Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), marzo-abril 2025,
Volumen 9, Número 2.

https://doi.org/10.37811/cl_rcm.v9i2

IMPLEMENTACIÓN E INSTALACIÓN DE UNA LIBRERÍA DE CINTAS PARA RESPALDO DE LOS SERVIDORES DE UNA EMPRESA AUTOMOTRIZ

IMPLEMENTATION AND INSTALLATION OF A TAPE LIBRARY TO BACKUP THE SERVERS OF AN AUTOMOTIVE COMPANY

Verónica Faríaz Veloz
Tecnológico Nacional de México

Claudia Anglés Barrios
Tecnológico Nacional de México

María Eugenia Sánchez Leal
Tecnológico Nacional de México

Marisela Palacios Reyes
Tecnológico Nacional de México

Jazmín Andrea García Navarro
Tecnológico Nacional de México

DOI: https://doi.org/10.37811/cl_rcm.v9i2.17004

Implementación e Instalación de una Librería de Cintas para Respaldo de los Servidores de una Empresa Automotriz

Verónica Faríaz Veloz[1]
veronica.fv@cdjuarez.tecnm.mx
https://orcid.org/0000-0001-8147-1573
Tecnológico Nacional de México, Campus Ciudad Juárez

Claudia Anglés Barrios
claudia.ab@cdjurez.tecnm.mx
https://orcid.org/0000-0002-8935-0968
Tecnológico Nacional de México, Campus Ciudad Juárez

María Eugenia Sánchez Leal
veronica.fv@cdjuarez.tecnm.mx
https://orcid.org/0000-0003-1410-2019
Tecnológico Nacional de México, Campus Ciudad Juárez

Marisela Palacios Reyes
marisela.pr@cdjuarez.tecnm.mx
https://orcid.org/0000-0003-2830-5829
Tecnológico Nacional de México, Campus Ciudad Juárez

Jazmín Andrea García Navarro
Jazmingarcia0305@gmail.com
https://orcid.org/0009-0003-5087-841X
Tecnológico Nacional de México, Campus Ciudad Juárez

RESUMEN

Hoy en día el tema de la seguridad de la información, la ciberseguridad y sus respaldos es crucial para todas las empresas, ya que son temas de suma importancia cuando se trabaja con información dentro de una compañía porque siempre hay la posibilidad de estar expuestos a correr riesgos de que esta pueda dañarse o perderse por completo. La investigación presentada se basó en la instalación y configuración de una librería de cintas, donde su principal objetivo fue realizar el respaldo de la información de los servidores de una empresa teniendo de esta manera, una solución local que permitiera la recuperación de manera rápida y confiable de los datos. El proyecto se realizó con el fin de mantener la integridad y confidencialidad de la información, ofreciendo también la disponibilidad de esta misma en caso de que la compañía sufra de algún ataque cibernético o algún desastre natural. Una de las principales causas por las que se realizó este proyecto es porque anteriormente la empresa había sufrido ataques y perdida de la información, tardando varias semanas para la recuperación total de esta, además de buscar minimizar los tiempos de inactividad y tener la disponibilidad de los archivos lo más pronto posible.

Palabras clave: seguridad, respaldos, librería de cintas, recuperación, disponibilidad

[1] Autor principal.
Correspondencia: veronica.fv@cdjuarez.tecnm.mx

Implementation and Installation of a Tape Library to Backup the Servers of an Automotive Company

ABSTRACT

Nowadays the issue of information security, cybersecurity and its backups is crucial for all companies, since they are issues of utmost importance when working with information within a company because there is always the possibility of being exposed to running risks that it can be damaged or lost completely. The research presented was based on the installation and configuration of a tape library, where its main operation was to back up the information of the company's servers, thus having a local solution that allows the recovery of data quickly and reliably. The project was carried out in order to maintain the integrity and confidentiality of the information, also offering its availability in case the company suffers a cyberattack or natural disaster. One of the main reasons why this project was carried out is because previously the company has suffered attacks and loss of information, taking several weeks for the total recovery of this, in addition to seeking to minimize downtime and have the availability of the files as soon as possible.

***Keywords**:* security, backups, tape library, recovery, availability

Artículo recibido 13 febrero 2025

Aceptado para publicación: 19 marzo 2025

INTRODUCCIÓN

Actualmente la empresa donde se desarrolló la investigación se encuentra en Cd. Juárez Chihuahua, en donde se requirió la instalación de una herramienta para el respaldo de la información que se maneja dentro de los servidores de la compañía.

Hoy en día uno de los recursos más importantes para cualquier industria es la información que se maneja dentro de ella, es por eso que es de suma importancia que el departamento de IT (tecnologías de la información) le garantice a la empresa que la información que se utiliza en sus equipos sea respaldada en caso de que sufra algún ataque cibernético. El implementar una herramienta para el respaldo de información es importante y de gran utilidad para poder recuperarla de manera rápida y poder continuar con las labores de la empresa lo más rápido posible.

La Seguridad de la Información se describe como todo aquello que rodea la protección de la información digital de fuerzas destructivas o acciones indeseadas de usuarios no autorizados, como puede ser un ciberataque o una filtración de datos, es un razonamiento y un conjunto coordinado y concreto de esfuerzos y soluciones de software implementados en una organización, diseñada para proteger de manera integral la información confidencial que se transmite cada día (FORTRA, 2021).

Toda la información que se encuentra en los dispositivos que se utilizan hoy en día, son expuestos a los delincuentes si no se cuenta con algunas medidas de seguridad, esto podría ocasionar graves consecuencias, como es la perdida de datos, y por la tanto en una compañía es pérdida de dinero.

De acuerdo con la ISO/IEC(2016) la seguridad como “Aquellos procesos, buenas prácticas y metodologías que buscan proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada”.

Como usuarios se debe prevenir y evitar ser parte de estos ataques, es por eso que existen distintas maneras de poder evadirlo, algunas de estas prácticas que se deben realizar, son:

- Mantener los dispositivos actualizados a la última versión de SO.
- No seleccionar enlaces o archivos adjuntos desconocidos.
- Usar contraseñas más seguras y difíciles de descifrar.
- Establecer la autenticación de dos factores.
- Evitar descargar software de internet de fuentes no seguras.

Así mismo, existen algunos conceptos que definen la seguridad de la información, estos conceptos son conocidos como Triada CID que es, la confidencialidad, integridad y disponibilidad.

La tríada CID es un modelo común que constituye la base para el desarrollo de sistemas de seguridad. Se utilizan para encontrar vulnerabilidades y métodos para crear soluciones, idealmente, cuando se cumplen los tres estándares, el perfil de seguridad de la organización es más sólido y está mejor equipado para manejar incidentes de amenazas (FORTINET, 2025). La definición de los términos es:

Confidencialidad

Se habla de confidencialidad, cuando hablamos de la privacidad, es decir evitar que la información que sea confidencial no sea divulgada a personas externas, el acceso a esta debe estar limitado, para evitar que en algún momento llegue a las personas incorrectas. A las personas que se les autorice el acceso a estos documentos, deben respetar las políticas de las compañías en la que trabajan. (Briceño, 2021)

Integridad

Las medidas de integridad protegen la información de alteraciones no autorizadas. Estas medidas garantizan la exactitud e integridad de los datos. La necesidad de proteger la información incluye tanto los datos que se almacenan en los sistemas como los que se transmiten entre sistemas, como el correo electrónico. Para mantener la integridad, no sólo es necesario controlar el acceso a nivel del sistema, sino también garantizar que los usuarios del sistema sólo puedan alterar la información para la que están legítimamente autorizados. Las contramedidas de integridad eficaces también deben proteger contra la alteración no intencionada, como los errores de los usuarios o la pérdida de datos como resultado de un mal funcionamiento del sistema (Comillas Universidad Pontificia, 2023).

Para que la integridad sea protegida se pueden realizar algunas soluciones, como la autentificación, comprobar y validar la entrada de datos. Un ejemplo de la integridad, es proporcionar autorización a ciertos usuarios a las carpetas compartidas que se manejan dentro de la empresa, para darles autorización se deberá pedir autorización al departamento de IT y al gerente o dueño de ella, así se evita que otros usuarios entren y modifiquen algo.

Disponibilidad

La disponibilidad consiste en que la persona autorizada pueda acceder a la información y al activo cuando lo necesite. A su vez, la información debe ser accesible fácilmente para las personas autorizadas

que la necesiten. “La propiedad debe ser accesible y utilizable por una entidad autorizada”, definición ISO 27000. En ocasiones, el no tener acceso a un determinado activo, puede suponer la necesidad de detener la producción, con los problemas que ello conlleva (INCIB CHILE, 2021).

En el ámbito de la ciberseguridad, se implementan medidas de protección para asegurar la continuidad del servicio, como la redundancia de servidores, la gestión de la capacidad y los planes de recuperación ante desastres. Estas acciones ayudan a minimizar las interrupciones y a asegurar que los sistemas estén disponibles cuando se necesiten (Patalano, 2022).

La ciberseguridad se puede encontrar en diferentes entornos, tales como:

- **Seguridad de la red:** Mantener las redes protegidas, para evitar que algún ataque cibernético. Se protegen todos los dispositivos de hardware como son: servidores, ruteadores, puntos de acceso, y los mismos datos que transitan por estos dispositivos.
- **Seguridad de los usuarios:** En este entorno la seguridad, protege toda la información personal del usuario. Como es nombre, direcciones, tarjetas de crédito, entre otro tipo de información personal que manejamos dentro de nuestros equipos.
- **Seguridad de las aplicaciones:** Se relaciona en conservar todos aquellos softwares que se utilizan a diario, para las actividades diarias laborales o personales, sin virus o amenazas que afecten en su funcionamiento.
- **Seguridad de hardware:** La seguridad de hardware es el cómo mantienen los dispositivos físicos seguros.
- **Recuperación ante desastres:** Se habla de la recuperación de la información ante desastre, cuando se habla de cómo una empresa actúa ante la situación, cuando se pierden los datos o son atacados y les roban la información y esto les impide seguir con sus actividades laborales. (Solleiro, 2022)

De acuerdo a las definiciones de la Unión Europea, IFT, UIT, y Palo Alto Network, la ciberseguridad es la protección de los datos, sistemas e información de los ataques diarios, el principal objetivo es ofrecer y garantizar a los usuarios la integridad y confiabilidad de la información. (Solleiro, 2022)

Según (Oracle, 2016)Las mejores prácticas de recuperación ante desastres (DR) empresarial consisten, principalmente, en el diseño y la implementación de sistemas de software y hardware con tolerancia a

fallos que pueden sobrevivir a un desastre (“continuidad empresarial”) y reanudar las operaciones normales (“reanudación empresarial”) con una intervención mínima y, en condiciones ideales, sin pérdida de datos. Construir entornos con tolerancia a fallos para cumplir con los objetivos de DR empresarial y las limitaciones presupuestarias reales puede resultar costoso y demorar mucho tiempo; además, exige un fuerte compromiso de la empresa.

Hasta ahora se definió lo que es la ciberseguridad y la seguridad de la información, y se puede observar que son dos temas con un mismo objetivo, pero distintos. La seguridad tiene como propósito proteger la información de riesgos que pueden ocasionar la pérdida total de ella, al contrario, la ciberseguridad su objetivo es principalmente la información y los sistemas que la procesan, almacenan o transmiten los datos. (Duque, 2021)

La investigación presentada se realizó en una empresa dedicada a la elaboración de productos de partes automotrices para el sistema de control de enfriamiento de los automóviles de diversas marcas. Anteriormente hubo problemas con los respaldos que se realizan para guardar la información de los servidores, ya que se tenía el servicio de un proveedor encargado de realizar los respaldos y estos no verificaban si se realizaban completamente o tenían alguna falla.

De acuerdo a (Quintana, 2024) El respaldo de datos es un medio de protección de la información que está destinado a evitar que esta se pierda. Cuando una empresa decide realizar un respaldo de datos significa que va a hacer una copia de archivos, documentos e incluso de la misma configuración del sistema. Lo anterior quiere decir que, en caso de pérdida, fallo de los sistemas, robo o infección, se contará con los elementos necesarios para dar continuidad a las operaciones.

Tener un respaldo de los datos es sencillamente una salvaguarda de cualquier negocio y ayuda en gran medida a conservar la confianza de los clientes y colaboradores de la organización. Además, garantiza la integridad y disponibilidad de la información crítica, permitiendo una rápida recuperación y minimizando el impacto de cualquier incidente que afecte la infraestructura. Todas las organizaciones manejan información importante y confidencial de la que dependen para que su negocio siga funcionando. Por lo tanto, la pérdida de la misma sería catastrófica pues no solo estarían perdiendo un par de datos sino todo el trabajo, los proyectos, el tiempo y el esfuerzo empleado en ellos.

Realizar un respaldo de datos es sumamente importante pues estos guardarán los activos de relevancia operativa de manera segura, alejados de riesgos de avería de los sistemas y de cualquier amenaza, como por ejemplo un ataque cibernético.

(OpenSys Technologies, 2015) menciona que la gestión de datos copiados es uno de esos términos que parecen tener diferentes significados para diferentes personas. En términos generales, se refiere a un método para la protección de datos que reduce el consumo de almacenamiento mientras hace que los datos sean más fáciles de usar.

Teniendo en cuenta todo lo anterior se continúa con el tema de la investigación; tiempo atrás surgió un problema con la solución de respaldos que tiene la empresa, donde no se pudo respaldar el 100% de la información que se perdió a causa de un ataque cibernético, además de que tardó varias semanas para la recuperación de los archivos, la compañía que es encargada de los respaldos, no verificaba si se realizaban en el tiempo que correspondía.

Contemplando lo que menciona (Luz, 2024) en donde menciona que en un escenario donde la gestión corporativa depende cada vez más de datos relevantes, es imprescindible contar con sistemas eficientes para almacenar información. En este contexto, la seguridad de datos acaba desempeñando un papel crucial.

Mantener los datos seguros y protegidos garantiza que las empresas consigan usar la información de forma estratégica y sigan en conformidad con las leyes de protección de datos de diversos países. No obstante, no todas las empresas entienden la importancia de mantener sus datos seguros. Esto hace que no apliquen buenas prácticas que evitan consecuencias mayores, como la pérdida de datos, penalidades legales e incluso afectar el posicionamiento de la empresa en el mercado.

Es por eso que el departamento de IT local busco implementar una solución con la instalación y configuración de la librería de cintas *Store Ever MSL2024* para evitar estos tipos de problemas y mantener la información respaldada en todo momento, manteniendo la integridad y confidencialidad de los datos, así como la disponibilidad de manera rápida de la información en caso de que la empresa sufra de algún ciberataque o algún error de software.

Existen distintos tipos de respaldos que son utilizados para guardar la información en caso de algún problema de pérdida, dependiendo de las actividades de la empresa es la opción que cada uno de ellos deciden cual es la más óptima.

Copia de respaldo en caliente o copia dinámica (Hot Backup): es una copia efectuada de los datos, aunque estén todavía disponibles para los usuarios y puedan estar siendo actualizados, estas proveen una solución conveniente a un sistema multiusuario porque no requieren sacar a los usuarios del sistema como se requiere en una copia convencional (Quishpe Reynoso, 2007).

Copia de respaldo en frio (Cold backup) también llamada copia de seguridad fuera de línea (*offline backup*): es una copia de seguridad de la base de datos durante la cual la base de datos está fuera de línea y no se puede acceder a la actualización. Esta es la forma más segura de hacer un respaldo porque evita el riesgo de copiar datos que pueden estar en proceso de actualización. Sin embargo, una copia de seguridad en frío implica tiempo de inactividad porque los usuarios no pueden acceder a la base de datos durante el respaldo (Hannan, 2019).

Aparte de si el respaldo se realiza en línea o fuera de línea existen diferentes tipos de backup en función de la cantidad de datos que se copian, ya sea cuando se copian la totalidad de los datos existentes (respaldos totales) o solo una parte de la información (respaldos parciales).

Dentro de los respaldos totales existen 2 tipos, los incrementales también llamados copias evolutivas ya que se realizan partiendo de una copia total y después solo se copian los datos que hayan cambiado desde la copia anterior, teniendo como ventaja la disminución de la cantidad de datos a copiar así como el tiempo que se lleva realizar esta copia, aunque su desventaja es que la restauración de la información es un poco más complicada; también están los respaldos diferenciales que al igual que los incrementales no se guardan todos los archivos, sino solo aquellos que han sido modificados, ignorando el bit de modificación y en su lugar examinan fechas de creación y modificación, es decir se guarda todo lo que haya sido creado y modificado desde la última copia de seguridad completa. (Quishpe Reynoso, 2007).

Ya que se tiene un plan de respaldos lo primero que se debe considerar es el soporte. Entre las características que deben tener los dispositivos que se utilizarán para respaldar los datos se encuentran las siguientes:

- **Confiable**: minimizar las posibilidades de error.

- **Volumen de datos:** tenerlo en cuenta a la hora de elegir el medio destino.
- **Rendimiento:** tiempo de acceso a los datos y velocidad de transferencia.
- **Importancia de los datos**: requerir un medio de resguardo rápido que permita una pronta recuperación.
- **Almacenamiento físico:** El resultado de un respaldo se debe guardar en un lugar seguro.

El almacenamiento de datos por lo general se basa en Cinta, o en Disco, dependiendo de la frecuencia de acceso a los datos requeridos para ser restaurados. Las soluciones basadas en cintas son de mayor utilidad en las empresas a la hora de almacenamiento ya que tienen un gran flujo de información, en el cual reduce los costos a largo plazo, con una gran ventaja por su tamaño ya que son relativamente pequeños con una gran capacidad de almacenamiento, por otra parte, las soluciones basadas de disco son las ideales cuando se ejecutan aplicaciones en tiempo continuo en el cual requieren de un acceso aleatorio a datos rápido y a la vez una recuperación efectiva a la hora de que ocurra algún desastre (Clavijo Bendeck, 2017).

Aunque en la actualidad también existe el respaldo de la información de datos y aplicaciones de los servidores de las empresas en la nube, funcionando igual que las anteriores, en donde se crea una copia de los archivos que tienen los servidores y se guarda en otro servidor que se encuentra fuera del sitio (en el caso de esta investigación era en los Estados Unidos), de acuerdo al problema planteado inicialmente, el respaldo en la nube no era suficiente para lo que la empresa necesitaba, por lo que se decidió implementar una librería de cintas para el respaldo de la información.

METODOLOGÍA

La investigación se enfocó en mejorar el plan de respaldo de la información de los servidores a través de la implementación de una librería de cintas, con el que básicamente se desea respaldar la información para evitar alguna perdida de datos en caso de que en algún momento se tenga algún tipo de ataque de ransomware(software malicioso que bloquea los archivos y pide un rescate por ellos) o un desastre natural, anteriormente la empresa contaba con otro tipo de respaldos como es el comvault, el cual permite proteger los datos y el respaldo de la organización en la nube, este proyecto se realizó con el fin

de beneficiar a los usuarios que diariamente trabajan con archivos e información importante en sus equipos de cómputo, estos archivos son importantes ya que contienen información de la empresa.

Es por eso que el departamento de IT de la empresa se dio a la tarea de planear una solución alterna a la que ya se tenía, realizando la instalación de cintas del HPE StoreEver MSL2024 trabajando en su configuración y administración dentro de una de las plantas del complejo.

Esta investigación es de tipo aplicada porque busca resolver un problema mediante la implementación de una librería de cintas para el respaldo eficiente de la información. Se considera experimental porque medirá el comportamiento de las variables de estudio en el proceso y el respaldo mediante la librería de cintas y determinará las mejoras o desventajas que resulten de la implementación.

La propuesta de proyecto requirió algunos recursos para su instalación, estos componentes de hardware fueron necesarios para continuar con las actividades del proyecto. Es por eso que se realizó una estimación de los posibles gastos que se tuvieron que adquirir. A continuación, se muestra en la tabla 1 el material, las unidades y el costo de cada uno de ellos.

Tabla 1 Recursos para la instalación

Recursos	Unidades	Costo
Tarjeta HBA Q-Logic de 2 puertos y 8GB.	1	$109.00 dlls.
Tarjeta HBA Q-Logic de 16GB de 4GB FC.	1	$419.00 dlls.
Cables de fibra.	2	$36.00 dlls
Unidad de cinta *HPE StoreEver MSL2024.*	1	$2572.00 dlls.
Cintas HPE RW Data Cartridge LTO Ultrium 8-12TB / 30 TB – write-on labels – Green – for StoreEver LTO-8 Ultrium.	16	$955.36 dlls.
Labor	1	$35 dlls / h.

También se enlistan los requisitos que fueron necesarios para la instalación de la biblioteca de cintas *HPE MSL2024,* la lista de estos se muestra iniciando por aquellos requerimientos específicos del lugar donde será instalado.

Requerimientos físicos

Electricidad: Los equipos que se encuentran en el cuarto de telecomunicaciones debieron ser suministrados por un sistema de alimentación ininterrumpida o UPS (Uninterruptible Power Supply) para que siempre se encuentren protegidos y en caso de que la electricidad falle estos no se apaguen y continúen con su funcionamiento normal.

Rack de montaje: Se necesitó contar con un gabinete para el montaje de los servidores, colocados a una distancia de 1.5 metros de la pared, no se deben colocar dos gabinetes seguidos. Algunas de las características del tamaño de estos son 600mm de ancho con un fondo de 600, 800, 900, 1000mm.

Iluminación: La iluminación mínima debió de ser de 450 Lux, considerando que la distancia entre la iluminación y el piso debe ser de 3 metros como mínimo, así como también el color de las paredes tuvo que ser clara, para que ayude a mejorar la iluminación.

Temperatura y humedad: La temperatura y humedad de los cuartos de telecomunicaciones debían respetar un rango relativo, ya que los equipos emiten bastante calor y es por eso que se tuvo que instalar un aire acondicionado en el cuarto o un mini Split para mantener la temperatura ambiente.

Sistema de tierra física: El gabinete tenía de estar conectado al sistema de tierras físicas con una lectura igual o menor a 5 Ohm con referencia a tierra.

Seguridad física

Control de acceso: Los controles de acceso son dispositivos utilizados para la seguridad de las puertas de un lugar en específico, este permite y restringe el acceso al usuario. En el cuarto de telecomunicaciones se incluyó este tipo de control, ya que no cualquiera debería tener autorización para ingresar.

Puerta metálica: El tamaño de la puerta debió ser de 0.90 m como mínimo y se necesitó que fuera metálica, para que en caso de algún incendio, el cuarto de telecomunicaciones este protegido, contando también con un mecanismo de cerrado automático abriendo siempre hacia afuera.

CCTV: El cuarto debía tener cámaras de seguridad con el fin de vigilar quien ingresa y quien sale estando suministradas por un UPS.

Registro de visitantes: También fue necesario tener una bitácora del personal que ingresa al cuarto.

Seguridad lógica

Contraseñas: Las contraseñas debían cumplir con una serie de políticas como son: tener más de 12 caracteres y no exceder de los 16, no incluir nombres o el usuario de la empresa, utilizar símbolos alfanuméricos, no contener espacios y cambiar la contraseña cada 90 días.

Segmentación de red: Solamente los usuarios que forman parte de la empresa deben tener acceso a las redes de la planta, ingresando con su usuario y contraseña.

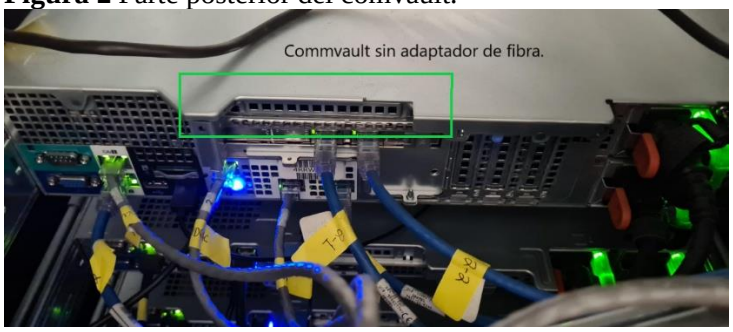
Para comenzar con la instalación de la librería de cintas, en la figura 1 se observa el dispositivo de comvault, este era el encargado de realizar los respaldos antes de que la librería de cintas fuera instalada. Este dispositivo se conectó directamente a la librería de cintas, pero antes de esto se le hicieron algunas configuraciones, como la instalación de un adaptador de bus de host *HPE 853011*, que fue necesario debido a que el dispositivo de la librería tiene conexiones de cables de fibra.

Figura 1 Dispositivo comvault.

Fuente: (Elaboración propia).

En la figura 2 se tiene la parte posterior del dispositivo de comvault, en la parte señalada en verde se observa que el dispositivo no tiene ninguna conexión para los cables de fibra, así que, fue necesario hacer la instalación del adaptador, ya que sin este, no sería posible la conexión entre el comvault y la librería de cintas.

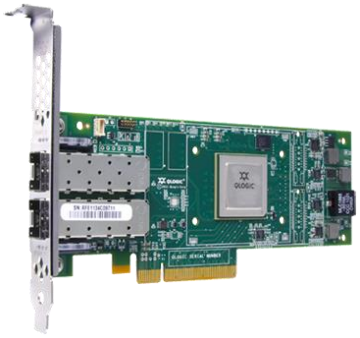
Figura 2 Parte posterior del comvault.



Fuente: (Elaboración propia).

A continuación, se muestra en la figura 3 el modelo de la tarjeta o adaptador para la conexión de los cables de fibra que fueron comprados para poder instalarlos y seguir con la instalación de la librería.

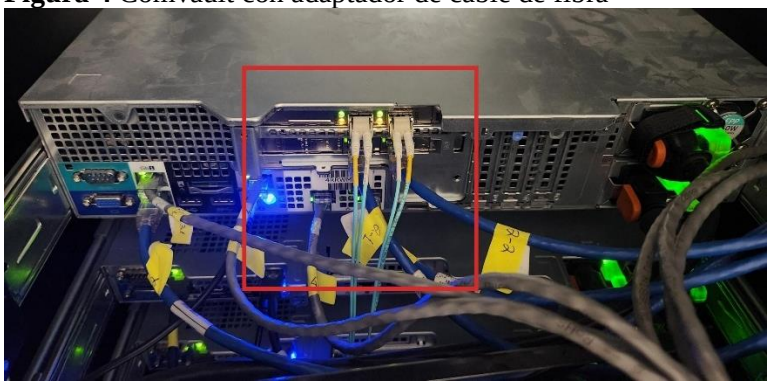
Figura 3 Adaptador de entradas de fibra



Fuente: (Elaboración propia).

En la figura 4 se observa que el adaptador de los cables de fibra ya fue instalado al igual que los cables, y se pudo continuar con la instalación de la librería, haciendo posible la conexión entre los dos dispositivos. Es importante mencionar que para hacer la instalación del adaptador, el comvault debe apagarse, una vez apagado se puede abrir e instalar la tarjeta, ya instalada se puede hacer la conexión de los cables de fibra.

Figura 4 Comvault con adaptador de cable de fibra



Fuente: (Elaboración propia).

Para continuar con el proceso del proyecto, el modelo del dispositivo que fue utilizado es un *HPE StoreEver MSL2024,* permitiendo realizar la configuración y administración desde otra ubicación, no es necesario encontrarse en el sitio para administrarlo, puede ser configurado remotamente desde el sitio web de *HPE.*

Estos dispositivos administran fácilmente sus medios dentro o fuera de la librería de cintas y varios cargadores extraíbles de 12 ranuras, así mismo, proporcionan una amplia gama de puntos de capacidad de 9.6 TB a 1440 TB de capacidad de almacenamiento comprimido.

Las características de la librería de cintas son:

- Gestión remota desde la página web de *HPE* utilizando el command view para las librerías de cintas.
- Lector de barras integrado.
- Cambio de unidades de cintas sin necesidad de herramientas.
- Compatibilidad de sistema operativo y software.
- Ofrece el más alto nivel de seguridad de encriptación para proteger la información.

En la figura 5 se puede observar que el modelo instalado es el *StoreEver MSL 2024 Tape Library,* es importante conocer el modelo ya que se puede tener una configuración parecida a otros, de tal manera que si no se configura correctamente no funciona.

Figura 5 Modelo de la librería de cintas.

Fuente: (Elaboración propia).

A continuación, en la figura 6 se tiene la parte posterior del dispositivo de la librería, en donde se visualizan las entradas de conexión con las que cuenta. La tecnología de este sistema es LTO-8, la cual permite que las unidades de cintas ajusten su velocidad de forma continua, manteniendo la transmisión por secuencias y optimizar el rendimiento, a la vez que se reducen los inicios/paradas para aumentar significativamente la fiabilidad de las unidades.

Figura 6 Parte posterior de la librería de cintas

Fuente: (Elaboración propia).

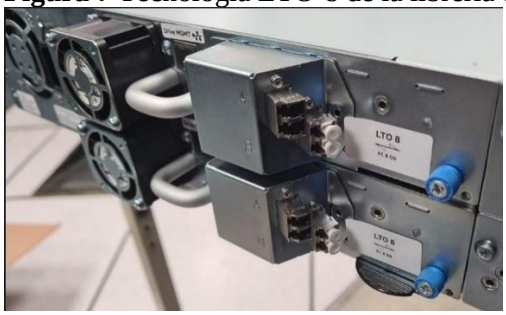
Algunas de las características del dispositivo de la librería son las que se muestran en la tabla 2, donde se menciona la tecnología que utiliza, en este caso es la tecnología LTO-8 Ultrium 45000, se menciona el número de unidades, la capacidad máxima que soporta, la transferencia de datos y la interfaz de la unidad de canal de fibra, esto con el fin de conocer un poco más de cómo funciona la unidad de almacenamiento.

Tabla 2 Características de la librería de cintas.

Características del MSL2024	
Tecnología de accionamiento compatible	LTO-9 Ultrium 45000. LTO-8 Ultrium 45000. LTO-7 Ultrium 45000. LTO-6 Ultrium 45000.
Número máximo de unidades	2
Capacidad máxima	1,08 PB (LTO-9 / 24 Ranuras).
Transferencia máxima de datos	2.6 TB/h (2 Unidades LTO-9)
Interfaz de unidad de canal de fibra nativo.	Canal de fibra nativo de 8GB. SAS de 12Gb/s (LTO-9) SAS de 6Gb/s (LTO-8)

En la figura 7 se observan las entradas de la tecnología LTO-8 que tiene la librería de cintas, es aquí donde se hizo la conexión de la fibra que va conectada directo al comvault.

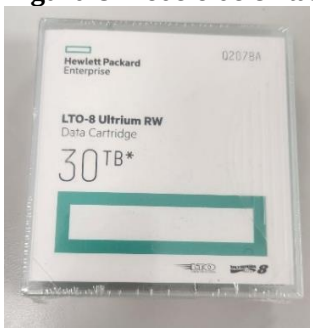
Figura 7 Tecnología LTO-8 de la librería de cintas.



Fuente: (Elaboración propia).

El modelo de las cintas que fueron instaladas en la librería son las que se muestran en la figura 8, se instalaron 24 cintas de 30TB cada una, y se hizo la compra de las cintas faltantes para cubrir el respaldo de un año completo, así de esta manera, cuando sea necesario cambiar una de las cintas, se tiene la respuesta en el sitio y se realiza el cambio.

Figura 8 Modelo de cintas para la librería.



Fuente: (Elaboración propia).

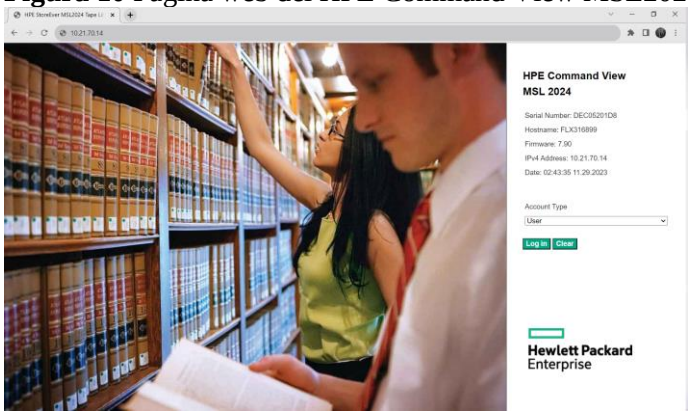
Para iniciar con la configuración de la librería de cintas fue necesario conectarse desde la página web, ya que no permitiría entrar remotamente porque no tiene configurada la IP y fue necesario conectarlo directo al dispositivo como se muestra en la figura 9 donde se conecta la computadora por medio del cable Ethernet.

Figura 9 Conexión a la librería de cintas.

Fuente: (Elaboración propia).

A continuación, se observa la pantalla inicial para el acceso a la plataforma de la administración y configuración de la librería de cintas en la figura 10. En el tipo de usuario se ingresa como administrador, ya que es el que permitirá realizar las configuraciones necesarias.

Figura 10 Página web del HPE Command View MSL2024.



Fuente: (Elaboración propia).

Una vez ingresando el usuario y la contraseña de administrador, aparece la pantalla con los datos de la librería en la figura 11, los cuales pueden servir para configuraciones en un futuro o para la misma configuración, en caso de que se tenga que actualizar.

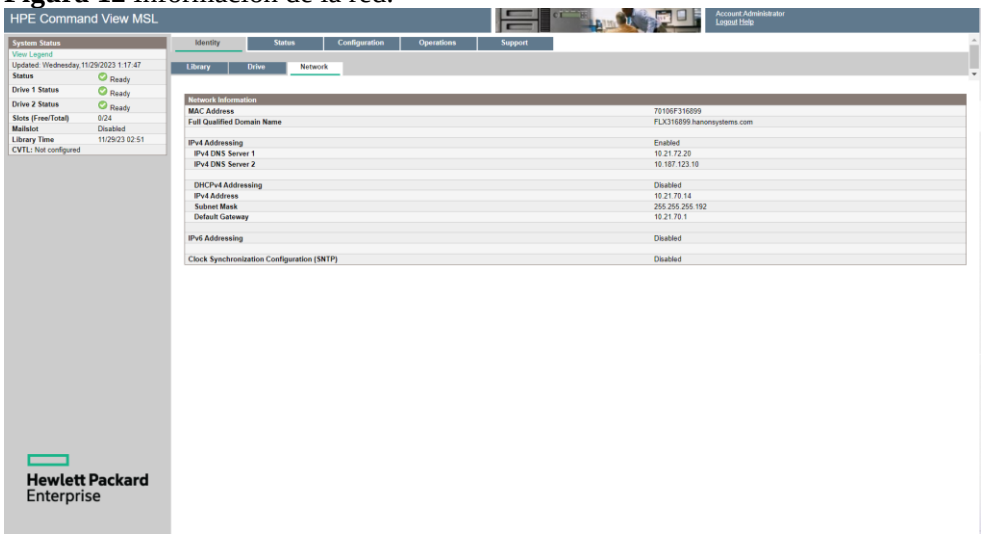
Figura 11 Información de la librería de cintas.

Fuente: (Elaboración propia).

A continuación, se realizó la configuración de la librería, en esta parte se le asignó una IP al dispositivo, un nombre al host, nombre de dominio, se configuró solamente el protocolo IPv4, se habilitó el HTTPS para poner a disposición la transferencia de datos y se activó el acceso restringido a la red. En la figura 12 se encuentra la información de la red como son, la dirección MAC (siglas en inglés de Medium Access Control) que tiene asignado, la IP, la máscara y el Gateway. En este caso los datos de este dispositivo son:

- *IP: 10.21.72.20*
- *Gateway: 10.21.70.1*
- *Mascara: 255.255.255.192*

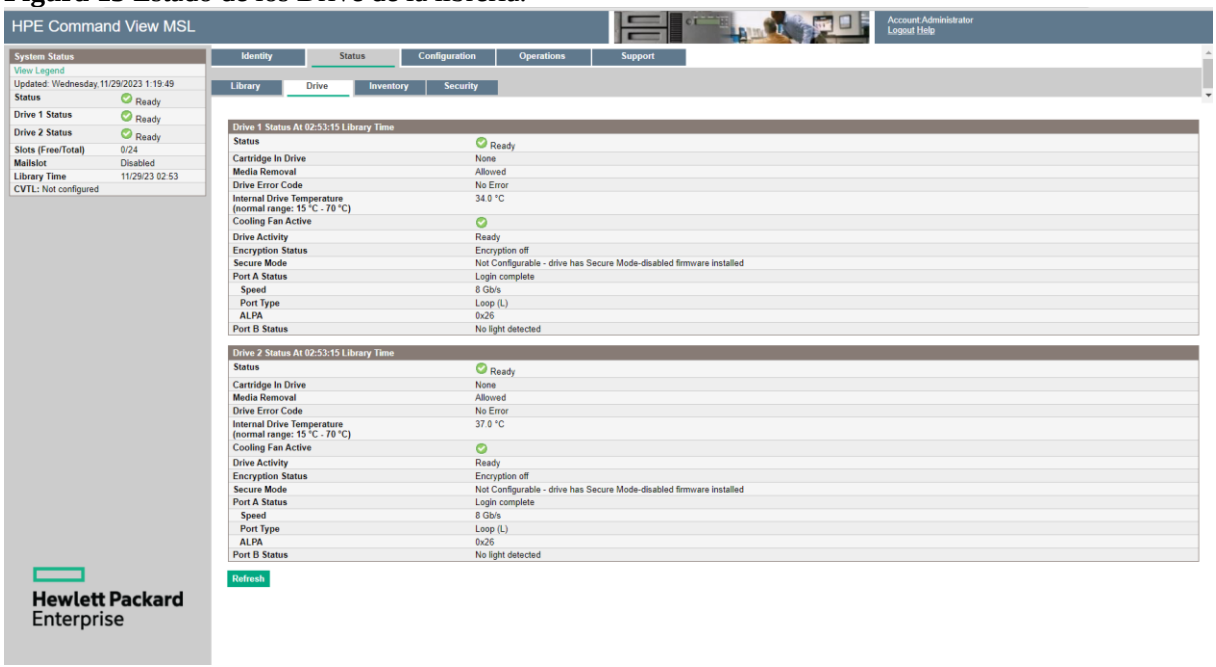
Figura 12 Información de la red.



Fuente: (Elaboración propia).

Continuando, con el proceso de la configuración en la Figura 13 se ubica la información y el status del drive de la librería. Si el estado está en verde significa que está funcionando correctamente, si está con una x la unidad tiene una falla, y si tiene el signo de advertencia quiere decir que está funcionando, pero posiblemente tenga una falla.

Figura 13 Estado de los Drive de la librería.



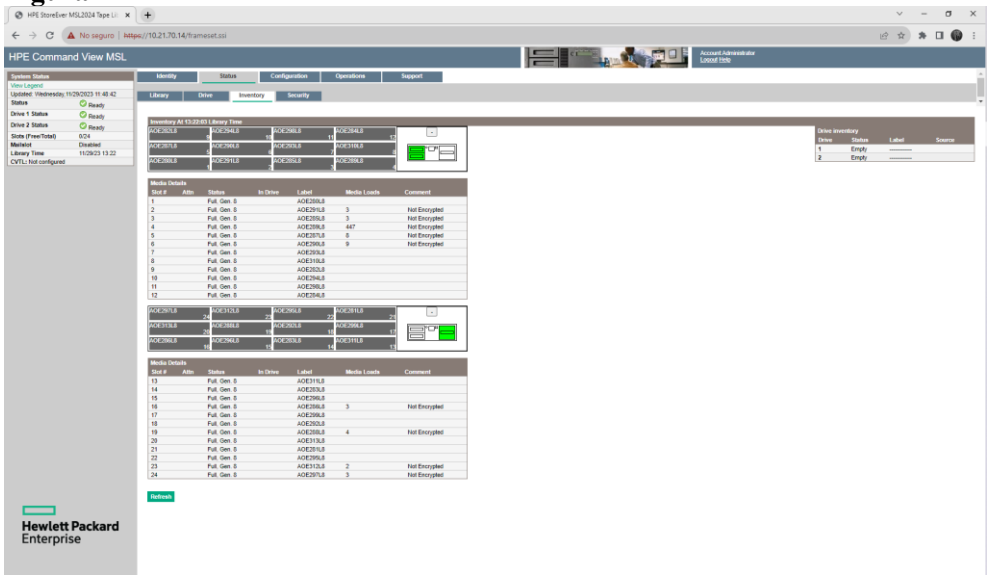
Fuente: (Elaboración propia).

En la figura 14 se muestra la página donde se encuentra información más detalladamente de los cartuchos de las cintas de unidades. Un rectángulo de color oscuro indica una ranura llena, un rectángulo rojo indica un cartucho con problemas y un rectángulo blanco indica una ranura vacía.

También es posible ver la información de las cintas como es:

- Número de ranuras. Enumero la “ranura” o el número de índice de cada ranura en el cargador de menor a mayor.
- Estado: Lleno o vacío al igual que la generación LTO (formato de cinta de almacenamiento de datos Linear Tape-Open) de la cinta.
- Etiqueta: Se muestran los datos de la etiqueta del código de barras de la cinta en ranura.
- Carga de medio: Es la cantidad de veces que la cinta se ha cargado en una unidad durante su vida útil.
- Comentarios: Son utilizados para agregar cualquier información adicional sobre la cinta.

Figura 14 Estado de las cintas.



Fuente: (Elaboración propia).

Por último, se observa en la figura 15 la librería de cintas en estado listo, esto significa que todo está correcto y está lista para realizar las copias de los respaldos del comvault. Para confirmar que esté funcionando correctamente ya que no mostró ningún error, se realizó el respaldo de la información para verificar su funcionamiento.

Figura 15 Librería de cintas correctamente funcionando.

Fuente: (Elaboración propia).

En la figura 16 se muestran los dispositivos que tiene conectado el comvault, los que se encuentran en color amarillo son los de la librería de cintas, así se observó que el comvault ya reconocía la librería, de esta manera se pudo confirmar que el dispositivo estaba funcionado y fue configurado correctamente.

Figura 16 Verificación de librería de cintas.

```
[root@mxpdnmasp01 /]# lsscsi
[0:2:0:0]    disk    DELL     PERC H730 Mini   4.26  /dev/sda
[0:2:1:0]    disk    DELL     PERC H730 Mini   4.26  /dev/sdb
[10:0:0:0]   cd/dvd  HL-DT-ST DVD-ROM DTA0N    D3C0  /dev/sr0
[11:0:0:0]   tape    HPE      Ultrium 8-SCSI   M571  /dev/st1
[12:0:0:0]   tape    HPE      Ultrium 8-SCSI   M571  /dev/st0
[12:0:0:1]   mediumx HP       MSL G3 Series    7.20  /dev/sch0
[13:0:0:0]   disk    EQLOGIC  100E-00          10.0  /dev/sdc
[14:0:0:0]   disk    EQLOGIC  100E-00          10.0  /dev/sdd
[15:0:0:0]   disk    EQLOGIC  100E-00          10.0  /dev/sde
[16:0:0:0]   disk    EQLOGIC  100E-00          10.0  /dev/sdf
[17:0:0:0]   disk    EQLOGIC  100E-00          10.0  /dev/sdg
[18:0:0:0]   disk    EQLOGIC  100E-00          10.0  /dev/sdh
[19:0:0:0]   disk    EQLOGIC  100E-00          10.0  /dev/sdi
[root@mxpdnmasp01 /]#
```

Fuente: (Elaboración propia).

En la imagen 17 se observan todos los dispositivos instalados correctamente en el rack, una vez que ya se comprobó el correcto funcionamiento de los dispositivos, el proyecto se finalizó con éxito.

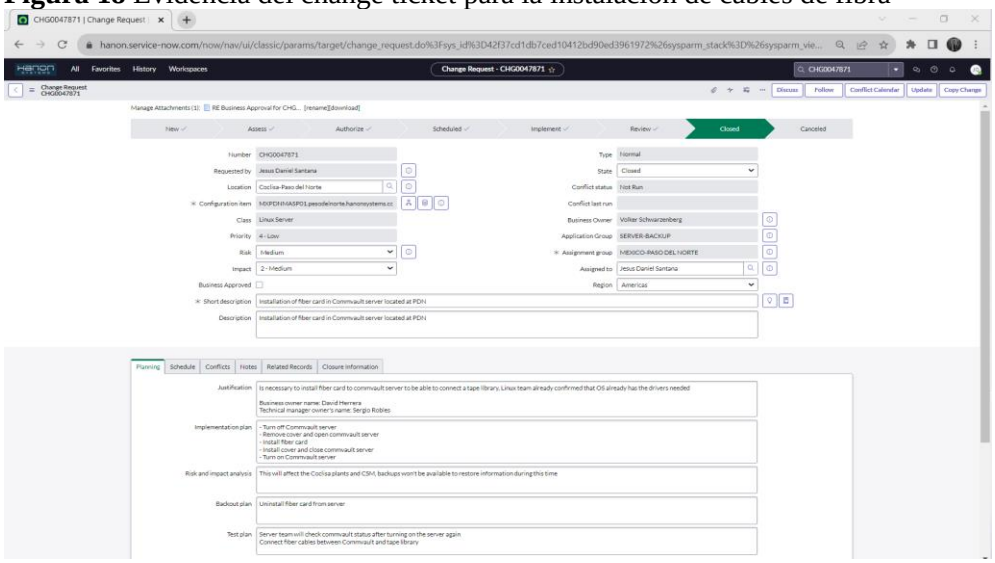
Figura 17 Dispositivos conectados.

Fuente: (Elaboración propia

Siguiendo las recomendaciones de la Librería de Infraestructura de Tecnologías de información (ITIL), se realizó la instalación y puesta en marcha del StoreEver MSL Tape Library de acuerdo a los estándares establecidos para el control de cambios por medio de una solicitud del sistema de gestión Service Now, en el cual se solicitó a los grupos de soporte de segundo nivel la instalación de la conexión entre el sistema comvault y la librería de cintas, así como también la solicitud para configurar una VLAN (virtual local area network por sus siglas en inglés) específica para la operación de la librería de cintas en el ambiente de la red local.

Para la instalación de los cables de fibra fue necesario realizar un change ticket mostrado en la figura 18 para realizar la configuración en el comvault una vez que ya estuviera conectada a la librería, y realizar la conexión entre los dos dispositivos.

Figura 18 Evidencia del change ticket para la instalación de cables de fibra



Fuente: (Elaboración propia).

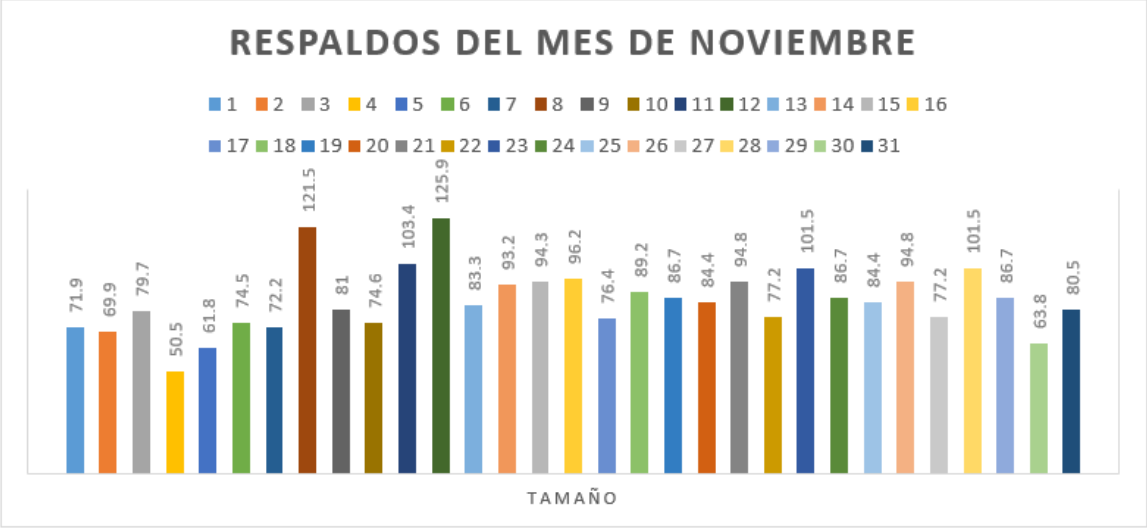
Almacenamiento fuera de sitio

Para el almacenamiento de las cintas fue necesario encontrar un lugar seguro ya que estas deben estar fuera del sitio donde se encuentran los servidores, es por eso que las cintas de los respaldos se guardaron en una caja fuerte en otra planta de la empresa en donde solo personal autorizado tiene acceso a ella, teniendo en cuenta que las cintas debían estar a una temperatura y humedad ambiente. Es por eso que se planeó que cada vez que la cinta tenga que ser cambiada en el dispositivo, se debe guardar en la caja fuerte y el personal que este de soporte en la planta donde se encuentran los servidores será el encargado de retirar las cintas y cambiarla, así mismo llevarla a la planta donde se estarán guardando las cintas.

RESULTADOS

En la figura 19 se puede observar un gráfico de los respaldos de un mes en particular, cada columna en la gráfica es un día del mes y el tamaño de los archivos que se respaldaron ese día, cumpliendo con los objetivos y metas los respaldos se realizaron a diario, respaldando el 100% de la información de los servidores. El tipo de respaldo que se utilizó es un respaldo incremental y completo, esto quiere decir que todos aquellos archivos que son modificados en un día son los que realizan la copia de estos.

Figura 19 Datos de los respaldos



Fuente: Propiedad de la empresa

En la figura 20 se puede observar el nombre de los servidores que son respaldados y cuando fue el último respaldo que se realizó. Este tipo de reportes se envían por correo al personal de IT, para poder verificar que el dispositivo esté funcionando correctamente y los respaldos se estén realizando cuando debe de ser.

Figura 20 Datos de los respaldos

Last Backup Time (1/1)

Device name	Task Name	Idle since
10.218.152.195	PDNPD012data	125 days ago
PDNPD017	PDNPD017	Past 24 hours
PDNPD012	PDNPD012	Past 24 hours
PDNPD025	PDNPD025 - TRESS	Past 24 hours
PDNPD020	PDNPD020 - HMES Primary	Past 24 hours
PDNPD014	PDNPD014	Past 24 hours
PDNPD016	PDNPD016	Past 24 hours
PDNPD026	PDNPD026 - TRESS SEC	Past 24 hours
PDNPD015	PDNPD015	Past 24 hours
CSFPD012	CSFPD012	Past 24 hours
PDNPD021	PDNPD021 - HMES Secondary	Past 24 hours
CSLPD012	CSLPD012	Past 24 hours

Fuente: Propiedad de la empresa.

Finalizando el proceso de la instalación y la configuración de la librería de cintas, se realizaron los reportes de los respaldos del servidor, en el funcionamiento de este proceso el servidor del Vmware y el MSA están conectados entre sí, por otro lado se tiene el Equalogic donde se administra toda esta información y el comvault realiza el respaldo de esta, por último la librería de cintas realiza una copia de la información que se respaldó en el comvault, así obtiene el respaldo de este servidor que ya ha respaldado todo.

CONCLUSIÓN Y DISCUSIÓN

Esta investigación buscaba realizar un respaldo de la información localmente mediante la instalación y configuración de una librería de cintas una vez finalizando el proyecto, el propósito y los objetivos del proyecto se cumplieron, en el proceso de la instalación y configuración de la librería se tuvieron algunas complicaciones, ya que cuando se realizó la instalación del cable de fibra en el comvault y se conectó con la librería de cintas, al momento de configurarla marcaba un error dentro de unos del drive, se tuvo que realizar un cambio de IP y de la VLAN a la que estaba conectado para verificar si se solucionaba el error, es por esto que se realizó la actualización del firmware de la Liberia, pero el error se encontraba dentro del drive, por lo que se solicitó la garantía de este para que se pudiera resolver el problema y así continuar con el proceso.

La implementación del dispositivo fue de gran utilidad para la empresa, ya que de esta forma se mantuvo la información respaldada y se mantiene disponible cuando el usuario la necesita.

Como recomendaciones, para conseguir un buen funcionamiento de la librería de cintas, se debe verificar cada cierto tiempo que esté funcionando correctamente, mantener el firmware actualizado cada que se tenga una actualización. Se recomienda realizar un plan de contingencia en la empresa, para en caso de que sea necesario y ocurra alguna emergencia se tenga un protocolo de lo que se tiene que realizar, este debe estar realizado conforme a los análisis de riesgos que existen, las estrategias de recuperación, como se desarrollaran estas estrategias y procedimientos.

REFERENCIAS BIBLIOGRÁFICAS

ISO/IEC 27000. (2016). Obtenido de Information technology–Security techniques–Information security management systems–Overview and : https://www.iso.org/standard/66435.html

Briceño, E. V. (Marzo de 2021). Seguridad de la informacion. Obtenido de https://3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf

Clavijo Bendeck, W. J. (2017). Universidad Nacional Abierta y a Distancia UNAD . Obtenido de Definición e implementación de un sistema de almacenamiento y respaldo de datos e información seguro para el Servicio Geológico Colombiano –SGC- sede CAN: https://repository.unad.edu.co/handle/10596/14382

Comillas Universidad Pontificia. (8 de Mayo de 2023). Obtenido de Confidencialidad, Integridad y Disponibilidad: https://ciberseguridad.comillas.edu/confidentiality-integrity-and-availability/

Duque, F. J. (Agosto de 2021). Universidad Nacional de Colombia. Obtenido de Sistema de Gestion de seguridad de la informacion: http://www.fadmon.unal.edu.co/fileadmin/user_upload/extension/cursos/imagenes_cursos/digitales_septiembre/sistema_de_gestion_de_seguridad-1.pdf

FORTINET. (2025). Obtenido de Tríada CIA: confidencialidad, integridad y disponibilidad: https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

FORTRA. (17 de mayo de 2021). Obtenido de ¿Qué es la Seguridad de la Información?: https://www.fortra.com/es/blog/que-es-la-seguridad-de-la-informacion

Hannan, E. (diciembre de 2019). ComputerWeekly.es. Obtenido de Respaldo en frío o respaldo fuera de línea: https://www.computerweekly.com/es/definicion/Respaldo-en-frio-o-respaldo-fuera-de-linea

INCIB CHILE. (22 de Octubre de 2021). Obtenido de La triada de la seguridad de información “CID”: https://incibchile.cl/triada-seguridad-informacion/

Luz, F. C. (27 de 11 de 2024). La importancia del almacenamiento y la seguridad de datos. Obtenido de https://cbltech.mx/blog/la-importancia-del-almacenamiento-y-la-seguridad-de-datos/

OpenSys Technologies. (29 de julio de 2015). Obtenido de ¿Qué es la gestión de datos copiados, y en qué se diferencia del respaldo tradicional?: https://opensys-mexico.blogspot.com/2015/06/que-es-la-gestion-de-datos-copiados-y.html

Oracle. (2016). StorageTek Enterprise Library Software Guía de gestión de datos fuera del sitio y recuperación ante desastres. Obtenido de https://docs.oracle.com/cd/E65192_01/ELSDR/drintro.htm#CHDEEEBD

Patalano, S. (2022). INTERBEL. Obtenido de Email & Ciberseguridad: https://www.interbel.es/blog/triada-cid/

Quintana, M. D. (28 de mayo de 2024). Respaldo de datos: qué es, tipos y qué información respaldar. Obtenido de https://www.servnet.mx/blog/respaldo-de-datos

Quishpe Reynoso, V. P. (Septiembre de 2007). Obtenido de

https://bibdigital.epn.edu.ec/bitstream/15000/1475/1/CD-0990.pdf

Solleiro, J. L. (01 de Junio de 2022). Universidad Nacional Autonoma de Mexico. Obtenido de https://www.icat.unam.mx/wp-content/uploads/2022/09/Vigilancia_Tecnologica_en_Ciberseguridad_Boletin.pdf