar una contraseña en el OCP antes de utilizarla en la RMI. Si el administrador pierde la contraseña, póngase en contacto con HP para generar una contraseña temporal que concederá acceso al administrador.

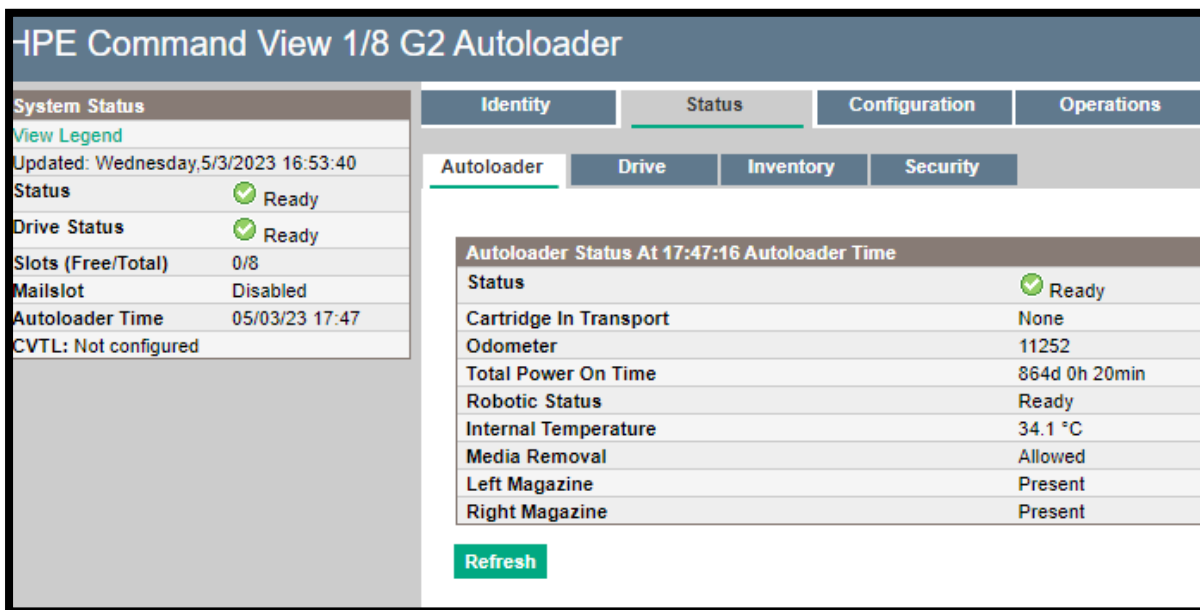
Service: sólo para personal de asistencia técnica de HP. La contraseña de servicio viene predeterminada de fábrica. En el OCP y en la RMI se utiliza la misma contraseña de servicio.

Código : 110723145
Clave : 6289



El inicio de sesión del usuario brinda acceso a las opciones Identity y Status, pero no a Configuration, Operations y Support. El nivel Administrator brinda acceso a todas las pantallas, excepto a Log configuration y HP Service.

5.5 Status Visualización de la información dinámica del dispositivo



The screenshot shows the HP Command View interface for an Autoloader. It features a 'System Status' sidebar on the left and a main content area with tabs for Identity, Status, Configuration, and Operations. The 'Status' tab is active, showing a 'Refresh' button and a table of autoloader details.

Autoloader Status At 17:47:16 Autoloader Time	
Status	Ready
Cartridge In Transport	None
Odometer	11252
Total Power On Time	864d 0h 20min
Robotic Status	Ready
Internal Temperature	34.1 °C
Media Removal	Allowed
Left Magazine	Present
Right Magazine	Present

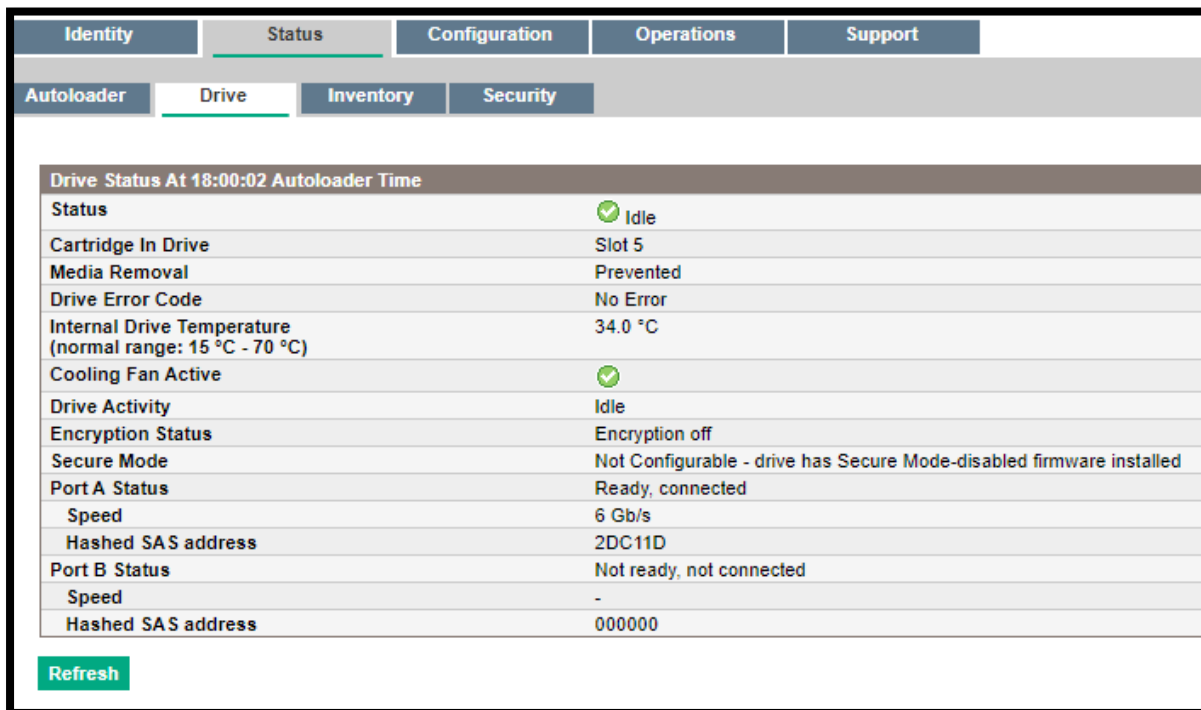
Figura 07: Ventana informativa de estado del autocargador de cintas

Cuando haga clic en Refresh, el estado se actualizará de inmediato. Es posible ver, pero no modificar, los siguientes valores:

- a) **Status:** estado general del dispositivo. El dispositivo funciona normalmente.
- b) **Cartridge in Transport:** número de ranura en donde se originó la cinta que se encuentra actualmente en la mecánica. Tendrá el valor None si no hay ninguna cinta en la mecánica.
- c) **Odometer:** cantidad total de movimientos que realizó el dispositivo desde su fabricación.
- d) **Total Power On Time:** cantidad de días, horas y minutos que el dispositivo estuvo encendido desde su fabricación.
- e) **Robotic Status:** estado actual de la mecánica y descripción de la operación que realiza actualmente.
- f) **Left Magazine:** tendrá el valor Present si el dispositivo detecta la presencia del cargador izquierdo.
- g) **Right Magazine:** tendrá el valor Present si el dispositivo detecta la presencia del cargador derecho.



5.6 Visualización de la información dinámica de la unidad



Drive Status At 18:00:02 Autoloader Time	
Status	Idle
Cartridge In Drive	Slot 5
Media Removal	Prevented
Drive Error Code	No Error
Internal Drive Temperature (normal range: 15 °C - 70 °C)	34.0 °C
Cooling Fan Active	
Drive Activity	Idle
Encryption Status	Encryption off
Secure Mode	Not Configurable - drive has Secure Mode-disabled firmware installed
Port A Status	Ready, connected
Speed	6 Gb/s
Hashed SAS address	2DC11D
Port B Status	Not ready, not connected
Speed	-
Hashed SAS address	000000

Figura 08: Ventana informativa de estado del DRIVE LTO7

En la Página Status - Drive, se brinda información detallada de la unidad de cinta del autocargador. Cuando haga clic en Refresh, el estado se actualizará de inmediato. Es posible ver, pero no modificar, los siguientes valores:

- Status:** estado de la unidad. La unidad funciona normalmente. La unidad funciona, pero puede presentar un problema que se debe solucionar. La unidad presenta errores.
- Cartridge in Drive:** información acerca del cartucho, si existe, que se encuentra actualmente en la unidad.
- Drive Error Code:** código de error de unidad actual, si la unidad presenta errores. Consulte para ver la lista de los códigos de error.
- Internal Drive Temperature:** temperatura interna indicada por la unidad. La temperatura normal se proporciona con fines de referencia y varía según el tipo de unidad de cinta. La unidad indicará que hay errores si existe alguna posibilidad de error a causa de la temperatura.

5.7 Cambio de la configuración del sistema

Los cambios en la configuración del sistema sólo se aplican tras seleccionar el botón Apply Selections o Submit. Una vez realizada la selección, una página de advertencia le informará acerca del impacto del cambio propuesto. En algunos casos, una ventana emergente le solicitará que confirme el cambio. En algunos casos también es necesario reiniciar el dispositivo.



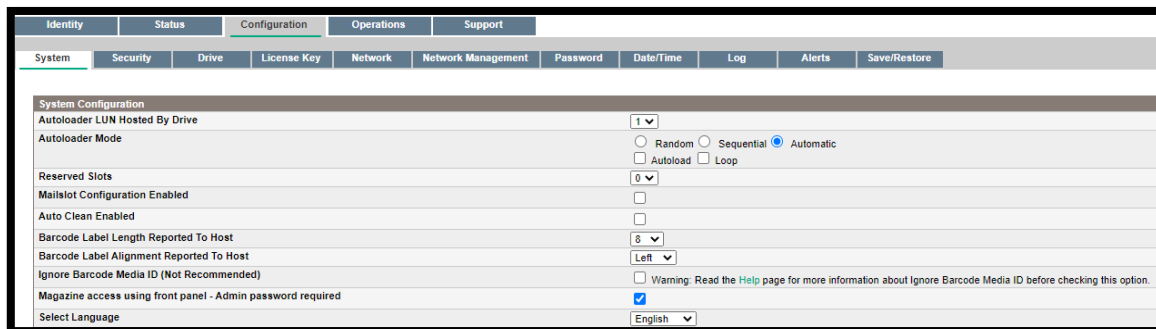



Figura 09: Ventana de configuración del autocargador de cintas

Los valores que pueden modificarse son:

- a) **Autoloader LUN Hosted by Drive:** siempre será 1 porque el autocargador tiene una sola unidad de cinta.
- b) **Autoloader Mode:** Random, Sequential, Automatic, Autoload y Loop. El autocargador admite tres modos: Random, Sequential y Automatic. El autocargador detecta automáticamente el modo necesario de la serie de comandos SCSI que recibe; no obstante, también se puede cambiar. Elija el modo de funcionamiento según las funciones del software encargado de controlar los cartuchos de cinta.
 - a. **Modo Random:** este modo se utiliza con una aplicación de copia de seguridad completa. Éste es el modo de funcionamiento más habitual. En el modo Random, el dispositivo no carga automáticamente las cintas en la unidad, sino que espera a recibir los comandos del software. El software de copia de seguridad debe ser compatible con la mecánica, que puede requerir un módulo de software adicional.
 - b. **Modo Sequential:** este modo se utiliza cuando el software de copia de seguridad NO es un software para mecánica o se diseñó sólo para unidades independientes. En el modo Sequential, el dispositivo carga y descarga automáticamente las cintas en la unidad. El operador determina la cinta que se cargará mediante la carga de la cinta deseada en la unidad de cinta. Cuando una cinta no se ha cargado por algún motivo, el dispositivo extrae automáticamente la cinta de la unidad, la coloca en la ranura original y luego carga la cinta de la siguiente ranura con el número más alto disponible. Para determinar con más detalle cómo desea cargar las cintas en la unidad de cinta durante el modo Sequential, puede configurar las opciones **Loop y Autoload** mediante el panel de control del operador.
 - c. **Autoload:** Cuando el modo Autoload está activado, el dispositivo carga automáticamente el cartucho de la ranura completa con el número más bajo en la unidad de cinta. A continuación, se produce el funcionamiento secuencial estándar.
 - d. **Loop:** Cuando el modo Loop está activado, el primer cartucho original de la secuencia se vuelve a cargar una vez que el dispositivo ha pasado por todos los cartuchos disponibles. Si el modo Loop está desactivado y se descargó el último cartucho, el dispositivo deja de cargar los cartuchos hasta que se cargue otro manualmente.



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
--	--	---------------------------

- e. **Modo Automatic:** la configuración predeterminada es el modo Automatic, que permite al dispositivo alternar entre los modos Random y Sequential en función de los comandos SCSI recibidos. El dispositivo permanece en el modo Sequential hasta que recibe comandos SCSI del cambiador de medios que activan el modo Random.
- c) **Active Slots:** cantidad de ranuras disponibles para el software de copia de seguridad. Es posible reservar hasta seis ranuras. Si la ranura de expansión está activada, la cantidad máxima de ranuras activas se reduce a una. También se pueden almacenar cintas de datos o de limpieza en el dispositivo y disminuir la cantidad de ranuras activas en consecuencia. Las ranuras se desactivan comenzando por el número más alto. El valor predeterminado consiste en activar la cantidad máxima de ranuras.
- d) **Mailslot Enabled:** configura la primera ranura como ranura de expansión o ranura de almacenamiento. La activación de la ranura de expansión disminuirá la cantidad total de ranuras de almacenamiento. De forma predeterminada, esta opción está desactivada.
- e) **Auto Clean Enabled:** cuando la función de limpieza automática está activada, el dispositivo carga automáticamente un cartucho de limpieza cuando la unidad de cinta debe limpiarse. El dispositivo identifica un cartucho de cinta como cartucho de limpieza si éste tiene una etiqueta de código de barras que comienza con CLN o después de cargar una cinta de limpieza sin etiquetar en la unidad de cinta. El autocargador puede utilizar un cartucho de limpieza de cualquier ranura, incluso si la ranura no está activa. El autocargador realiza un seguimiento del conteo de uso de cada cartucho de limpieza. Cuando haya varios cartuchos de limpieza disponibles, el autocargador elegirá primero un cartucho de limpieza desconocido para que el autocargador pueda iniciar el seguimiento del conteo de uso del cartucho. Si el autocargador conoce el conteo de uso de todos los cartuchos de limpieza, elegirá el de mayor conteo de uso. De forma predeterminada, la función de limpieza automática está desactivada. Es posible activar la limpieza automática, aunque no haya cartuchos de limpieza en el dispositivo. En este caso, el dispositivo mostrará un mensaje de advertencia.
- f) **Barcode Label Length Reported to Host:** cantidad de caracteres de código de barras notificados a la aplicación host. Esta opción proporciona compatibilidad de intercambio con bibliotecas que tienen capacidades de lectura de código de barras más limitadas. El valor predeterminado es 8.
- g) **Barcode Label Alignment Reported to Host:** configura el final de los caracteres de la etiqueta de código de barras que se notificarán a la aplicación host si se informan menos caracteres que la cantidad máxima. Por ejemplo, cuando se informan sólo seis caracteres de la etiqueta de código de barras 12345678, si la alineación está configurada hacia la izquierda, el autocargador indicará 123456. Si la alineación está configurada hacia la derecha, el autocargador indicará 345678. De forma predeterminada, esta opción está configurada en la alineación izquierda.

5.8 Cambio de la configuración de la unidad

Utilice la Página Configuration: Drive para cambiar el ID SCSI de la unidad de cinta y apagar o encender la unidad de cinta. Utilice la Página Configuration: Drive (SAS) para encender o apagar una unidad SAS. Las unidades SAS no requieren ninguna configuración.

Código : 110723145
Clave : 6289



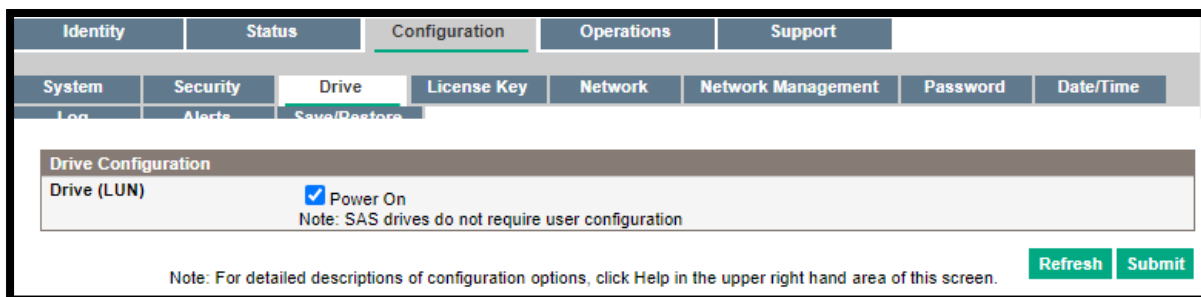


Figura 10: Ventana de configuración de apagado del DRIVE
5.9 Procedimientos para la limpieza de drive

Consola RMI

Utilice la Página Support: Clean Drive para limpiar la unidad de cinta.

Slot #: permite seleccionar el número de ranura de la cinta de limpieza.

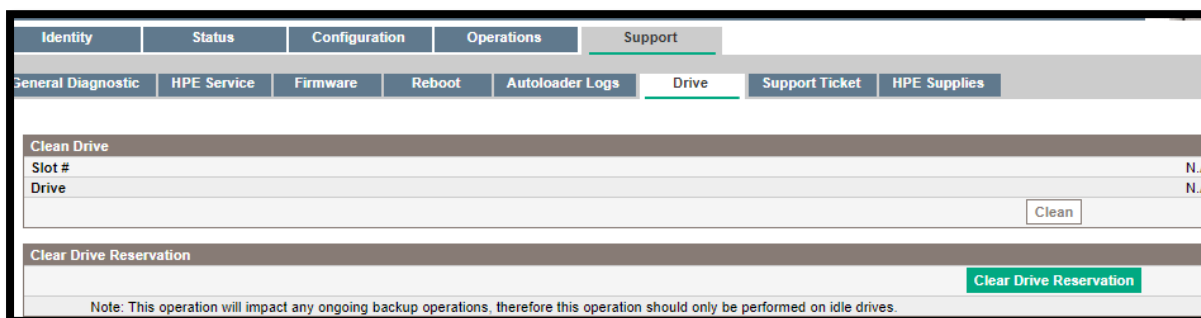


Figura 11: Ventana de tarea de limpieza (CLEAN) del DRIVE

Cuando la función de limpieza automática está activada, el dispositivo carga automáticamente un cartucho de limpieza cuando la unidad de cinta debe limpiarse. El dispositivo identifica un cartucho de cinta como cartucho de limpieza si éste tiene una etiqueta de código de barras que comienza con CLN o después de cargar una cinta de limpieza sin etiquetar en la unidad de cinta.


El autocargador puede utilizar un cartucho de limpieza de cualquier ranura, incluso si la ranura está reservada. El autocargador realiza un seguimiento del conteo de uso de cada cartucho de limpieza.

Cuando haya varios cartuchos de limpieza disponibles, el autocargador elegirá primero un cartucho de limpieza desconocido para que el autocargador pueda iniciar el seguimiento del conteo de uso del cartucho. Si el autocargador conoce el conteo de uso de todos los cartuchos de limpieza, elegirá el de mayor conteo de uso.

De forma predeterminada, la función de limpieza automática está desactivada. Es posible activar la limpieza automática, aunque no haya cartuchos de limpieza en el dispositivo. En este caso, el dispositivo mostrará un mensaje de advertencia.

Precaución:



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
--	--	---------------------------

Sólo se puede activar la función de limpieza automática en la aplicación de copia de seguridad o en el autocargador, pero no en ambos.

Configuración de Limpieza automática por Panel de LCD



Figura 12: Autocargador de cintas

- En la pantalla principal, pulse Previous o Next hasta que la pantalla muestre Configuration. Pulse Enter para realizar la selección.
- Pulse Previous o Next hasta que la pantalla muestre Configure Auto Cleaning. Pulse Enter para realizar la selección.
- Pulse Previous o Next hasta que la pantalla muestre Auto Cleaning Disabled o Auto Cleaning Enabled. Para cambiar la configuración de la limpieza automática, pulse Enter.
- Pulse Previous o Next hasta que la pantalla muestre la configuración que desea. Pulse Enter.

5.10 Inventario de cintas

5.10.1 Cartuchos de cinta y cargadores

En esta parte se explica qué soportes utilizar con el autocargador y cómo etiquetar y proteger contra escritura los cartuchos de cinta. Al etiquetar y manipular con cuidado los cartuchos de cinta, se extiende su vida útil y la del cargador de cintas.

5.10.2 Cartuchos de cinta.

Es importante el uso adecuado de los cartuchos de cinta, así como también darles el mantenimiento requerido.

Precaución:

No desmagnetice nunca los cartuchos. Estos cartuchos de datos se grabaron previamente con una señal magnética. Esta señal es necesaria para utilizar el cartucho con la unidad de cinta. No acerque objetos con carga magnética al cartucho.


Para asegurar una duración más prolongada de los cartuchos de datos, siga estas directrices:

- Utilice sólo los cartuchos de datos diseñados para su dispositivo.
- Limpie la unidad de cinta cuando se encienda el LED de unidad Clean.
- Utilice únicamente cartuchos de limpieza universales Ultrium.

No dejar que los cartuchos se caigan. Un golpe fuerte podría dañar el contenido interno del cartucho o el cartucho y dejarlo inservible.

Código : 110723145
Clave : 6289



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
--	--	---------------------------

No exponer los cartuchos de datos a la luz directa del sol ni a fuentes de calor, incluidos calefactores portátiles y conductos de calefacción.

La temperatura de funcionamiento de los cartuchos de datos oscila entre 10 °C y 35 °C. La temperatura de almacenamiento oscila entre los -40 °C y +60 °C en un entorno libre de polvo en el cual la humedad relativa sea de entre 20% y 80% (sin condensación).

Si el cartucho de datos ha estado expuesto a temperaturas fuera de los rangos especificados, establezca el cartucho a la temperatura ambiente durante el mismo período de tiempo que estuvo expuesto a temperaturas extremas o durante 24 horas (el menor de los dos períodos). No colocar los cartuchos de datos cerca de fuentes de alimentación electromagnéticas o de potentes campos magnéticos como monitores, motores eléctricos, altavoces o equipos de rayos X. Una exposición a energía electromagnética o a campos magnéticos puede destruir los datos y el código de servo integrado escrito en los soportes por el fabricante de cartuchos. Por este motivo, el cartucho puede quedar inutilizable.

5.10.3 Etiquetado de los cartuchos de cinta

Coloque etiquetas de identificación únicamente en el área designada del cartucho.

El dispositivo contiene un lector de código de barras que lee las etiquetas de las cintas y almacena los datos de inventario en la memoria. Luego, el dispositivo proporciona esa información a la RMI, el OCP y la aplicación host. Al adjuntar una etiqueta de código de barras a cada cartucho de cinta, se permite que el lector de código de barras identifique los cartuchos rápidamente, y así se disminuye el tiempo necesario para realizar el inventario. Procure usar etiquetas de código de barras en los cartuchos de cinta.

Sugerencia:

El escáner de código de barras debe explorar cada cinta o la parte posterior de la ranura de almacenamiento hasta leer la etiqueta del código de barras de la ranura de almacenamiento o del cartucho, o determinar si la ranura está vacía. El escáner del código de barras permite identificar un cartucho etiquetado adecuadamente en la primera exploración. En la segunda exploración, permite identificar una ranura vacía. Intenta varias exploraciones más y, a continuación, intenta determinar si hay un cartucho sin etiqueta en la ranura. Esta identificación demora cuatro veces más que la de un cartucho etiquetado correctamente. Aunque no necesite la información del código de barras, utilice las etiquetas de código de barras para acelerar el tiempo necesario para realizar el inventario.

El software de host podría tener que localizar la siguiente información mediante el código de barras asociado:

- Fecha del formato o la inicialización
- Reserva de soportes de cinta
- Datos contenidos en la cinta
- Antigüedad de la copia de seguridad

Código : 110723145
Clave : 6289





PERÚ

Ministerio de Educación

DOCUMENTO NORMATIVO

Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana

Código

MA-00X-02-DRELM

- Errores encontrados al usar la cinta (para determinar si la cinta es defectuosa)

Importante:

El mal uso y el desconocimiento de la tecnología de código de barras puede producir fallos en la restauración y la copia de seguridad. Para asegurarse de que los códigos de barras cumplen los estándares de calidad, adquiéralos siempre en un distribuidor autorizado y nunca los imprima usted mismo.

Los cartuchos de cinta Ultrium tienen una zona hueca situada en el frente del cartucho, al lado del conmutador de protección contra escritura. Use dicha zona para pegar la etiqueta de código de barras con reverso adhesivo. Aplíquela sólo como se muestra en la ilustración:

5.11 Protección contra escritura de los cartuchos de cinta

Todos los cartuchos de cinta regrabables disponen de un conmutador de protección contra escritura para evitar que los datos se borren o se sobrescriban accidentalmente. Antes de cargar un cartucho en el dispositivo, asegúrese de que el conmutador de protección contra escritura situado en la parte frontal del cartucho está colocado de la manera deseada.

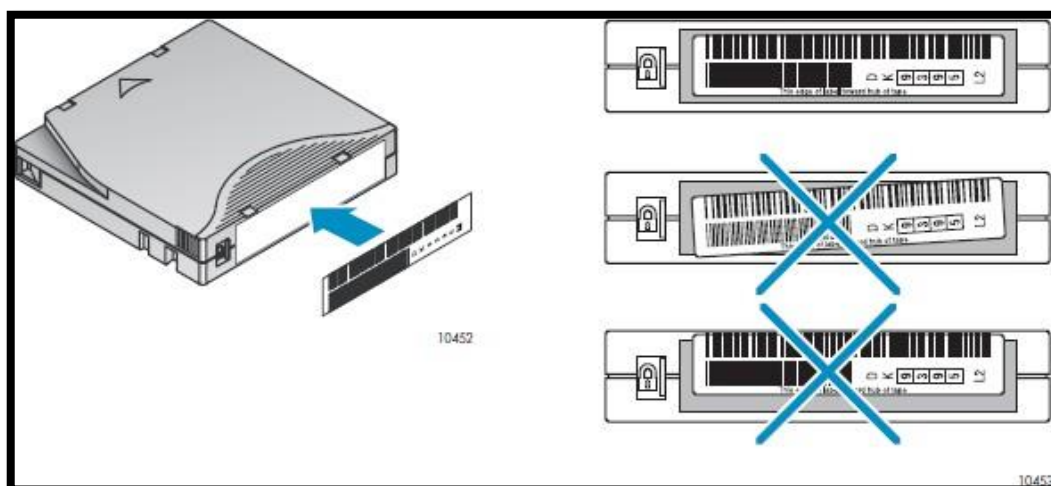


Figura 13: Etiquetado correcto de cinta

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autoría de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

Código : 110723145
Clave : 6289





PERÚ

Ministerio
de Educación

DOCUMENTO NORMATIVO

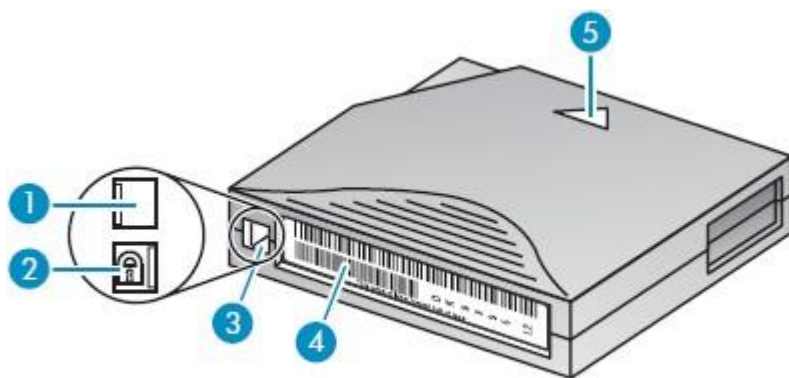
Manual de generación de copias de seguridad
(BACKUPS) de la Dirección Regional de
Educación de Lima Metropolitana

Código

MA-00X-02-DRELM

Girar el conmutador hacia la izquierda para permitir que el dispositivo escriba datos en el cartucho. Girar el conmutador hacia la derecha para proteger el cartucho contra escritura. Un indicador, como una marca roja o un pequeño candado, indican que el cartucho está protegido contra escritura.

- Habilitado para escritura
- Protegido contra escritura
- Conmutador de protección contra escritura
- Etiqueta de código de barras
- Flecha de indicación de inserción



10454

Figura 14: Protección de sobrescritura de cinta

5.12 Compatibilidad con lectura retroactiva

Los cartuchos de datos Ultrium de HP son totalmente compatibles con los productos de cinta Ultrium de HP StorageWorks. Dado que los soportes Ultrium de HP tienen el logotipo de Ultrium, se pueden utilizar con cualquier otro dispositivo que no sea de HP, pero que también tenga el logotipo de Ultrium. Actualmente la DRELM cuenta con el tipo de DRIVE de tecnología LTO-7.



	LTO-5 Ultrium 3000	LTO-6 Ultrium 6250	LTO-7 Ultrium 15000	LTO-8 Ultrium 30750	LTO-9 Ultrium 45000
Performance					
Sustained transfer rate, native	140 MB/s	160 MB/s	300 MB/s	300 MB/s	300 MB/s
Sustained transfer rate, compressed (assumes 2:1 data compression for LTO-4 and 5; 2.5:1 compression for LTO-6 and higher)	280 MB/s	400 MB/s	-	-	-
Burst transfer rate	600 MB/s (with 6Gb/s SAS)				1200 MB/s (with 12Gb/s SAS)
Data rate matching range	47-140 MB/s (native)	54-160 MB/s (native)	100-300 MB/s (native)	100-300 MB/s (native)	100-300 MB/s (native)
Average locate time (BOT - MOT)	52 s typical for a 1.5 TB tape (native)	50 seconds typical for LTO 6 media	60 seconds for LTO 7 media	60 seconds for LTO-8 media	60 seconds for LTO-9 media
Average load time	>19s	24s	12s	15s	17s
Average unload time	19s	19s	17s	24s	28s – 275s
Rewind time from EOT	96s (1.5 TB tape)	98s (2.5TB tape)	114s (6TB tape)	114s	123s
Rewind tape speed	9.0 m/s				
Reliability					
MTBF	250,000 hours at 100% duty cycle				
Uncorrected Error Rate	1 in 1x10 ¹⁷ bits		1 in 1x10 ¹⁹ bits		
Media Compatibility					
	LTO Ultrium 3 (Read only); LTO Ultrium 4 (Read and Write); LTO Ultrium 5 (Read and Write)	LTO Ultrium 4 (Read only); LTO Ultrium 5 (Read and Write); LTO Ultrium 6 (Read and write)	LTO Ultrium 5 (Read only); LTO Ultrium 6 (Read and Write); LTO Ultrium 7 (Read and write)	LTO Ultrium 7 (Read and Write); LTO Ultrium 8 (Read and Write)	LTO Ultrium 8 (Read and Write); LTO Ultrium 9 (Read and Write)

Figura 15: Tipos de tecnología del DRIVE de cintas

Fuente: https://www.hpe.com/psnow/doc/c04123270.pdf?jumpid=in_pdp-psnow-qs

5.13 Cargadores (autoloaders)

El dispositivo cuenta con cargadores extraíbles. El acceso al cargador está protegido por una contraseña. Por razones de seguridad, el movimiento mecánico se detiene cuando se extrae un cargador.

Los cargadores se pueden abrir mediante el panel de control del operador (OCP), la interfaz de gestión remota (RMI) o por liberación manual. HP recomienda liberar el cargador con el OCP (panel frontal) o la RMI (consola Web). El cargador se debe extraer de forma manual únicamente cuando haya un fallo en el proceso del OCP o la RMI, o cuando el dispositivo ya no tenga alimentación.

Importante:

Se puede liberar un cargador manualmente, en caso de atasco o falla. Sin embargo, este proceso manual se deberá utilizar únicamente si el cargador no se puede liberar mediante el panel de control del operador o la interfaz de gestión remota.





El esquema de numeración de ranuras del cargador izquierdo y derecho se muestran a continuación.

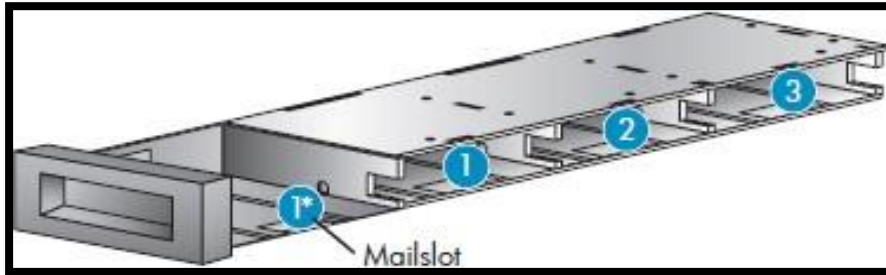


Figura 16: Cargador de cintas izquierdo del autocargador de cintas

Cargador izquierdo: numeración con ranura de expansión habilitada

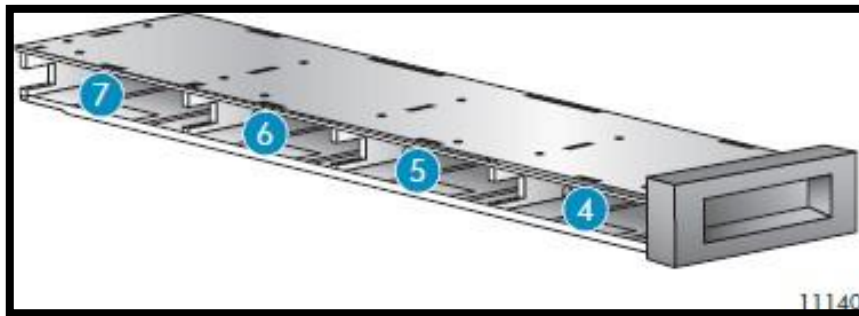


Figura 17: Cargador de cintas derecho del autocargador de cintas

Cargador derecho: numeración con ranura de expansión habilitada

Cuando la ranura de expansión está deshabilitada, se utiliza la ranura 1 y las demás se vuelven a numerar de manera acorde.

5.14 Traslado de soportes

Utilice la Página Operations: Move Media para trasladar cartuchos de cinta dentro del dispositivo.

Importante:

El traslado manual de soportes puede interferir con las operaciones del software de copia de seguridad. Asegúrese de que las copias de seguridad estén completas antes de trasladar soportes.





PERÚ

Ministerio de Educación

DOCUMENTO NORMATIVO

Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana

Código

MA-00X-02-DRELM

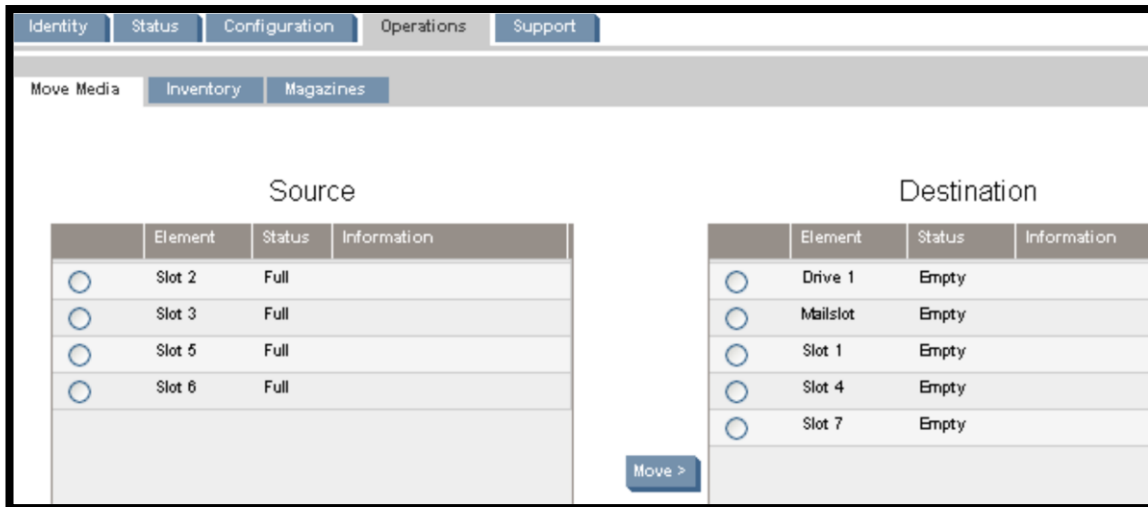


Figura 18: Ventana de operaciones para movimiento de cintas

Para trasladar una cinta, seleccione el origen y el destino, y haga clic en el botón Move ubicado en el centro de la pantalla para iniciar el traslado.

5.15 Actualización del inventario actual de soportes

Utilice la Página Operations: Inventory para hacer que el dispositivo vuelva a explorar las cintas y actualice el inventario de soportes.

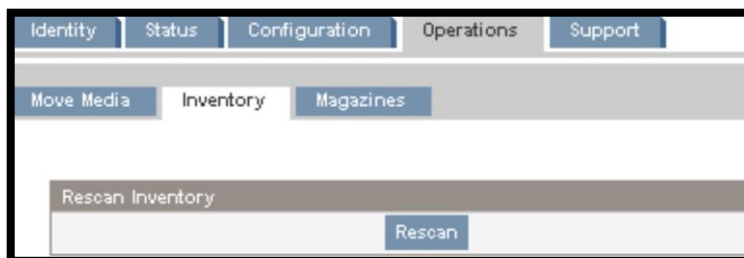


Figura 19: Ventana de operaciones para ejecución de inventario de cintas

5.16 Liberación y sustitución de cargadores

Utilice la Página Operations: Magazines para liberar el cargador derecho o izquierdo. Cuando haga clic en Release, el dispositivo desbloqueará el cargador y aparecerá el mensaje Left Magazine Unlocked o Right Magazine Unlocked en la pantalla del OCP. El cargador no se mueve hasta que se extrae del dispositivo. Si no se quita el cargador después de unos segundos, el dispositivo lo bloqueará. Al sustituir el cargador, el dispositivo realizará un inventario de los cartuchos de cinta del cargador.

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autoría de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

Código : 110723145
Clave : 6289



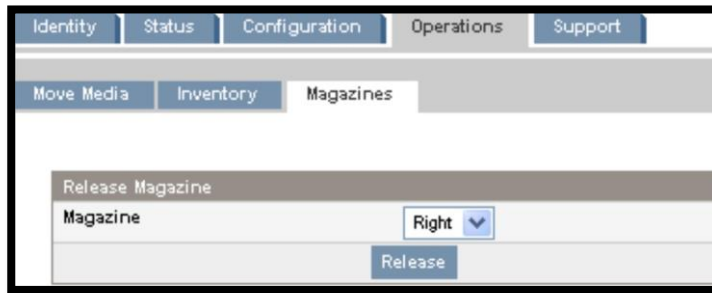


Figura 20: Ventana para desmontar los cargadores de cintas izquierda o derecha

5.17 Visualización del inventario del cartucho de cinta

En la Página Status: Inventory, se brinda información detallada de la cinta de la unidad de cinta, con un resumen de las cintas ubicadas en las ranuras de los cargadores. El rectángulo oscuro indica que la ranura está completa, el amarillo que el cartucho tiene un problema y el blanco que la ranura está vacía.

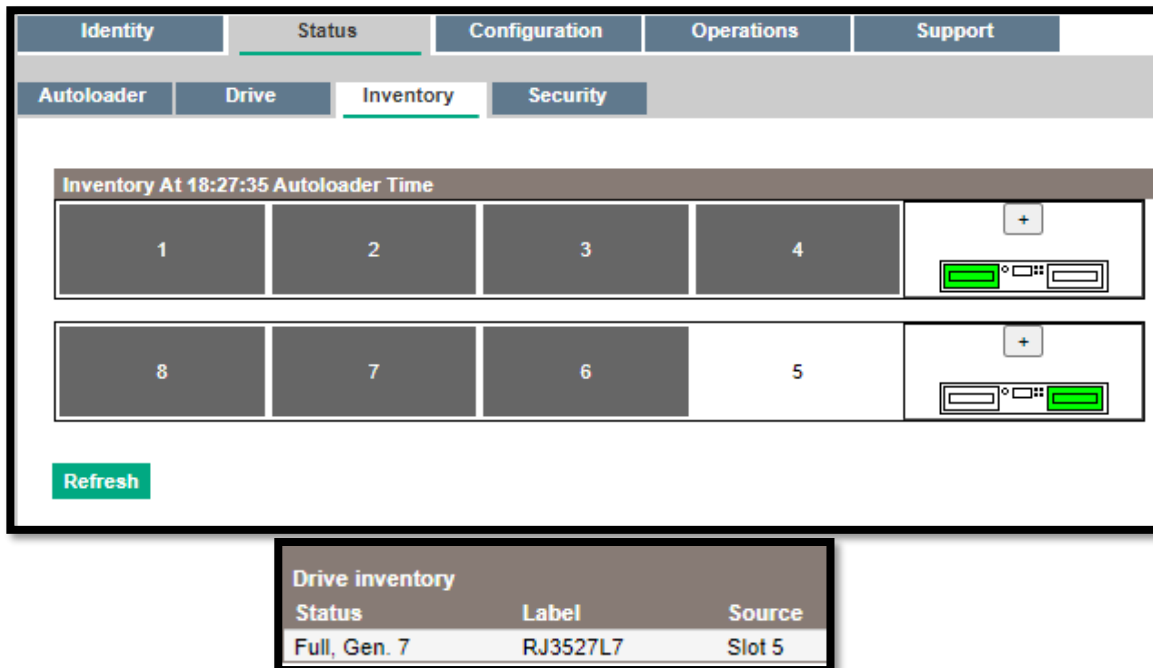


Figura 21: Ventana informativa del inventario de cintas

Para obtener información detallada sobre las cintas ubicadas en un cargador, haga clic en el botón + para expandir la imagen del cargador.





Inventory At 18:34:52 Autoloader Time

Slot #	Attn	Status	In Drive	Label	Media Loads	Comment
1		Full, Gen. 7		CCB000L7	57	Not Encrypted
2		Full, Gen. 7		RJ3521L7	840	Not Encrypted
3		Full, Gen. 7		RJ3525L7	660	Not Encrypted
4		Full, Gen. 7		CCB002L7	30	Not Encrypted

Slot #	Attn	Status	In Drive	Label	Media Loads	Comment
5		Empty	1	-----		Not Encrypted
6		Full, Gen. 7		RJ3536L7	165	Not Encrypted
7		Full, Gen. 7		CCB006L7	91	Not Encrypted
8		Full, Gen. 7		RJ3529L7	87	Not Encrypted

Figura 22: Ventana informativa detallada del inventario de cintas

En el panel Media Details, encontrará las siguientes opciones:

- a) **Slot #:** muestra, de menor a mayor, "Mailslot" o el número de índice de cada ranura del cargador.
- b) **Attn:** indica el estado de atención de las ranuras de almacenamiento o brinda información acerca del estado de la ranura de expansión.
- c) **Status:** Full o Empty.
- d) **In Drive:** muestra un valor cuando la cinta de la ranura está en una unidad.
- e) **Label:** datos de la etiqueta de código de barras de la cinta que se encuentra en la ranura.
- f) **Media Loads:** cantidad de veces que se cargó la cinta en una unidad en toda su duración. Este campo puede estar vacío si no se cargó la cinta en una unidad de este dispositivo o si se modificó el inventario.
- g) **Comment:** cualquier información adicional sobre la cinta de la ranura (por ejemplo, Clean Tape si el cartucho es una cinta de limpieza).

5.18 Visualización del inventario del cartucho de cinta Panel LCD

En la pantalla principal, pulse Previous o Next hasta que la pantalla muestre Operations. Pulse Enter para realizar la selección. Pulse Previous o Next hasta que la pantalla muestre Perform Inventory. Pulse Enter para realizar la selección.





PERÚ

Ministerio de Educación

DOCUMENTO NORMATIVO

Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana

Código

MA-00X-02-DRELM

Mientras el inventario esté en progreso, la pantalla mostrará Scanning. El autocargador comprueba si la unidad y las ranuras contienen cintas para actualizar la información del inventario.

Nota:

Este comando sólo es necesario si el inventario del dispositivo difiere del que aparece en el panel frontal. Esto no debería ocurrir en condiciones normales de funcionamiento.

5.19 Inventario actual de cintas Backup disponibles

N°	CÓDIGO DE CINTA	TIPO
1	RJ3533	LTO7
2	RJ3534	LTO7
3	RJ3520	LTO7
4	RJ3537	LTO7
5	RJ3528L7	LTO7
6	RJ3535L7	LTO7
7	RJ3538	LTO7
8	CCA960L7	LTO7
9	CIS459	LTO7
10	CIS458	LTO7
11	RJ3539L7	LTO7
12	RJ3523L7	LTO7
13	RJ3524L7	LTO7
14	RJ3529L7	LTO7
15	CIS453L7	LTO7
16	CIS451L7	LTO7
17	CIS450L7	LTO7
18	RJ3522L7	LTO7
19	RJ3526L7	LTO7
20	RJ3521	LTO7
21	RJ3525	LTO7
22	RJ3527	LTO7
23	RJ3532	LTO7
24	RJ3531	LTO7
25	RJ3530	LTO7
26	CIS457	LTO7
27	CIS456	LTO7
28	CCB002	LTO7
29	CCB006	LTO7
30	RJ3536	LTO7
31	CCB000	LTO7

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autoría de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

Código : 110723145
Clave : 6289





PERÚ

Ministerio
de Educación

DOCUMENTO NORMATIVO

Manual de generación de copias de seguridad
(BACKUPS) de la Dirección Regional de
Educación de Lima Metropolitana

Código

MA-00X-02-DRELM

N°	CÓDIGO DE CINTA	TIPO
32	CCB003	LTO7
33	CIS461	LTO7
34	CCB005	LTO7
35	CCB001	LTO7
36	CIS455	LTO7
37	CCA976L7	LTO7
38	CCA975L7	LTO7
39	CCA974L7	LTO7
40	CCA973L7	LTO7
41	CCA970L7	LTO7
42	CCA971L7	LTO7
43	CCA972L7	LTO7
44	CCA977L7	LTO7
45	CCA978L7	LTO7
46	CCA979L7	LTO7

Fuente: Elaboración propia

5.20 Inventario de servidores y sistemas respaldados


5.20.1 Servidores virtuales y/o físicos respaldados con copia única en cintas

Copia única, debido a que los sistemas de información se encuentran inactivos y/o no reciben actualizaciones diarias.

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autoría de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

Código : 110723145
Clave : 6289



	PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
---	--	--	---------------------------

Copias únicas completas de todo el servidor

N°	Nombre de la máquina virtual	IP	Estado	Tipo de copia	Código de cinta	Mes/año de la copia	Sistema operativo	Nombre de equipo	Descripción de servidor	Tipo de servidor	Tamaño	Tiempo
1	10.9.1.1	10.9.1.1	Inactivo	Única	Rj352017	Apr-23	Windows server 2008	P_del_01	Dominio "del" antiguo	Virtual	172 gb	02 hr
2	10.9.1.124	10.9.1.124	Inactivo	Única	Rj353417	Apr-23	Centos	Servdrelm.124.drelm.gob.pe	Sistema de monitoreo del aire acondicionado y ups	Virtual	18 gb	13 min
3	10.9.1.180	10.9.1.180	Inactivo	Única	Rj35371t	Apr-23	Windows 7	Servdrelm-180	Servidor de escalafón - legix	Virtual	647 gb	03 hr 46 min
4	10.9.1.24	10.9.1.24	Activo	Única	Rj353317	Apr-23	Windows server 2008 r2	Win-sinad-web	Servidor de aplicaciones - sinad	Virtual	189 gb	02 hr 05 min
5	10.9.1.26	10.9.1.26	Inactivo	Única	Rj35371t	Apr-23	Windows server 2008 r2	Servdrelm-26	Base de datos del sistema de libro de reclamaciones	Virtual	145 gb	54 min
6	10.9.1.82	10.9.1.82	Inactivo	Única	Rj353417	Apr-23	Windows server 2012 r2	Servdrelm-82	Distribución de materiales 2019 drelm - ugel	Virtual	392 gb	02 hr 22 min
7	10.9.1.83	10.9.1.83	Inactivo	Única	Rj353417	Apr-23	Windows server 2012 r2	Servdrelm-83	Servidor de denuncias (0 corrupción) - sasie v1.0	Virtual	77 gb	37 min
8	10.9.1.83_01	10.9.1.83	Inactivo	Única	Rj353417	Apr-23	Windows server 2012 r2	Servdrelm-83	Servidor de denuncias (0 corrupción) - sasie v1.1	Virtual	96.3 gb	44 min
9	10.9.1.86	10.9.1.86	Activo	Única	Rj353417	Apr-23	Windows server 2012 r2	Servdrelm-86	Reporte de apoyo a la productividad - rap	Virtual	26.3 gb	33 min
10	10.9.1.96	10.9.1.96	Inactivo	Única	Rj353417	Apr-23	Centos	Servdrelm-96*	Servidor central de llamadas antiguo	Virtual	120 gb	33 min

Código : 110723145
Clave : 6289





PERÚ

Ministerio de Educación

DOCUMENTO NORMATIVO

Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana

Código


MA-00X-02-DRELM

N°	Nombre de la máquina virtual	IP	Estado	Tipo de copia	Código de cinta	Mes/año de la copia	Sistema operativo	Nombre de equipo	Descripción de servidor	Tipo de servidor	Tamaño	Tiempo
11	10.9.1.97	10.9.1.97	Inactivo	Única	Rj3537lt	Apr-23	Windows server 2008 r2	Servdrelm-97	Solarwindws monitoreo de red	Virtual	68.2 gb	29 min
12	Aplicaciones ii	10.9.1.18	Inactivo	Única	Rj3537lt	Apr-23	Centos	Linux	Servidor de aplicaciones 2.0	Virtual	40 gb	11 min
13	Domiii	10.9.1.201	Activo	Única	Rj353417	Apr-23	Windows server 2012 r2	Servdrelm-201	Servidor de dominio "drelm" secundario	Virtual	26.4 gb	27 min
14	Fe	10.9.1.207	Inactivo	Única	Rj3537lt	Apr-23	Centos	Localhost.local	Firma electrónica - fe (piloto)	Virtual	5.51 gb	03 min
15	Flujo_02	10.9.1.19	Inactivo	Única	Rj3537lt	Apr-23	Windows server 2008	Servdrelm-19	Sistema de flujo de expedientes	Virtual	81.6 gb	34 min
16	Noe	10.9.1.80	Activo	Única	Rj353717	Apr-23	Centos	Firma	Repositorio de firma digital noe	Virtual	2.07 tb	01 día 09 hr 45 min
17	Recauda ii	10.9.1.98	Activo	Única	Rj353417	Apr-23	Windows server 2012 r2	Servdrelm-198-1	Sistema de recaudación de institutos 2022	Virtual	117 gb	03 hr 25 min
18	Reloj	10.9.1.106	Activo	Única	Rj353717	Apr-23	Windows server 2012 r2	Servdrelm11	Sistema sica de asistencia (reloj)	Virtual	246 gb	02 hr 29 min
19	Reniec	10.9.1.85	Activo	Única	Rj3537lt	Apr-23	Windows server 2012 r2	Servdrelm-85	Pide reniec	Virtual	31.1 gb	36 min
20	Sasie	10.9.1.83	Inactivo	Única	Rj3537lt	Apr-23	Windows server 2012 r2	Servdrelm-83	Servidor de denuncias (0 corrupción) - sasie v2.0	Virtual	35.1 gb	23 min
21	Sasie 2.0	10.9.1.83	Inactivo	Única	Rj3537lt	Apr-23	Windows server 2012 r2	Servdrelm-83	Servidor de denuncias (0 corrupción) - sasie v2.1	Virtual	55.1 gb	01 hr 11 min
22	Servidorvpn	10.9.1.212	Activo	Única	Rj3537lt	Apr-23	Centos	Servdrelm	Conexión virtual al servidor del minedu - sup y tcp	Virtual	2.44 gb	05 min

Código : 110723145

Clave : 6289



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO	Código
	Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	MA-00X-02-DRELM

N°	Nombre de la máquina virtual	IP	Estado	Tipo de copia	Código de cinta	Mes/año de la copia	Sistema operativo	Nombre de equipo	Descripción de servidor	Tipo de servidor	Tamaño	Tiempo
23	Sinad-del	10.9.1.10	Activo	Única	Rj3537lt	Apr-23	Windows server 2003	Sinad.del	Sistema de sinad antiguo 2014	Virtual	63.9 gb	29 min
24	Sql	10.9.1.205	Inactivo	Única	Rj3534I7	Apr-23	Windows server 2012 r2	Servdrelm-205	Servidor de base de datos sica	Virtual	500 gb	03 hr 25 min
25	10.9.1.12	10.9.1.12	Activo	Única	Rj3534I7	Apr-23	Windows server 2016	Drelm120029	Servidor de archivos de instaladores	Virtual	2 tb	11 hr

Fuente: Elaboración propia

Código : 110723145
Clave : 6289




Copias únicas de carpetas alojadas en los servidores

N°	IP	ESTADO	TIPO DE COPIA	CÓDIGO DE CINTA	MES/AÑO DE LA COPIA	SISTEMA OPERATIVO	NOMBRE DE EQUIPO	DESCRIPCIÓN DE SERVIDOR	TIPO DE SERVIDOR	TAMAÑO	TIEMPO	CARPETAS	COMENTARIO
1	10.9.1.204	ACTIVO	ÚNICA	RJ3528L7	Feb-23	WINDOWS SERVER 2012 R2	SERVDRELM-204	Servidor de Archivos 01 - ETI	VIRTUAL	1.23 TB	02 días 11 hr 15 min	Carpeta 01 al 13	
2	10.9.1.91	ACTIVO	ÚNICA	RJ3535LT	Feb-23	WINDOWS SERVER 2012 R2	SERVDRELM-91	Sistema y archivos de Microformas	FISICO	2.48 TB	01 día 07hr 15 min	Carpeta Files Repositorio parte 01: 1-1-1-INSPECCION 1-16-39-PRUEBA 123 1-16-39-PRUEBA 2021 1-17-40-RDR-RJ-2021 1-18-142-DIGITAL-MESA DE PARTES 1-19-44-PLANILLAS 1-20-46-LEGAJOS CAS 1-3-5-AUDITORIA 2020 1-3-5-DIG-21 1-3-5-DIG-SGS	Las carpetas y archivos seleccionados que aloja el servidor tienen copia única.

Código : 110723145
Clave : 6289



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
---	--	---------------------------


N°	IP	ESTADO	TIPO DE COPIA	CÓDIGO DE CINTA	MES/AÑO DE LA COPIA	SISTEMA OPERATIVO	NOMBRE DE EQUIPO	DESCRIPCIÓN DE SERVIDOR	TIPO DE SERVIDOR	TAMAÑO	TIEMPO	CARPETAS	COMENTARIO
3	10.9.1.91	ACTIVO	ÚNICA	CIS459L7	Mar-23	WINDOWS SERVER 2012 R2	SERVDRELM-91	Sistema y archivos de Microformas	FISICO	45.3 GB	01 día 07hr 15 min	Unidad D, todas las carpetas excepto la del nombre "SERVER-CYBERSCAN-28122021"	Las carpetas y archivos seleccionados que aloja el servidor tienen copia única.
4	10.9.1.91	ACTIVO	ÚNICA	CCA960L7	Feb-23	WINDOWS SERVER 2012 R2	SERVDRELM-91	Sistema y archivos de Microformas	FISICO	2.42 TB	01 día 18hr 43 min	Carpeta Files Repositorio parte 02.	Las carpetas y archivos seleccionados que aloja el servidor tienen copia única.

Fuente: Elaboración propia

Código : 110723145
Clave : 6289



Página 34 de 45


 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
--	--	---------------------------

5.20.2 Servidores virtuales y/o físicos respaldados diariamente, semanalmente, quincenalmente y/o mensual en cintas

Copias de forma diaria, semanal, quincenalmente y/o mensual, debido a que los sistemas de información se encuentran en constante crecimiento de almacenamiento de información, por lo que el tiempo de respaldo es variable de acuerdo al tipo de servidor que aloja los sistemas de información.

- Para los sistemas de información y base de datos que se encuentran alojados en servidores virtuales, el tiempo de demora de un respaldo de tipo FULL BACKUP, se sitúa en un rango de 30 minutos a 04 horas.
- Para el servidor de microformas y de archivos (File Server) que se encuentran alojados en servidores físicos y virtual con un tamaño de información de aproximadamente de 20 TB, el tiempo de demora de un respaldo de tipo FULL BACKUP, se sitúa en un rango de 3 días a 7 días.
- El tiempo de demora de un respaldo de tipo INCREMENTAL, se sitúa en un rango de 03 a 15 minutos. Cabe indicar, que las tareas de copias de seguridad del tipo INCREMENTAL solo se aplican al servidor de microformas y de archivos (File Server).




 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
---	--	---------------------------

Copias de seguridad de los sistemas de información prioritarios

N°	IP	Estado	Carpeta	Nombre de Equipo	Descripción del servidor	Tipo de Servidor	Tamaño de copia completa (Full Backup)	Tiempo de copia completa (Full Backup)	Programación de copia completa (Full Backup)	Programación de copia incremental	Tiempo de copia incremental
1	10.9.1.91_1	Activo	Toda la unidad C	SRVHPE	Servidor del Sistema y archivo de Microformas	FISICO	29.4 GB	01 hr 23 min	A las 14:00 hrs y luego cada 1 día		
2	10.9.1.91_2	Activo	Files/Cyberrepositorio	SRVHPE	Servidor del Sistema y archivo de Microformas	FISICO	391 GB	06 hr 36 min	Cada 30 días*	A las 17:25 hrs y luego cada 1 día	26min
3	10.9.1.91_3	Activo	Compartir/ActividadesSpam	SRVHPE	Servidor del Sistema y archivo de Microformas	FISICO	1.70 TB	20 hr 48 min	Cada 30 días*	A las 17:15 hrs y luego cada 1 día	10 min
4	10.9.1.91_3	Activo	Compartir/Inventario y control 2023	SRVHPE	Servidor del Sistema y archivo de Microformas	FISICO	2.16 TB	01 día 03 hr 29 min	Cada 30 días*	A las 17:35 hrs y luego cada 1 día	10 min
5	10.9.1.91_3	Activo	Compartir/Inventario y control 2022	SRVHPE	Servidor del Sistema y archivo de Microformas	FISICO	2.16 TB	01 día 03 hr 29 min	Cada 30 días*	A las 17:00 hrs y luego cada 1 día	10 min
6	10.9.1.91_3	Activo	Compartir/Microformas 01 - 2018	SRVHPE	Servidor del Sistema y archivo de Microformas	FISICO	1.00 TB	12 hr 47 min	Cada 30 días*	A las 17:10 hrs y luego cada 1 día	10 min
7	10.9.1.91_3	Activo	Toda la carpeta compartir excepto Actividades Spam y Microformas 01- 2018	SRVHPE	Servidor del Sistema y archivo de Microformas	FISICO	1.00 TB	12 hr 15 min	Cada 30 días*	A las 16:45 hrs y luego cada 1 día	10 min
8	10.9.1.204	Activo	Toda la unidad D	SERVDRELM-204	Servidor de archivos 01 - ETI	VIRTUAL	500 GB	08 hr 21 min	Cada 30 días*	A las 17:45 hrs y luego cada 1 día	10 min
9	10.9.1.105	Activo	Todo el servidor virtual	SERVDRELM-105	Servidor de Base de datos MYSQL - (Mesa de partes virtual, Acceso a la	VIRTUAL	51.6 GB	50 min	A las 06:30 hrs y luego cada 1 día		

Código : 110723145
Clave : 6289



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO	Código
	Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	MA-00X-02-DRELM

N°	IP	Estado	Carpeta	Nombre de Equipo	Descripción del servidor	Tipo de Servidor	Tamaño de copia completa (Full Backup)	Tiempo de copia completa (Full Backup)	Programación de copia completa (Full Backup)	Programación de copia incremental	Tiempo de copia incremental
					Información Pública)						
10	10.9.1.99	Activo	Todo el servidor virtual	SERVDRELM-99	Servidor de Aplicaciones (Mesa de partes virtual, Acceso a la Información Pública)	VIRTUAL	449 GB	03 hr 28 min	A las 22:00 hrs y luego cada 1 día		
11	10.9.1.6	Activo	Todo el servidor virtual	SERVDRELM-06	Servidor del Sistema SIAF	VIRTUAL	454 GB	03 hr 32 min	A las 01:40 hrs y luego cada 1 día		
12	10.9.1.25	Activo	Todo el servidor virtual	SERVDRELM-25	Servidor del Sistema SIGA	VIRTUAL	179 GB	01 hr 11 min	A las 05:15 hrs y luego cada 1 día		
13	10.9.1.23	Activo	Todo el servidor virtual	WIN-SINAD-BD	Servidor de Base de datos SINAD	VIRTUAL	570 GB	04 hr 04 min	A las 17:50 hrs y luego cada 1 día		
14	10.9.6.168	Activo	Todo el servidor virtual	SERVDRELM-168	Servidor del sistema NEXUS DRELM	VIRTUAL	500 GB	03 hr 06 min	A las 10:00 hrs y luego cada 1 día		
15	10.9.1.202	Activo	Todo el servidor virtual	SERVDRELM-202	Servidor de Active Directory drelm.gob.pe (DOMINIO)	VIRTUAL	49.1 GB	44 min	A las 09:10 hrs y luego cada 1 día		
16	10.9.1.27	Activo	Todo el servidor virtual	SERVDRELM-27	Servidor del sistema SISPER	VIRTUAL	217 GB	01 hr 34 min	A las 07:30 hrs y luego cada 1 día		

Fuente: Elaboración propia

**De acuerdo a la infraestructura actual del centro de datos de la DRELM el tiempo de respaldo del servidor de microformas y el servidor de archivos es de 3 a 7 días (considerando fallas externas de las tareas de ejecución de las copias), estos se realizan de manera mensual y en cintas. Cabe indicar, que durante ese tiempo no existirá copias de seguridad en cintas de los otros sistemas de información.*

Código : 110723145
Clave : 6289



Página 37 de 45

Tipo de copia - Full Backup (Copia Completa)

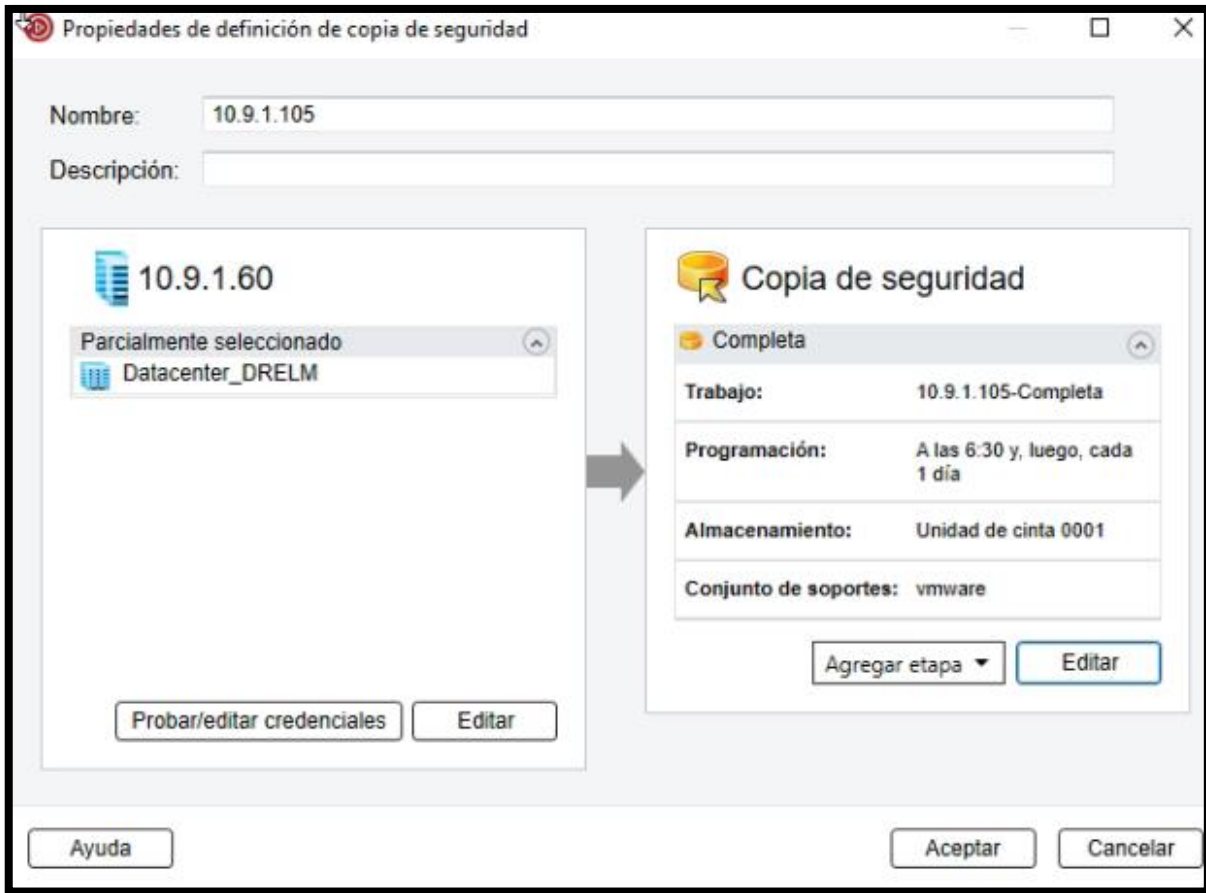


Figura 23: Política Full Backup configurada de manera diaria de un servidor virtual



Tipo de Copia Incremental

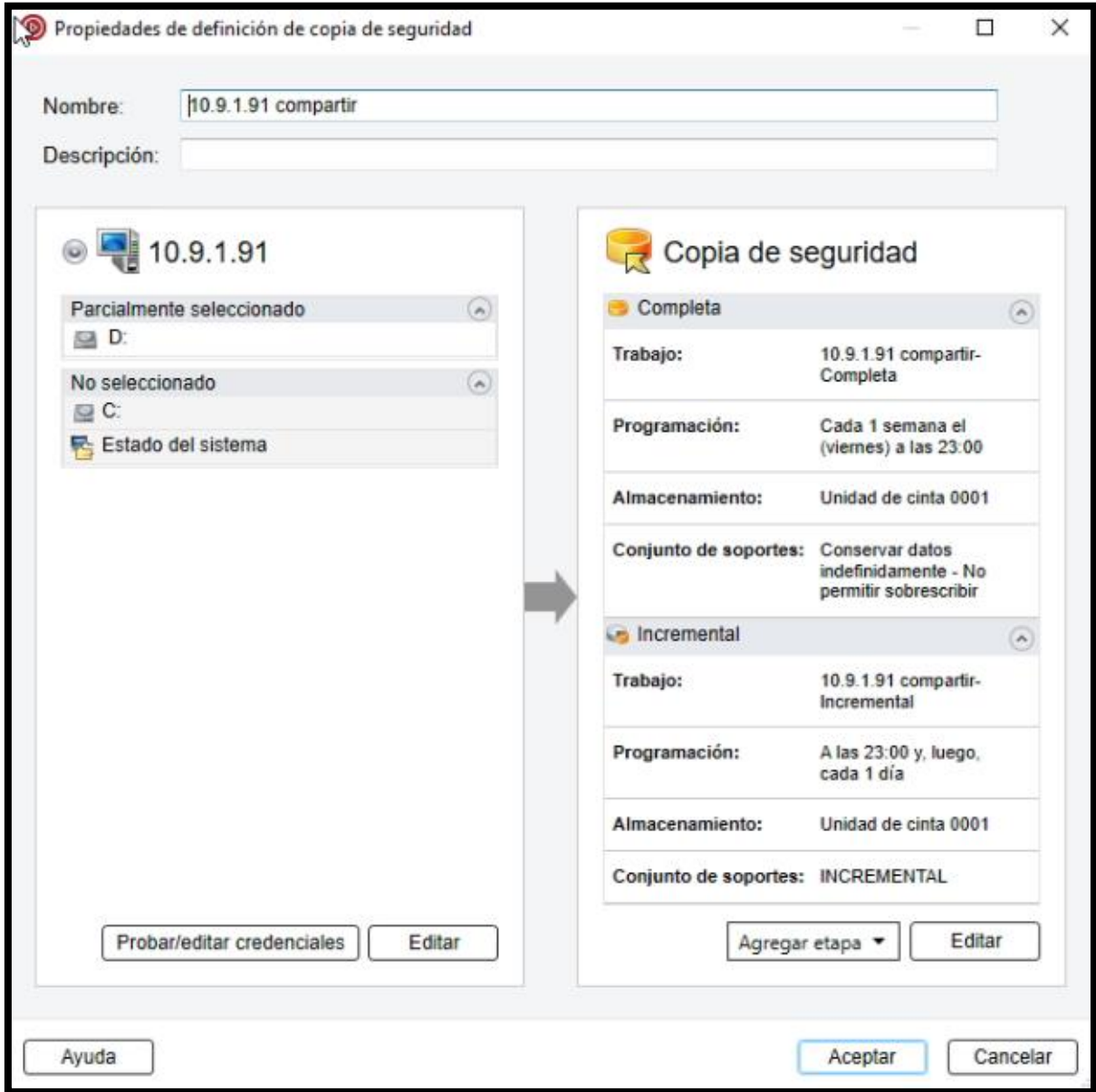


Figura 24: Política Incremental configurada de manera diaria de un servidor físico que es utilizado como servidor de archivos.



Actualmente existe un soporte de medios para backups (copias de seguridad) incrementales y otro para full backups.

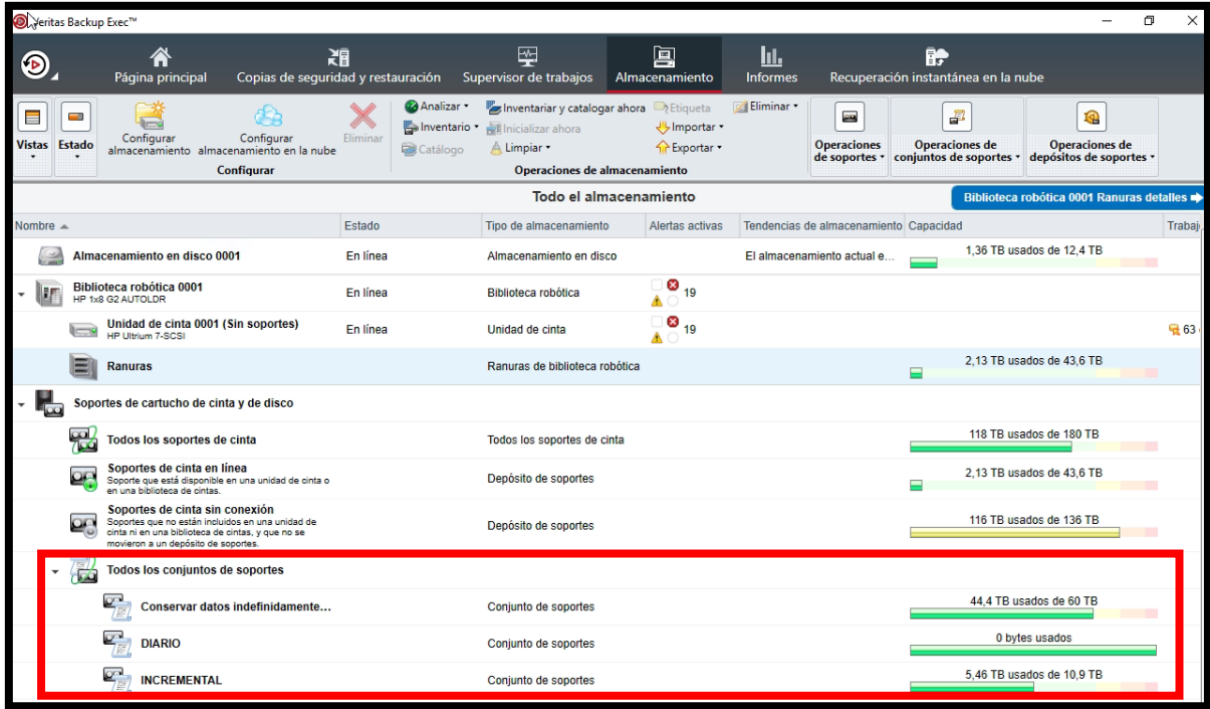


Figura 25: Conjunto de soportes

El servidor de Backup cuenta con almacenamiento en cintas de aproximadamente 43,6 TB.

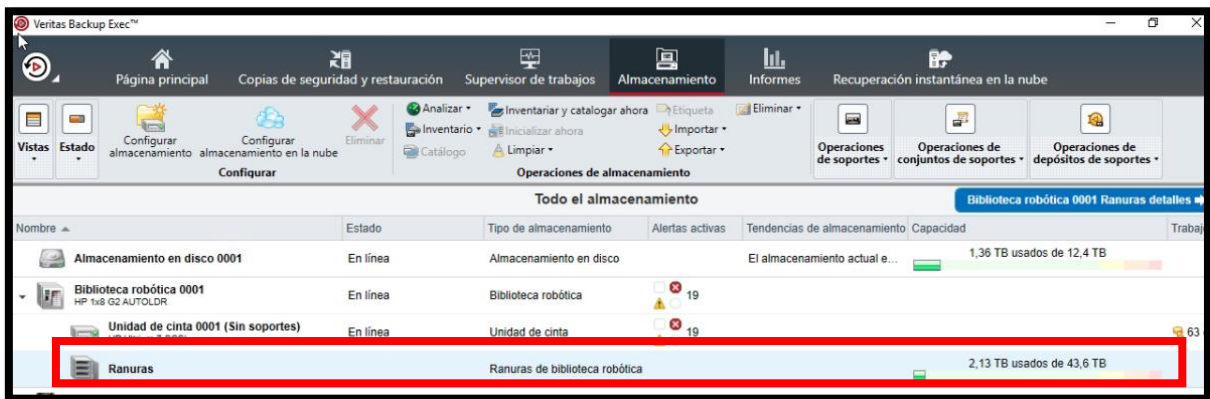

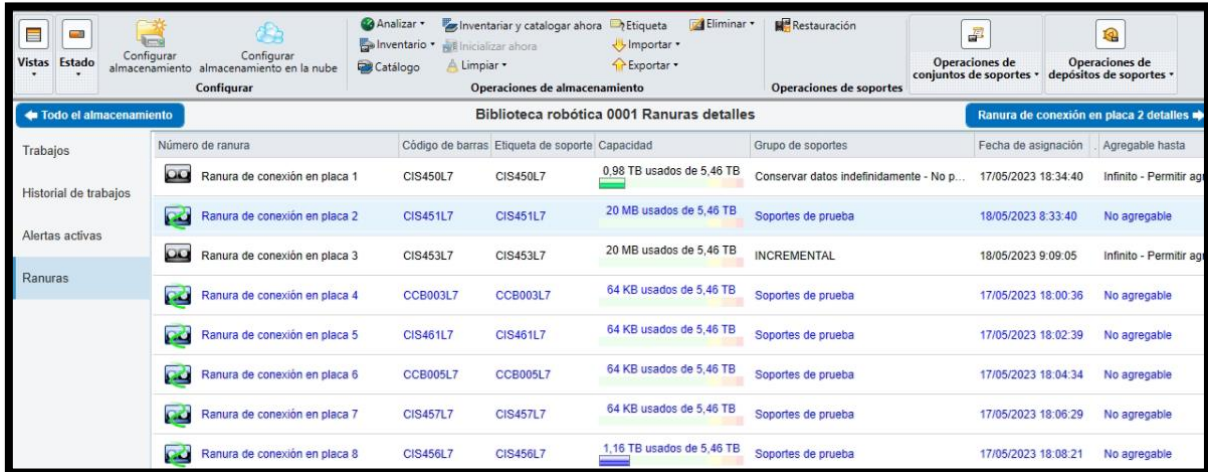


Figura 26: Capacidad de almacenamiento en cintas



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
--	--	---------------------------

El autocargador de cintas tiene la capacidad para 8 Slots, se puede apreciar ocho (8) cartuchos de cinta disponibles para el respaldo de la información.



Número de ranura	Código de barras	Etiqueta de soporte	Capacidad	Grupo de soportes	Fecha de asignación	Agregable hasta
Ranura de conexión en placa 1	CIS450L7	CIS450L7	0,98 TB usados de 5,46 TB	Conservar datos indefinidamente - No p...	17/05/2023 18:34:40	Infinito - Permitir ag
Ranura de conexión en placa 2	CIS451L7	CIS451L7	20 MB usados de 5,46 TB	Soportes de prueba	18/05/2023 8:33:40	No agregable
Ranura de conexión en placa 3	CIS453L7	CIS453L7	20 MB usados de 5,46 TB	INCREMENTAL	18/05/2023 9:09:05	Infinito - Permitir ag
Ranura de conexión en placa 4	CCB003L7	CCB003L7	64 KB usados de 5,46 TB	Soportes de prueba	17/05/2023 18:00:36	No agregable
Ranura de conexión en placa 5	CIS461L7	CIS461L7	64 KB usados de 5,46 TB	Soportes de prueba	17/05/2023 18:02:39	No agregable
Ranura de conexión en placa 6	CCB005L7	CCB005L7	64 KB usados de 5,46 TB	Soportes de prueba	17/05/2023 18:04:34	No agregable
Ranura de conexión en placa 7	CIS457L7	CIS457L7	64 KB usados de 5,46 TB	Soportes de prueba	17/05/2023 18:06:29	No agregable
Ranura de conexión en placa 8	CIS456L7	CIS456L7	1,16 TB usados de 5,46 TB	Soportes de prueba	17/05/2023 18:08:21	No agregable

Figura 27: Cintas disponibles

5.21 Servidores virtuales respaldados diariamente con apoyo de la herramienta VMWARE

La DRELM tiene implementado una plataforma de virtualización para la administración de máquinas virtuales de la marca VMWARE.



Figura 28: Versión del software VMware



Dicha herramienta permite ejecutar una tarea de respaldo mediante un snapshot o imagen instantánea de un disco, el cual es una copia del archivo de disco de la máquina virtual (VMDK) en un momento concreto. Conserva el sistema de archivos del disco y la memoria del sistema de nuestra VM, permitiéndonos volver a esa imagen guardada o snapshot en el caso de que algo vaya mal.

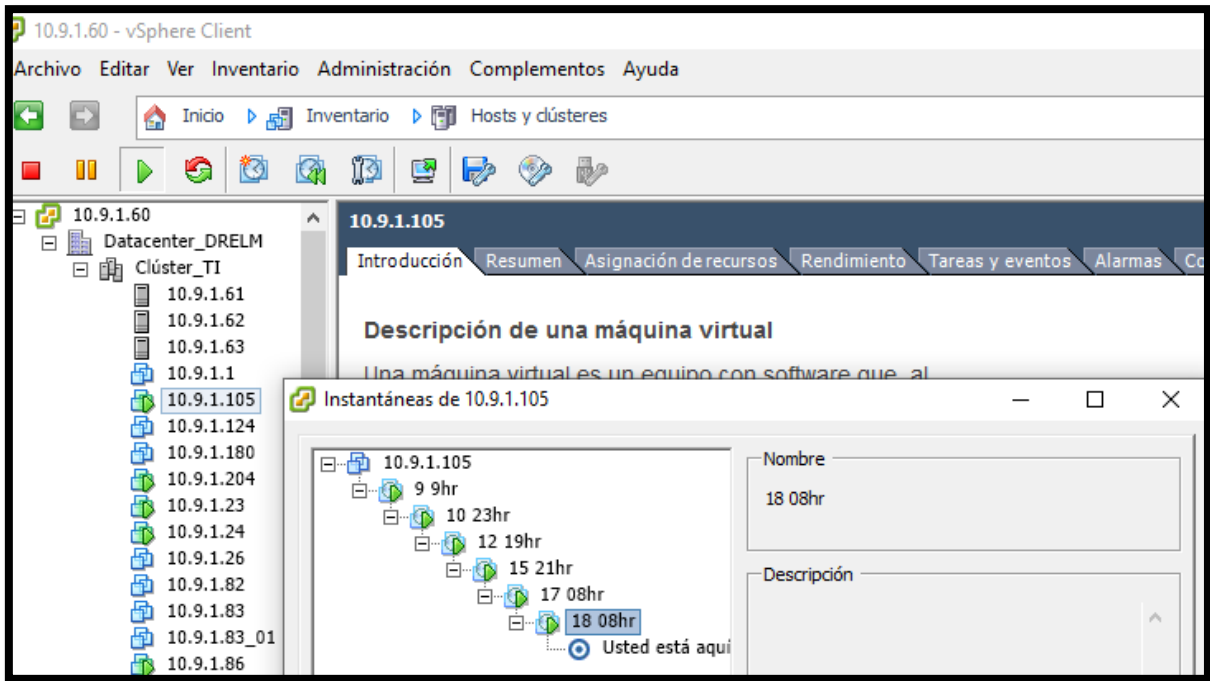



Figura 29: Vista de administración de instantáneas

Los snapshots o imagen instantánea pueden ser auténticos salvavidas cuando actualizamos o parcheamos aplicaciones y servidores.



 PERÚ Ministerio de Educación	DOCUMENTO NORMATIVO Manual de generación de copias de seguridad (BACKUPS) de la Dirección Regional de Educación de Lima Metropolitana	Código MA-00X-02-DRELM
--	--	---------------------------

Copias de seguridad de máquinas virtuales con herramienta Vmware

N°	IP	Estado	Nombre máquina virtual	Descripción del servidor	Tamaño	Tipo de Servidor	Programación de copia de tipo snapshot
1	10.9.1.105	Activo	10.9.1.105	Servidor de Base de datos MYSQL - (Mesa de partes virtual, Acceso a la Información Pública)	160 GB	VIRTUAL	A las 22:00 hrs y luego cada 1 día
2	10.9.1.204	Activo	10.9.1.204	Servidor de archivos 01 - ETI	3 TB	VIRTUAL	A las 22:00 hrs y luego cada 1 día
3	10.9.1.23	Activo	10.9.1.23	Servidor de Base de datos SINAD	600 GB	VIRTUAL	A las 22:00 hrs y luego cada 1 día
4	10.9.1.209	Activo	204	Servidor de archivos 01 - Oficinas	3 TB	VIRTUAL	A las 22:00 hrs y luego cada 1 día
5	10.9.1.99	Activo	Apps	Servidor de Aplicaciones (Mesa de partes virtual, Acceso a la Información Pública)	750 GB	VIRTUAL	A las 22:00 hrs y luego cada 1 día
6	10.9.1.206	Activo	ArchivoOAD	Servidor de archivos 02 - OAD	1 TB	VIRTUAL	A las 22:00 hrs y luego cada 1 día
7	10.9.1.6	Activo	CloneI	Servidor del Sistema SIAF	1 TB	VIRTUAL	A las 22:00 hrs y luego cada 1 día
8	10.9.1.203	Activo	Dfsone	Servidor de archivos 03 - Oficinas	4 TB	VIRTUAL	A las 22:00 hrs y luego cada 1 día
9	10.9.1.202	Activo	DomII	Servidor de Active Directory drelm.gob.pe (DOMINIO)	160 GB	VIRTUAL	A las 22:00 hrs y luego cada 1 día
10	10.9.1.201	Activo	DomIII	Servidor secundario de Active Directory drelm.gob.pe (DOMINIO)	40 GB	VIRTUAL	A las 22:00 hrs y luego cada 1 día
11	10.9.6.168	Activo	Nexus	Servidor del sistema NEXUS DRELM	500 GB	VIRTUAL	A las 22:00 hrs y luego cada 1 día
12	10.9.1.25	Activo	SERVDRELM-25	Servidor del Sistema SIGA	360 GB	VIRTUAL	A las 22:00 hrs y luego cada 1 día
13	10.9.1.27	Activo	SERVDRELM-27	Servidor del sistema SISPER	250 GB	VIRTUAL	A las 22:00 hrs y luego cada 1 día

Fuente: Elaboración propia

Código : 110723145
Clave : 6289

Página 43 de 45



5.22 Formato de registro de reporte de sistemas de información con copias de respaldo

N°	IP	Tipo de Copia	Código de cinta	Fecha y hora de inicio de copia	Fecha y hora final de copia	Descripción del servidor	Tipo de servidor	Tamaño de la copia	Tiempo de la copia

Fuente: Elaboración propia





5.23 Pruebas de restauración de copias de seguridad

El objetivo principal de las pruebas de restauración de copias de seguridad es garantizar que los datos y sistemas respaldados puedan ser recuperados de manera efectiva en caso de una pérdida de datos o un desastre. El plan de pruebas también busca identificar y solucionar cualquier problema relacionado con la recuperación de datos.

Las pruebas de restauración de copias de seguridad deben cubrir todos los sistemas y datos críticos respaldados, incluyendo servidores, bases de datos, archivos y cualquier otro elemento vital para el funcionamiento del negocio.

Procedimiento de pruebas:

- Identificar el tipo de copias de seguridad: Determinar si se realizarán pruebas de restauración de copias de seguridad completas o incrementales.
- Verificación de la integridad de los datos, la funcionalidad de los sistemas restaurados y el tiempo de recuperación.
- Las pruebas de restauración de copias de seguridad se realizan cada 30 días.
- Seleccionar los sistemas de información que se utilizarán en las pruebas. Esto puede incluir bases de datos de producción, archivos de configuración y cualquier otro elemento relevante.
- Restaurar las copias de seguridad seleccionadas en un entorno de prueba aislado. Verificar que los sistemas y datos se recuperen correctamente y que estén operativos.
- Registrar y documentar los resultados de las pruebas, incluyendo cualquier problema identificado durante el proceso de restauración de la copia de seguridad y las acciones tomadas para resolverlos.

Registro y resultado de la restauración

N°	Fecha y hora de restauración	Servidor	Tipo de Backup	Carpeta	Fecha y hora de la copia a restaurar	Tiempo de la restauración	Resultado	Comentarios

Fuente: Elaboración propia

