UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE INGENIERÍA DE SISTEMAS

DISEÑO DE UNA METODOLOGÍA PARA EL RESPALDO Y REPLICACIÓN DE SERVIDORES

Trabajo de titulación previo a la obtención del
Título de Ingenieros de Sistemas

AUTORES: EDISON SANTIAGO CRUZ LEMA

ERICK DANIEL NARANJO MENDOZA

TUTOR: MANUEL RAFAEL JAYA DUCHE

Quito – Ecuador

2025

CERTIFICADO DE RESPONSABILIDAD Y AUDITORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, Edison Santiago Cruz Lema con documento de identificación N°1724420383; y Erick Daniel Naranjo Mendoza con documento de identificación N°1725032781; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 7 de agosto de 2025

Atentamente,

Edison Santiago Cruz Lema
1724420383

Erick Daniel Naranjo Mendoza
1725032781

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Nosotros, Edison Santiago Cruz Lema con documento de identificación N° 1724420383; y Erick Daniel Naranjo Mendoza con documento de identificación N.° 1725032781, expresamos nuestra voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Proyecto Técnico: "Diseño de una metodología para el respaldo y replicación de servidores", el cual ha sido desarrollado para optar por el título de: Ingenieros de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 7 de agosto de 2025

Atentamente,

Edison Santiago Cruz Lema
1724420383

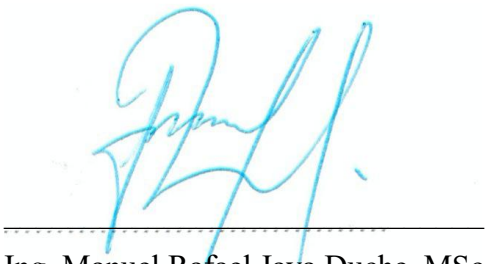
Erick Daniel Naranjo Mendoza
1725032781

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Manuel Rafael Jaya Duche con documento de identificación N°1710631035, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: DISEÑO DE UNA METODOLOGÍA PARA EL RESPALDO Y REPLICACIÓN DE SERVIDORES, realizado por Edison Santiago Cruz Lema con documento de identificación N°1724420383 y Erick Daniel Naranjo Mendoza con documento de identificación N°1725032781 respectivamente, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 7 de agosto de 2025

Atentamente,



Ing. Manuel Rafael Jaya Duche, MSc.
1710631035

DEDICATORIA

Dedico este trabajo para la mujer que me dio la vida: Patricia Lema. Su cariño y apoyo incondicional han sido mi mayor inspiración al igual que el de mis hermanos Erick Vásconez y Ruby Vásconez. Sin su guía y aliento constante, este logro no habría sido posible.

A mi hijo, Ezequiel Cruz, por ser mi inspiración diaria y recordarme la importancia de luchar por mis sueños.

A mi abuelita, Marita Lema, cuyos sacrificios y enseñanzas han sido fundamentales en mi formación.

Y a toda mi familia y amigos que han estado a mi lado durante este viaje, por su amistad y apoyo constante.

Santiago Cruz

Dedico este trabajo a quienes han sido el corazón de mi esfuerzo y motivación.

A mi madre, María Mendoza, por ser ejemplo de fortaleza, entrega y compromiso. Su presencia ha sido una fuente constante de aliento en cada etapa de mi vida.

A mi padre, Milton Naranjo, por su sabiduría, consejos y por impulsarme siempre a dar lo mejor de mí.

A Gabriela Delgado, mi compañera de vida, por caminar a mi lado con paciencia, cariño y fe en lo que somos capaces de construir juntos.

Erick Naranjo

AGRADECIMIENTO

Extiendo mi más sincero agradecimiento a todas las personas que, de manera directa o indirecta, contribuyeron al desarrollo de este trabajo de titulación. En particular, expreso un especial reconocimiento al Ing. Rafael Jaya, cuya orientación, compromiso y constante apoyo fueron fundamentales en cada etapa del proceso.

A mi familia, en especial a mi madre, Patricia Lema, por su amor incondicional, comprensión y por ser mi principal fuente de fortaleza y motivación a lo largo de este proceso. Finalmente, agradezco a Dios por concedernos la sabiduría y la fortaleza necesarias para culminar satisfactoriamente este proyecto.

Santiago Cruz

Este trabajo no habría sido posible sin el apoyo y acompañamiento de personas muy importantes en mi vida, a quienes quiero agradecer profundamente.

Mi gratitud al Ing. Rafael Jaya, por su orientación clara, su compromiso y por brindarme siempre su tiempo y conocimientos durante el desarrollo de esta tesis.

A mis padres, María Mendoza y Milton Naranjo, gracias por su ejemplo, su cariño y por creer en mí en cada etapa de este camino.

A Gabriela Delgado, mi prometida, por estar a mi lado con paciencia, ánimo y confianza en cada momento, incluso en los más exigentes.

Erick Naranjo

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente trabajo de titulación se enfoca en el diseño de una solución orientada al respaldo y replicación de servidores, con el fin de garantizar la disponibilidad y continuidad de los servicios ante posibles fallos o interrupciones, el objetivo es establecer una metodología que asegure la integridad de los datos y disponibilidad en el caso de los diferentes efectos secundarios que puedan suscitarse que ocasionen una pérdida de datos, lo cual posibilita una recuperación segura y puntual de la información. Para el desarrollo del proyecto, se ha propuesto dos tipos de metodología; la primera estructurada para respaldar servidores y la segunda para replicarlos, a través de la herramienta Veeam Backup & Replication; este diseño se lo realizo en el primer caso a través de 7 etapas (evaluación inicial, implementación de Veeam Backup & Replication, configuración de las tareas de respaldo, almacenamiento y gestión de respaldo, recuperación ante desastres, monitoreo y reportes, mantenimiento y actualización); y para el segundo caso a través de 5 etapas (evaluación inicial y planificación, instalación y configuración de Veeam Backup & Replication, configuración de replicación de máquinas virtuales, configuración de la recuperación automática y failover, mantenimiento y actualización). Es importante tener en cuenta que la funcionalidad del proyecto se ha confirmado utilizando una prueba de concepto real completamente operativa, obteniendo como resultados que la copia de seguridad fue realizada en dos minutos cuarenta y dos segundos (02:42), procesó 50 GB y transfirió 7.7 GB; y el trabajo de replicación tuvo una duración de cinco minutos treinta y ocho segundos (05:38), procesó 50GB y transfirió 11.7GB. Se concluye que a través de las pruebas realizadas se ha demostrado la idoneidad y eficacia de las herramientas seleccionadas, confirmando que cumplen con los requisitos y expectativas del proyecto.

Palabras clave: eficacia, metodología, recuperación, replicación, respaldo.

ABSTRACT

The current degree work focuses on designing a solution for server backup and replication, the objective is to establish a methodology that ensures the integrity of the data and availability in the case of the different side effects that may occur that result in data loss, allowing for reliable and timely recovery. For the development of the project, two types of methodology have been proposed; the first structured to backup servers and the second to replicate them, through the Veeam Backup & Replication tool; This design was carried out in the first case through 7 stages (initial evaluation, implementation of Veeam Backup & Replication, configuration of backup tasks, storage and backup management, disaster recovery, monitoring and reporting, maintenance and updating); and for the second case through 5 stages (initial evaluation and planning, installation and configuration of Veeam Backup & Replication, configuration of virtual machine replication, configuration of automatic recovery and failover, maintenance and update). It is important to note that the functionality of the project has been confirmed using a fully operational real proof of concept, obtaining as results that the backup was performed in two minutes forty-two seconds (02:42), processed 50 GB and transferred 7.7 GB; and the replication job lasted five minutes thirty-eight seconds (05:38), processed 50GB and transferred 11.7GB. It is concluded that through the tests carried out, the suitability and effectiveness of the selected tools have been demonstrated, confirming that they meet the requirements and expectations of the project.

Keywords: efficacy, methodology, recovery, replication, backup.

CAPÍTULO I

ANTECEDENTES Y GENERALIDADES

1.1 INTRODUCCIÓN

Las tecnologías de la información y la comunicación (TIC) utilizadas por las organizaciones atraviesan un proceso continuo de transformación y mejora. En este contexto, resguardar la información generada por una entidad constituye una responsabilidad crucial para los equipos encargados de la gestión tecnológica. En sus inicios, esta labor se realizaba de manera rudimentaria, con escasos niveles de automatización y confiabilidad. Entre las prácticas habituales de respaldo se incluía la transferencia de datos a dispositivos como discos externos, memorias USB o cintas magnéticas, como medida indispensable para garantizar la preservación de la información.

Sin embargo, este tipo de soluciones se convierten por sí mismas en un problema para las organizaciones modernas por sus limitaciones y escasas garantías al momento de la recuperación, y no son aplicables para empresas grandes las cuales incluyen cientos de máquinas virtuales y máquinas de usuarios finales que necesitan ser respaldadas (Chango y otros, 2017).

En la actualidad empresas, colegios, universidades, corporaciones, importadoras, etc., se encuentran bajo la presión de ofrecer sus servicios ya sea a través de internet o por medio de su propia intranet, lo que ha ocasionado sin tomar en cuenta la dimensión de la organización que estás produzcan una cantidad excesiva de información delicada e importante la cual indiscutiblemente debe ser resguardada.

Debido a estas opciones de acceso a internet las herramientas tecnológicas como servicio tienen una alta demanda, Por esta razón, resulta fundamental que la empresa cuente con un plan de recuperación ante desastres, el cual asegure la continuidad operativa de los servicios ante cualquier eventualidad.

Para cumplir con estos estándares las diferentes organizaciones están implementando metodologías para el respaldo y replicación de servidores con el fin de tener un plan emergente de recuperación ante posibles fallas.

Las diferentes metodologías de respaldo y replicación de servidores se han convertido en la última línea de defensa de una organización, cuando los controles han fallado, el sistema de copias de seguridad, restauración y replicación de datos es el control final, que puede prevenir eventos drásticos, pérdidas de información, paralización de operaciones e incluso el fracaso de una organización.

(Cajamarca, 2019) señala que: cualquier incidente de paralización de servicios o pérdida de información de una empresa provoca alarmas en las organizaciones afectando no solo a los bienes tangibles de las instituciones sino también a la imagen corporativa de esta, lo que ocasiona grandes pérdidas económicas debido a la indisponibilidad de los servicios. En consecuencia, disponer de un sistema de recuperación ante desastres permite a la organización minimizar tanto el tiempo de interrupción de los servicios tecnológicos como la pérdida de información, facilitando una restauración eficiente y estructurada tras una eventual contingencia.

Debido a lo explicado anteriormente el objetivo del presente proyecto investigativo es diseñar una metodología para el respaldo y replicación de servidores, y de esta manera garantizar que la información de las organizaciones esté debidamente resguardada ante las amenazas que puedan presentarse y de esta forma minimizar el período sin actividad tecnológica y el daño a la información con una restauración veloz y estructurada tras un siniestro.

El proyecto de titulación se ha estructurado de la siguiente manera: Primeramente, se determina el principal problema, sus causas y posibles soluciones, en el próximo capítulo se establece la meta principal del proyecto y las metas específicas, mediante las cuales se llega a la solución del problema. A continuación, se lleva a cabo un análisis bibliográfico orientado a

establecer las definiciones y fundamentos teóricos esenciales que sustentan el desarrollo del presente proyecto. Posteriormente se describe el marco metodológico en donde se presentan los recursos y técnicas empleadas para llevar a cabo el proyecto, en la próxima sección de resultados se expone el procedimiento llevado a cabo en cinco etapas: Evaluación de la situación presente.; Definir los procedimientos más adecuados que se adapten al caso de estudio; Análisis comparativo de los diferentes software de respaldo y replicación de servidores; Diseño de la solución (metodología); Experimentación en un escenario de pruebas. Finalmente, en el último capítulo se detallan las conclusiones y recomendaciones generales conseguidas una vez terminado el trabajo investigativo.

1.2 ANTECEDENTES

A nivel mundial se han realizado numerosos estudios principalmente por parte de las industrias tecnológicas como Veeam y Vmware, sobre los desafíos que enfrentan las entidades al no ser capaces de recuperarse de catástrofes naturales o de naturaleza informática, conociendo que en la actualidad dependemos cada vez mas de estas tecnologías y cualquier incidente traen consigo daños graves (Cajamarca, 2019).

A lo largo de su historia, la mayoría de las organizaciones han enfrentado incidentes que generan la pérdida de datos y la interrupción de aplicaciones o servicios, ocasionados por fallos de hardware, errores de software, problemas eléctricos o factores humanos. Estas situaciones pueden derivar en extensos periodos de inactividad, afectando gravemente la productividad. Además de las pérdidas económicas, este tipo de eventos repercute negativamente en la imagen institucional, debilitando la confianza de los usuarios y motivando su migración hacia proveedores alternativos. El desafío no solo radica en la pérdida de datos, sino también en el tiempo que se necesita para reiniciar la producción de sus servicios con la mínima repercusión posible (Cajamarca, 2019).

En América Latina, menos del 50% de las organizaciones han introducido un plan de eliminación de desastres, y la mayoría de ellas se basan únicamente en copias de seguridad y no introducen métodos de restauración de servicios a otro centro de datos (Hernández, 2021).

En el contexto ecuatoriano, no se dispone de una normativa de aplicación general que exija a las organizaciones la implementación obligatoria de planes de recuperación ante desastres. No obstante, las entidades del sector financiero, especialmente las instituciones bancarias, sí están sujetas a regulaciones específicas establecidas por la Superintendencia de Bancos.

Importadora Luna tiene más de 20 años de trayectoria en ecuador, se dedican a la importación de repuestos automotrices en el mercado nacional e internacional, el sistema de respaldo de la Importadora mencionada no se encuentra automatizada actualmente, dado que hay procesos que se realizan de forma manual, podemos, por ejemplo, mencionar el respaldo de los servidores. Esto puede ocasionar deficiencias en cuanto a seguridad, ya que se comprometen tanto la integridad de los datos como la confiabilidad de los sistemas de información, lo que puede estar equivocado, aumentando las copias de seguridad obsoletas en el momento de la determinación, ya sea natural o causada por una persona.

1.3 PROBLEMÁTICA

En la actualidad, la mayoría de las organizaciones carecen de un sistema de respaldo y replicación optimizado; y cuando disponen de uno, en muchos casos este no se encuentra implementado de manera adecuada, lo que compromete la eficiencia y seguridad de la gestión de la información, debido a que para conseguirlo se necesita un estudio anterior que se base principalmente en la necesidad particular de cada situación, por este motivo el presente trabajo de investigación busca diseñar una metodología para el respaldo y replicación de servidores que pueda ser aplicada a un caso práctico dentro de la Importadora Luna con la meta de asegurar el correcto funcionamiento de esta ante cualquier desastre o problema inesperado.

1.4 JUSTIFICACIÓN

El aumento exponencial de datos en los sistemas de información en este momento permite que lleguen nuevos sistemas de información que genera aún más información que es crítica y debe ser compatible de manera eficiente, así como el requisito legal para mantener información histórica durante varios años hace que la compra de una herramienta de soporte automatizada sea importante m (Terán D. , 2013)

Actualmente, la información se ha considerado uno de los activos más importantes en negocios u organizaciones ya que depende de cómo se la maneje para determinar el éxito o fracaso de la organización, existen varias amenazas: tanto físicas como lógicas que pueden causae que la información desaparezca.

Según estadísticas recogidas en un informe de la empresa: International Business Machines (IBM), de las instituciones con pérdidas de información por desastres, solo el 6% por ciento perdura a largo plazo, 51% quiebran en menos de un año y 43% no abren más (Cajamarca, 2019).

A nivel Latinoamericano menos del 50% de las empresas tienen implementado un plan de recuperación ante desastres, y en la gran mayoría de ellas su plan se basa únicamente en copias de seguridad y no implementan métodos de restauración de servicios en otro data center o proveedor cloud (Rock, 2020).

Por los motivos expuestos anteriormente, se hace indispensable que las diferentes organizaciones dispongan de un plan de contingencia que abarque el respaldo y replicación de servidores, de esta manera se asegura un correcto funcionamiento de la organización ante cualquier desastre o problema inesperado.

El presente proyecto busca convertirse en un documento que incluya todas las reglas, criterios y sugerencias sobre el programa seleccionado, con el fin de diseñar una metodología para

el respaldo y replicación de servidores y aplicarlo a un caso práctico dentro de la organización Importadora Luna como una fase de experimentación.

1.5 OBJETIVOS

1.5.1 Objetivo General

Diseñar una metodología, a través de un aplicativo VMWARE para el respaldo y replicación de servidores.

1.5.2 Objetivos Específicos

Crear una metodología que pueda ser implementada en cualquier organización con el fin de asegurar la recuperación de información a través de copias de seguridad y replicación de servidores.

Evaluar la metodología en un estudio de caso real para conocer su factibilidad de implementación.

Realizar pruebas de efectividad, con el fin de evidenciar cuantitativamente la viabilidad de la metodología, desarrollando un ambiente de pruebas.

CAPÍTULO II

MARCO TEÓRICO

2.1.1 Centro de datos

Es un espacio en el cual una empresa mantiene y gestiona la infraestructura de TI utilizada para ejecutar su negocio. Es un área que contiene servidores y sistemas de guardado donde se realizan, gestionan y conservan datos y contenido de aplicaciones. Para algunas compañías, se trata de una simple celda tipo jaula, mientras que para otras puede ser una sala privada que alberga una determinada cantidad de estantes dependiendo del tamaño de la empresa (Interconexion, 2015).

Según el sitio web de VMWARE; "Un centro de datos es una instalación física centralizada que contiene computadoras, redes, almacenamiento y otros equipos de TI que respaldan las operaciones comerciales. Las computadoras del centro de datos contienen o brindan aplicaciones, servicios e información críticos para el negocio" (Broadcom, 2023).

2.1.1.1 Componentes de un centro de datos

2.1.1.1.1 Espacio Físico

Es crucial establecer correctamente el lugar físico que ocupará el centro de datos. Esto usualmente abarca toda la zona del centro de datos y los lugares relacionados como almacenes, áreas eléctricas, etc (Maldonado, 2022).

2.1.1.1.2 Piso imaginario

Conocido también como piso falso el cual es un sistema de reja elevada que se coloca en los centros de datos. Cables, sistemas de aire y eléctricos se sitúan en el espacio que queda entre el piso fijo y el piso falso, asegurando un mejor flujo de aire para la refrigeración y climatización del espacio, y simplificando el manejo de los cables y sistema eléctrico. Aquí se pueden localizar sistemas de protección como extintores y sensores de humo. El suelo falso se compone de un

estándar que se sitúa a 30 cm del suelo real. Esto puede fluctuar en función del peso y la fuerza que los equipos impriman, así como su uso en el centro de datos (Maldonado, 2022).

2.1.1.1.3 Planta eléctrica

También conocido como cuarto eléctrico se relaciona con la provisión de energía para todo el centro de datos, lo cual abarca los paneles, cables y varios tipos de conectores. Se debe considerar que en el caso de que el centro de datos esté localizado en múltiples ubicaciones, los voltajes de funcionamiento pueden diferir de un sitio a otro. Asimismo, aquí se incluyen los sistemas de alimentación eléctrica de respaldo (Maldonado, 2022).

2.1.1.1.4 Sistemas de respaldo eléctrico

Incorpora todos los sistemas de backup eléctrico encargados de proporcionar el suministro de electricidad al centro de datos frente a cualquier avería por cualquier motivo. Este sistema cuenta con baterías de gran tamaño que son identificadas como fuentes de energía ininterrumpidas o generadores eléctricos; es fundamental establecer la capacidad del generador que funcionará en el centro de datos (Maldonado, 2022).

2.1.1.1.5 Cableado

El sistema de cables es un conjunto completo de cables situados en el centro de datos. Este facilitará la comunicación mediante la utilización de ciertas clases de conectores que conectarán los cables y comunicarán sistemas y servidores de forma local y remota. Los usuarios solo tendrán que vincular los servidores en el sistema estructurado de cableado del centro de datos con un cable básico al sistema principal (Maldonado, 2022).

2.1.1.1.6 Enfriamiento

El sistema de refrigeración se refiere a los aparatos y medios mediante los cuales se puede controlar la temperatura del entorno y gestionar la humedad del centro de datos. Este sistema integra sistemas de climatización para conseguirlo. Cada armazón de servidores puede contar con

su propio sistema de refrigeración, como congeladores o sistemas que se sustentan en el flujo de agua (Maldonado, 2022).

2.1.1.1.7 Dispositivos para extinguir fuego

Este conjunto abarca todos los equipos y materiales relacionados con la identificación de humo y la lucha contra incendios en el centro de procesamiento de datos. Los más utilizados son los sistemas de rociadores de agua, los agentes gaseosos para extinguir fuego y los extinguidores portátiles (Maldonado, 2022).

2.1.1.1.8 Otros componentes

Además de estos, existen varios elementos que no se clasifican como primordiales, pero que, si deben ser considerados y considerados, y que se hallan en los contextos de un centro de datos. Esto abarca, por ejemplo, aparatos para identificar goteras, mitigación de terremotos, sistemas de seguridad física como identificadores biométricos y cámaras de vigilancia (Maldonado, 2022).

2.1.1.2 Seguridad en centro de datos

La seguridad del centro de datos cubre varias áreas interrelacionadas y muy diferentes, estos van desde la protección física de computadoras y componentes de hardware hasta proteger la información de una computadora o las redes a través de las cuales se comunica con el universo. Hay diferentes clases de riesgos que debemos resguardar en un Centro de datos; tales como riesgos físicos, interrupciones eléctricas, fallos involuntarios de los usuarios, malware, hurto, daño o alteración de los datos. Sin embargo, hay tres aspectos básicos que definen la seguridad de la información y son: confidencialidad, integridad y disponibilidad (Jiménez, 2017). A continuación, se definen los diferentes tipos de seguridad en un centro de datos.

Tabla 1

Tipos de seguridad en un centro de datos

Seguridad Física
Es la implementación de obstáculos tangibles y métodos de regulación, que actúan como acciones preventivas y reacciones ante riesgos relacionados con los activos y datos sensibles.
Hace alusión a las medidas de seguridad, sistemas de protección que están presentes tanto dentro como en las proximidades de la sala de computación, así como las formas de conexión a distancia hacia y desde dicha área; utilizados para salvaguardar el equipo y los dispositivos de almacenamiento de información.
Seguridad Lógica
Se trata de implementar límites y métodos que protejan el acceso a la información, permitiendo que solo aquellos con autorización puedan acceder a ella.

Nota. La tabla indica los tipos de seguridad que existen en un centro de datos. Fuente: Segu-info, 2016 & Jiménez, 2017.

2.1.2 Seguridad de la información

La seguridad de la información es un conjunto de medidas preventivas y reactivas que toma una organización para proteger la información tratando de mantener sus dimensiones las cuales son confidencialidad, disponibilidad e integridad (Delgado, 2018).

Figueroa et al. (2021) definen a la seguridad de la información como a un conjunto de medidas y técnicas utilizadas para controlar y proteger todos los datos procesados dentro de una organización y para garantizar que los datos no salgan de los sistemas establecidos de la organización. Es una parte importante de la gestión de una empresa porque los datos que gestiona son fundamentales para las operaciones que realiza (Figueroa y otros, 2021).

2.1.2.1 Principios básicos de la seguridad de la información

Tal como se ha señalado previamente, existen tres pilares fundamentales en la seguridad de la información. A continuación, se procede a definir cada uno de estos conceptos esenciales.

Tabla 2

Fundamentos esenciales de la protección de la información

Confidencialidad	Integridad	Disponibilidad
es la característica que previene la distribución de datos a individuos o plataformas no permitidas. En términos generales, garantiza que el acceso a la información sea solo para quienes tengan la correspondiente autorización.	busca mantener los datos libres de modificaciones no autorizadas. La integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.	la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Nota. La tabla indica los fundamentos esenciales de la protección de la información. Fuente: Jiménez (2017).

2.1.2.2 Políticas de Seguridad de la Información

La norma ISO/IEC 27001 es un estándar reconocido a nivel internacional que define los requisitos necesarios para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI), con el fin de proteger los activos de información de una organización. Este enfoque tiene como propósito salvaguardar tres principios fundamentales de la seguridad de la información: la confidencialidad, la integridad y la disponibilidad de los datos dentro del entorno organizacional. Esta normativa ofrece un esquema para la protección de la información que asiste a las entidades en la detección y manejo eficaz de sus amenazas de seguridad de la información. Los requisitos establecidos por la norma poseen un carácter general y están diseñados para ser aplicables a cualquier organización, sin importar su tipo, tamaño o sector de actividad.

Para garantizar la efectividad de las políticas y reglamentos dentro de una organización, es fundamental que estos sean comunicados adecuadamente a todos los involucrados en el proceso, a través de programas de capacitación y desarrollo de competencias.

El responsable debe evaluar las necesidades, indicar los controles, indicar los riesgos referentes a la seguridad e integridad de la información, determinar con la administración de la organización el tipo de almacenamiento y la accesibilidad de la información (Jiménez, 2017).

La norma ISO/IEC 27001, enfocada en la gestión de la seguridad de la información, destaca la relevancia de implementar medidas eficaces de respaldo de datos. Estas prácticas tienen como finalidad preservar la integridad y disponibilidad de la información, así como asegurar los recursos necesarios para su administración. Los procesos de copia deben ejecutarse conforme a políticas definidas y ser sometidos a revisiones periódicas para verificar su eficacia.

Es fundamental que toda información vital para las operaciones de una organización disponga de una copia de respaldo actualizada, almacenada en un lugar seguro, con el propósito de garantizar la continuidad del negocio ante la eventual inaccesibilidad de la fuente primaria. Las acciones preventivas y de contingencia deben ser constantes, considerando la tecnología, los recursos humanos y la infraestructura.

2.1.3 Historia de los respaldos de información

Los primeros backups de programas informáticos se realizaron en carretes de cinta magnética de gran tamaño, también en papel: tarjetas perforadas y cintas de papel. En el periodo subsiguiente, los backups se guardan mayormente en discos de diferentes medidas. No obstante, las computadoras actuales carecen incluso de unidades de disquete, por no mencionar los equipos para procesar tarjetas perforadas. Ahora, los backups se redactan en CDs, discos duros, unidades flash o mediante la red. A continuación, expondremos la historia de estos aparatos y procedimientos, intentando vincularlos con la copia de seguridad (Terán, 2013).

2.1.3.1 Copias de seguridad de tarjetas perforadas consideradas como un punto de inflexión en el progreso de los backups

Tabla 3

Tarjetas perforadas

Historia de la copia de seguridad
La primera generación de computadoras digitales se inició en 1951 con la creación del UNIVAC I (Computadora Automática Universal), desarrollada por Mauchly y Eckert. Estas máquinas utilizaban tubos de vacío como elementos fundamentales para la lógica, tambores magnéticos giratorios para el almacenamiento interno de datos y programas, y tarjetas perforadas para la entrada de información y el almacenamiento externo. En este sentido, las tarjetas perforadas representan una de las primeras formas de almacenamiento utilizadas para realizar respaldos de datos. A principios de la década de 1960, comenzaron a desarrollarse las primeras estrategias de copias de seguridad. Posteriormente, las cintas magnéticas se consolidaron como el método preferido debido a la confiabilidad de sus unidades, su capacidad para escalar y su costo relativamente bajo.

Nota. La tabla indica la relación entre las copias de seguridad y las tarjetas perforadas. Fuente: Terán (2013).

2.1.3.2 El progreso de los discos duros y las copias de respaldo de disco a disco

En 1956, IBM introdujo el primer disco duro, estableciendo un precedente significativo en el campo del almacenamiento digital. Desde entonces, esta tecnología ha experimentado un desarrollo acelerado y constante. A partir del lanzamiento del IBM PC/XT en 1983, el disco duro se estableció como un elemento fundamental en la mayoría de las computadoras personales. Diversos fabricantes han impulsado su evolución; por ejemplo, en 1982, Hitachi lanzó el primer disco con una capacidad superior a 1 GB. Un desarrollo significativo en esta área fue la aparición, a principios de la década de 1990, de la tecnología RAID (Redundant Array of Independent Disks), la cual utiliza múltiples discos duros para distribuir o duplicar datos entre ellos, mejorando la redundancia y el rendimiento (Terán, 2013).

2.1.3.3 Disquetes y su contribución a la copia de seguridad

Los disquetes se vieron como una innovación importante para mover información de una computadora a otra. Aunque su capacidad de almacenamiento era inferior a la de los discos duros, su costo reducido y su versatilidad contribuyeron a su gran popularidad. Por supuesto, esta situación impactó en el ámbito de las copias de seguridad. Desde 1973, tras la introducción de 8 pulgadas - SSSD, que permitía el movimiento de pequeñas cantidades de datos, los discos comenzaron a ser utilizados de manera extensa para efectuar copias de seguridad. Sin embargo, dado que estos discos eran bastante económicos y útiles, rápidamente se transformó en uno de los medios de copia de seguridad más habituales entre los usuarios de viviendas y pequeñas empresas (Terán, 2013).

2.1.3.4 CD-R/RW y DVD - Nuevos Medios de copia de seguridad

Durante los años 90, CD-R no se empleaba frecuentemente para respaldos, a causa de sus elevados costos. Sin embargo, posteriormente, cuando el CD-ROM se estableció como un componente común en casi todos los equipos de cómputo y los costos de los discos compactos experimentaron una notable reducción, los backups en CD ganaron gran popularidad y se extendieron ampliamente. El CD casi distanció los disquetes para el inicio del nuevo milenio. La capacidad de 4 GB del DVD desde 1995 sólo ha consolidado esta tendencia (Terán, 2013).

2.1.3.5 Discos HD-DVD y Blu-ray

Tabla 4

La última generación de sistemas de respaldo y copia de seguridad

Discos Blu-ray y HD-DVD
Lásers Blu-ray que emplean tintes orgánicos, como el formato Blu-ray de Sony (entre 23 GB y 54 GB) y el HD-DVD de Toshiba, representan un avance hacia la disminución adicional de los costos de los medios extraíbles, además de incrementar la capacidad y mejorar la usabilidad. Se introdujeron en el mercado en 2006 y en la acyualidad se consideran una opción prometedora para los dispositivos de respaldo de datos.

Nota. La tabla muestra la nueva generación de medios de copia de seguridad. Fuente: Terán (2013).

2.1.3.6 En línea y de red: Soluciones de Backup

El incremento en la generación de copias de seguridad guarda una estrecha relación con el desarrollo de las tecnologías de red y el crecimiento exponencial del uso de Internet. Conforme aparecieron las redes locales, se permitió realizar backups remotas a otras computadoras vinculadas a la misma. Las redes locales y globales permiten el almacenamiento de volúmenes críticos de datos en dispositivos remotos a nivel mundial. Para asegurar la protección frente a desastres o eventos adversos específicos del sitio, es común que las organizaciones opten por trasladar las copias de respaldo a una ubicación externa o bóveda fuera de las instalaciones principales.

2.1.4 Sistemas de respaldo o Backups

La cantidad de información que procesan las empresas está creciendo rápidamente, al igual que la necesidad de protegerla. La información proviene de diversas fuentes como servidores de aplicaciones, usuarios, máquinas virtuales, etc. Las copias de seguridad se utilizan básicamente para tres propósitos: recuperación ante desastres, recuperación empresarial y almacenamiento de información a largo plazo. El objetivo principal de la recuperación ante desastres consiste en restaurar la totalidad o la mayor parte de los datos y sistemas tecnológicos afectados, garantizando así la continuidad operativa tras la ocurrencia de un desastre natural o una emergencia. La recuperación generalmente se realiza en un sitio de respaldo o recuperación ante desastres que tiene

la misma infraestructura o una similar que el sitio principal y está listo para complementar el entorno de producción mediante el respaldo (Chango y otros, 2017).

Las copias de seguridad resultan beneficiosas frente a diversos sucesos y usos: rescatar los sistemas y datos de una catástrofe informática, natural o ataque; recuperar un pequeño número de archivos que podrían haber sido borrados accidentalmente, corrompidos, infectados por un virus informático u otros motivos; almacenar datos históricos de manera más asequible que los discos duros y además posibilitando el desplazamiento a lugares diferentes (Jiménez, 2017).

2.1.4.1 Riesgos a los que están expuestos los sistemas informáticos

Es ampliamente reconocido que la información y los datos constituyen activos fundamentales para las organizaciones. Sin embargo, en muchos casos, las empresas carecen de la infraestructura adecuada para gestionarlos de forma eficiente. Con frecuencia, se implementan soluciones básicas que otorgan cierta capacidad de almacenamiento al núcleo del negocio, pero estas suelen estar limitadas por equipos con deficiencias tanto en hardware como en software. La tecnología no está exenta de fallos, y las copias de seguridad se emplean como un método de contingencia si ocurre algún fallo o error. Las interrupciones en el ámbito informático pueden presentarse bajo múltiples formas, entre las que se incluyen infecciones por software malicioso, fallas eléctricas, errores en componentes de hardware o software, interrupciones en la red, accesos no autorizados por parte de ciberdelincuentes, errores humanos, así como desastres naturales como incendios e inundaciones, entre otros. Si bien no es factible eliminar por completo la ocurrencia de interrupciones, la organización puede anticiparse mediante estrategias adecuadas que permitan mitigar sus posibles impactos sobre la continuidad del negocio. La duración del tiempo requerido para responder una empresa determinará la severidad de sus efectos (Terán, 2013).

Existen diferentes tipos de riesgos, los principales son los que se detallan a continuación.

Tabla 5

Tipos de riesgos

Errores humanos	Vandalismo	Fallos hardware
errores realizados sin propósito, como la eliminación accidental de datos por los usuarios.	incidentes o destrozos intencionados que pueden afectar a la infraestructura TIC.	originados por errores y comportamientos incorrectos en elementos hardware.
Sabotaje informático	**Ciberataque**	**Desastres naturales**
insulto o manipulación deliberada de terceros o ex empleados.	problemas ocasionados por ciberdelincuentes, secuestros de sistemas por rasomware, virus u otro malware.	Algunos ejemplos de desastres naturales son terremotos, inundaciones o incendios, que pueden destruir todo en poco tiempo.

Nota. La tabla indica los principales tipos de riesgos básicos de la SI. Fuente: Hernández (2021).

2.1.4.2 Técnicas de backup

Es importante que los servidores web guarden regularmente copias de respaldo o backups. Estos backups pueden hacerse utilizando un sistema distribuido, en el que cada servidor tiene su propio drive o utilizando un sistema centralizado conectado al servidor (Areitio, 2008). Para preservar los datos del servidor web, se pueden utilizar tres técnicas backup que se detallan a continuación.

Tabla 6

Técnicas de Backup

Backup completo	Backup incremental	Backup diferencial
se realiza una salvaguardia de todos los ficheros del sistema.	sólo selecciona los ficheros que han cambiado desde el último backup completo o bien desde el último backup incremental. Reduce el espacio de almacenamiento, pero complica las recuperaciones de ficheros. Para recuperar un fichero es preciso utilizar la última salvaguarda completa y todas las incrementales posteriores hasta el momento.	sólo selecciona los ficheros que han cambiado desde la última salvaguarda completa. Para recuperar un fichero es preciso utilizar la última salvaguarda completa y la última diferencial

Nota. La tabla indica las técnicas de backup. Fuente: Desongles, Balongo & Ochoa (2002).

2.1.4.3 Medios de respaldo

Tabla 7

Estrategias de copias de seguridad o medios de respaldo

Medios de respaldo
Al diseñar una estrategia de respaldo, uno de los aspectos fundamentales a considerar es el tipo de medio de almacenamiento que se utilizará. Esta elección está determinada por diversos factores, entre ellos el volumen de información a respaldar, la frecuencia con la que se realizan las copias, la disponibilidad requerida de los datos y el tiempo estimado para su recuperación. Generalmente, se opta por soluciones basadas en cinta o disco, en función de la velocidad de acceso y la periodicidad con la que se necesita restaurar la información.

Nota. La tabla indica las estrategias de respaldo. Fuente: (Quishpe, 2007).

A continuación, se detallan los dos tipos de soluciones.

Tabla 8

Tipos de soluciones

Soluciones basadas en disco	
El respaldo basado en disco resulta especialmente adecuado para entornos donde se ejecutan aplicaciones de forma continua, las 24 horas del día y los 7 días de la semana, ya que permite un acceso aleatorio rápido a los datos y ofrece una recuperación prácticamente inmediata en caso de fallos o desastres.	
Soluciones basadas en cinta	
En el ámbito empresarial e institucional, uno de los dispositivos de respaldo más empleados son las cintas magnéticas, debido a su capacidad para manejar grandes volúmenes de información. Su popularidad se debe a varias ventajas: son reutilizables, lo que reduce significativamente los costos a largo plazo; además, presentan un diseño físico compacto combinado con una alta capacidad de almacenamiento. Esta solución ofrece, entre otros beneficios, los siguientes:	
1	**Menor costo total de propiedad:** En comparación con las soluciones basadas en disco, las cintas presentan una inversión inicial y operativa significativamente más baja, especialmente en entornos de almacenamiento a largo plazo.
2	**Soporte duradero y reutilizable:** Las cintas ofrecen una larga vida útil y pueden ser utilizadas múltiples veces. Además, su portabilidad permite almacenarlas fuera del sitio principal, facilitando planes de recuperación ante desastres.
3	**Alta fiabilidad en la recuperación:** Garantizan una restauración precisa y segura de los datos respaldados, incluso después de múltiples ciclos de uso, manteniendo la integridad de la información.
4	**Escalabilidad:** Pueden adaptarse fácilmente a infraestructuras de distintos tamaños, desde pequeñas organizaciones hasta centros de datos empresariales, sin comprometer la eficiencia ni el rendimiento.

Nota. La tabla indica dos tipos de soluciones. Fuente: (Quishpe, 2007)

2.1.4.4 Modelos de respaldo

Existen dos tipos de copias de respaldo, en caliente y en frío.

Tabla 9

Hot Backup

Copias de respaldo en caliente (Hot backup) o copia dinámica
Este tipo de respaldo se realiza mientras los datos permanecen accesibles para los usuarios e incluso pueden estar siendo modificados durante el proceso. Las copias en caliente representan una solución eficaz para entornos multiusuario, ya que no es necesario interrumpir el acceso al sistema ni desconectar a los usuarios, a diferencia de los métodos de respaldo tradicionales que requieren suspender la operación del sistema para garantizar la integridad de la información.
Las copias de respaldo en caliente conllevan ciertos riesgos inherentes. Si los datos son modificados durante el proceso de copia, existe la posibilidad de que el respaldo no refleje con precisión el estado final de la información. En situaciones de recuperación, como una falla del sistema, estas inconsistencias deben ser gestionadas adecuadamente. Algunas bases de datos avanzadas mitigan este riesgo mediante la generación de registros (logs) previos a la copia y mediante técnicas de monitoreo específicas que preservan la integridad de los datos. Aunque este tipo de respaldo puede afectar temporalmente el rendimiento del sistema, representa un compromiso aceptable cuando se prioriza la disponibilidad continua de las aplicaciones. Por ello, su uso es común en sistemas que operan de forma ininterrumpida, como Microsoft Exchange o Microsoft SQL Server.

Nota. La tabla indica la definición de copias de respaldo en caliente. Fuente: (Quishpe, 2007)

Tabla 10

Cold Backup

Copias de respaldo en frío (Cold backup)
Las copias de respaldo fuera de línea se realizan cuando el sistema y sus servicios no están en operación. Este tipo de respaldo es común en situaciones donde se requiere capturar una imagen exacta del sistema en un momento específico, o cuando la aplicación no permite realizar copias en línea. La principal desventaja de este enfoque es que los datos no están disponibles para los usuarios durante el proceso de respaldo, lo que puede afectar la continuidad operativa en entornos que requieren alta disponibilidad.

Nota. La tabla indica la definición de copias de respaldo en frío. Fuente: Quishpe (2007).

2.1.4.5 Estrategia para realizar respaldos

Una estrategia efectiva de copias de seguridad es esencial para manejar los datos de manera segura y eficiente. Es importante mencionar que no existe una única estrategia aplicable a todas las organizaciones, ya que cada una tendrá que adaptar la estrategia a sus propias necesidades, sin embargo, se definen unos mínimos aplicables a la mayoría de las organizaciones, las cuales se detallan a continuación en la tabla 11 (Hernández, 2021).

Tabla 11

Estrategias mínimas aplicables

Almacenamiento Principal	Almacenamiento secundario
Se necesita disponer de dos tipos de almacenamiento para alojar las copias. Lo ideal es contar como repositorio principal de backup un medio que sea rápido y permita optimizar el espacio usado. Para este cometido lo más recomendable en términos de velocidad, confiabilidad y seguridad es unas almacenamiento en disco en cualquiera de sus distintas tecnologías: SAN, NAS o DAS.	Una vez realizadas las copias en disco, se necesita realizar una segunda copia en otro medio de almacenamiento distinto, entre los recomendados se destacan las unidades de cinta LTO/DAT o una segunda cabina de disco.
Almacenamiento fuera del sitio	**Programación y periocidad**
También conocido como backup cloud , consiste en efectuar la copia de seguridad en un almacenamiento externo proporcionado por un tercero. Tienen como finalidad garantizar la disponibilidad de la copia en caso de incidente grave en la ubicación principal del sistema de backup, es importante que el proveedor cloud seleccionado cumpla con los requisitos legales pertinentes según el tipo de datos del que se va hacer copia.	Es la frecuencia con la cual se realizará la copia de seguridad, esta periodicidad se ajusta a las necesidades de la organización, el algunas ocasiones los archivos o datos se actualizan con frecuencia durante el día y puede requerir que se realicen copias de seguridad con más frecuencia. En situaciones normales, se puede considerar realizar una copia de seguridad al final de cada día.

Nota. La tabla indica las estrategias mínimas aplicables a la mayoría de las organizaciones. Fuente: Hernández (2021).

Otras circunstancias pueden exigir la realización de copias de seguridad instantáneas de las modificaciones para minimizar la pérdida de datos en caso de un incidente. Los requerimientos de

RPO definidos por la entidad serán los que establezcan la frecuencia de la copia de seguridad (Hernández, 2021).

A continuación, en la Tabla 12 se define una estrategia básica que podría ser relevante para la gran mayoría de las entidades, considerando un período común de backups durante las noches y los fines de semana, se observa un ejemplo de planificación de backups periódicos para un mes utilizando copias diferenciales a disco (D), copias a disco (F) y copias a cinta (C) (Hernández, 2021).

Tabla 12

Planificación de Backup

Lunes	Martes	Miércoles	Jueves	Viernes	Sábado Domingo
D	D	D	D	D	F + C
D	D	D	D	D	F + C
D	D	D	D	D	F + C
D	D	D	D	D	F + C

Nota. La tabla indica un ejemplo de una planificación de Backup. Fuente: Hernández (2021).

2.1.5 Servidores

Marchionni (2021) describe lo siguiente: un "Servidor" o "Host", también conocido como anfitrión, es un tipo de ordenador diseñado con potentes capacidades de procesamiento, que tiene la responsabilidad de ofrecer diversos servicios a redes de datos, tanto inalámbricas como por cables; además, facilita el acceso a cuentas de correo electrónico, la gestión de dominios empresariales, así como el alojamiento de sitios web entre otras tareas.

Otra definición citada por (Valdivia, 2017) define al servidor como una herramienta de software diseñada para manejar solicitudes de un usuario y ofrecer una contestación adecuada. Los servidores pueden funcionar en cualquier clase de ordenador, incluso en equipos específicos que se denominan "el servidor".

Los servidores se instalan mejor en gabinetes especiales llamados racks, que le permiten colocar varios Servers en compartimentos especiales y ahorrar espacio, y como permanecen estacionarios, son más seguros. Los servidores deben operar las 24 horas del día, los 365 días del año (Jiménez, 2017).

2.1.5.1 Modelos de servidores

Existen diversos tipos de servidores, los cuales pueden implementarse tanto en entornos físicos como virtuales. Su clasificación puede realizarse según sus características técnicas, fabricantes o los servicios que proporcionan. A continuación, se expone esta última categorización, basada en las funciones que desempeñan dentro de la infraestructura tecnológica.

Tabla 13

Tipos de servidores

Servidores de impresión	Servidores web	Servidores de base de datos
tiene conectadas varias impresoras de red y administran las colas de impresión según la petición de sus clientes.	este tipo de servidores se encarga de almacenar sitios en la red interna (intranet). Pueden publicar cualquier aplicación web, brindarle la seguridad correspondiente y administrarla por completo.	lo más importante de estos servidores es la posibilidad de manejar grandes cantidades de datos y generar información. Para contener todo este material generalmente se conectan a un storage.
Servidores de comunicaciones	**Servidores de directorio**	**Servidores de correo electrónico**
Además, estos servidores pueden ofrecer servicios de preatención telefónica cuando se integran con una consola telefónica, permitiendo gestionar y canalizar las llamadas entrantes de manera eficiente antes de su atención directa.	se ocupan de almacenar los datos de todos los usuarios de la red, propiedades y características que los identifican.	Los servidores de correo electrónico permiten la gestión centralizada de todos los mensajes dentro de una empresa. Para manejar el elevado volumen de datos, estos sistemas suelen integrarse con soluciones de almacenamiento dedicadas (storage). Además, muchos servidores incorporan funciones de protección, tales como filtros antispam, listas blancas y negras, así como herramientas antivirus, con el objetivo de garantizar la seguridad y confiabilidad en la comunicación.
Servidores de archivos		
Estos sistemas facilitan la compartición de materiales y su almacenamiento seguro, además de ofrecer una capacidad significativamente mayor en comparación con los dispositivos de escritorio. Asimismo, pueden estar conectados a múltiples unidades de almacenamiento (storage) de diferentes capacidades para ampliar su rendimiento y flexibilidad.		

Nota. La tabla indica una caracterización de los tipos de servidores. Fuente: Marchionni (2021).

2.1.6 Medios de respaldo

Al diseñar una estrategia de respaldo, el primer aspecto a evaluar es el tipo de soporte que se utilizará para almacenar las copias de seguridad. Esta decisión depende de varias variables, como la cantidad de datos que se replicarán, la frecuencia de la replicación, la disponibilidad y el tiempo necesario para la recuperación del sistema.

2.1.7 Veeam backup & replication

Se trata de un software creado por Veeam Software con el objetivo de efectuar copias de seguridad, restaurar y duplicar datos en máquinas virtuales. Se introdujo inicialmente en 2008 y es un componente de Veeam Availability Suite. Veeam fue uno de los primeros proveedores en desarrollar software de respaldo adaptado a las máquinas virtuales (Veeam, 2023).

CAPÍTULO III

METODOLOGÍA

Para este proyecto se ha utilizado el software veeam backup & replication en conjunto con un ambiente de pruebas sobre VMWare, lo que permite la automatización de tareas de respaldo y replicación resolviendo así el problema que actualmente sucede en Importadora Luna.

El objetivo de la propuesta es cubrir las necesidades fundamentales de la empresa en términos de respaldo de datos y duplicación de servidores. La relevancia de llevar a cabo el proyecto se fundamenta en las áreas administrativa, operativa y financiera.

En el área de administración, puede crear fácilmente cronogramas para copias de seguridad diarias, semanales, mensuales y anuales, junto con planes de respaldo y sus etapas de duración.

En el área operativa, la participación del usuario con el sistema de respaldo confirmará que la configuración de respaldo se haya realizado de manera correcta y actuará de manera adecuada si se presenta un fallo durante el proceso.

En el ámbito financiero existirá una reducción en la utilización de dispositivos para la copia de seguridad, puesto que ahora se normalizarán y se emplearán de manera eficiente.

3.1 Métodos

Para el desarrollo del presente proyecto de titulación se aplicaron principalmente dos técnicas metodológicas, seleccionadas en función de los objetivos propuestos y la naturaleza del estudio.

3.1.1 Método Exploratorio

Este método se utilizó en la investigación con el objetivo de resaltar los aspectos clave del problema e identificar los procedimientos apropiados para avanzar en futuras investigaciones, incluyendo conceptos esenciales y casos de éxito, entre otros.

3.1.2 Método Descriptivo

Brindó la oportunidad de identificar las principales características de las herramientas de backup de datos, lo que permitió llevar a cabo un análisis comparativo que evalúa las similitudes y diferencias entre ellas, y así proponer la mejor solución para aplicarla como fase experimental dentro de Importadora Luna.

3.2 Técnicas

3.2.1 Investigación bibliográfica

Esta técnica facilitó la elaboración de la parte teórica del proyecto de investigación, lo que permitió que exista una familiarización con los conceptos clave relacionados con el tema, consultando fuentes confiables como libros, artículos y recursos en internet.

3.2.2 Entrevista verbal

Este método se empleó para recopilar la información necesaria y comprender el estado actual de Importadora Luna, así como para investigar cómo se llevaban a cabo los backups, en caso de contar con un sistema de respaldo y replicación antes de implementar la solución propuesta. Además, permitió conocer el tamaño de la información que debía ser respaldada en Importadora Luna.

3.2.3 Investigación de Campo

Este tipo de estudio resulta pertinente, ya que permite examinar el problema directamente en el entorno donde se originan los hechos. Esta aproximación facilita una comprensión más profunda de las dificultades que enfrenta Importadora Luna al no disponer de una solución automatizada para el respaldo y la replicación de información. En consecuencia, este enfoque contribuye significativamente a la formulación de propuestas viables y al cumplimiento de los objetivos planteados en el presente trabajo de investigación.

3.2.4 Observación

Esta metodología, en combinación con la investigación de campo, posibilitó la visita al lugar de los sucesos, o sea, Importadora Luna, con el propósito de examinar su estructura y funcionamiento, así como identificar las políticas y procedimientos relacionados con el almacenamiento de la información, en caso de que existan.

3.2.5 Experimentación

Gracias a la aplicación de esta técnica, fue posible establecer un escenario de pruebas adecuado para la evaluación del proyecto, esto permitió observar el funcionamiento de la herramienta Veeam Backup & Replication, demostrando la eficacia del software escogido.

3.3 Análisis de requerimientos HW o SW

A continuación, se describen los requisitos de hardware y software necesarios para la implementación del proyecto, tomando como base la matriz de compatibilidad proporcionada por VMware.

Tabla 14

Compatibilidad con VMware

Matriz de compatibilidad com Vmware		
Virtualización	Máquinas Virtuales	Hosts
Vmware	Todos los sistemas operativos coportados por Vmware	ESXI 8.0
vSphere 8.0	Todas las aplicaciones	ESXI 7.0 hasta Update 3
vSphere 7.0 y superior	Todos los sistemas de archivos	ESXi 6.x
vSphere 6.x		

Nota. La tabla indica los requerimientos de hardware y software. Elaborado por: Los Autores.

Tabla 15

Requerimiento de hardware y software

Requerimientos de Hardware
CPU x86 y x64 en arquitectura Intel y AMD
Memoria 8 GB de RAM mas 550 mb por cada tarea de respaldo concurrente
Almacenamiento 9.5 GB para la instalación del producto y Microsoft.Net Framework 4.7.2, 10 GB por cada 110 maquinas virtaules para almacenar el gatalogo(data persistente), adicional 110 GB para carpeta de cache de Instant recovery (data no persistente)
Tarjeta de red de almenos 1 Gbps para el prototipo ye en entornos de alta demanda debe ser de 10 Gbps.
Requerimientos de Software
Microsoft Windows Server 2025
Microsoft Windows Server 2022
Microsoft Windows Server 2019
Microsoft Windows Server 2016
Microsoft Windows Server 2012 R22, 3
Microsoft Windows Server 2012, 3
Microsoft Windows 11 (versions 21H2, 22H2, 23H2, 24H2)
Microsoft Windows 10 (versions 1909 to 22H2)
Microsoft Windows 10 LTS (versions LTSB 1607, LTSC 1809, LTSC 2021)
Veeam backups & replication no puede ejecutarse en versiones sin soporte de
Para la instalación local o remota administe la siguientes bases de datos
PostgreSQL 14.x
PostgreSQL 14.x
Microsoft SQL Server 2012
Microsoft SQL Server 2014
Microsoft SQL Server 2016
Microsoft SQL Server 2017
Microsoft SQL Server 2019
Microsoft SQL Server 2022
SQL Server Express Edition hasta un maximo de 10 GB
Durante la instalación el sistema realiza la verificación de la configuración del sistema para determinar si tods los prerequisitos de software estan disponibles en maquina deonde se planea instalar Veeam Backups & Replication. Si falta alguno de los prerequisitos el asistente ofrecera instalar de manera automática.
Microsoft .NET Framework 4.7.2
Microsoft ASP.NET Core Shared Framework 8.0
Microsoft Edge WebView2 Runtime 130.0.2849.56 (not installed for Microsoft Windows Server 2012 and 2012 R2 due to the version incompatibility)
Microsoft PowerShell 5.1
Microsoft Report Viewer Redistributable 2015
Microsoft SQL Server System CLR Types (both for SQL Server and PostgreSQL installations)
Microsoft Universal C Runtime
Microsoft Visual C++ 2015-2022 Redistributable 14.40.33810
Microsoft Windows Desktop Runtime 8.0"

Nota. La tabla indica los requerimientos de hardware y software. Fuente: Veeam Backup & Replication support for vSphere (2025).

3.4 Procedimiento de la metodología

En este apartado se detalla el diseño de la solución, definiendo la arquitectura del sistema y el diagrama general.

3.4.1 Arquitectura del sistema

En este grado inicial de abstracción, se descomponen los subsistemas que conforman la solución en secciones y se detalla la interconexión entre estos. Se desarrolló una estructura estándar, adaptable y escalable conforme a las demandas de Importadora Luna.. La arquitectura propuesta es ampliable según los requerimientos de cada organización, permitiendo agregar componentes conforme sea necesario.

Tabla 16

Arquitectura del sistema

Arquitectura de Backup	Arquitectura de Replicación
comprendida por backup server, proxy server.	es el mismo proxy que el de backup.

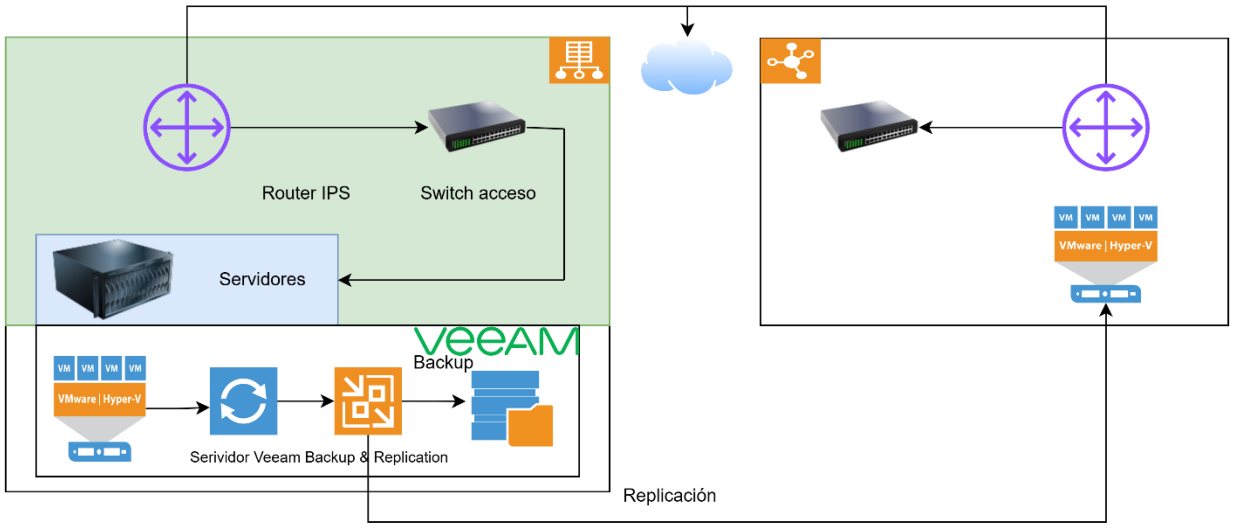
Nota. La tabla indica la arquitectura del sistema. Elaborado por: Los Autores.

3.4.2 Arquitectura completa

En esta sección se muestra el diagrama general que ilustra todos los componentes que conforman la solución propuesta, así como las interacciones y relaciones entre ellos.

Figura 1

Arquitectura completa



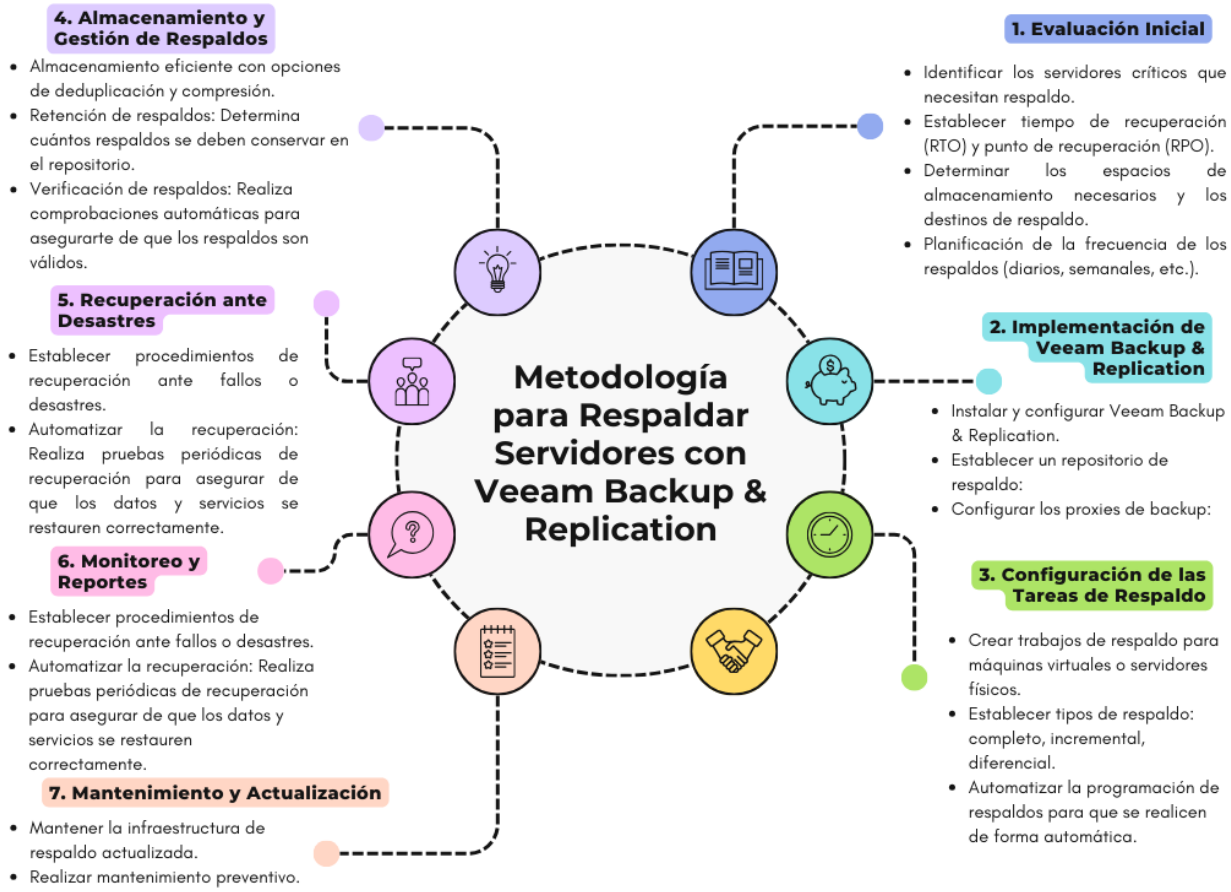
Nota. Se presenta el diagrama general. Elaborado por: Los Autores.

3.5 Desarrollo de la metodología

En esta sección se presentan dos mapas conceptuales que ilustran el funcionamiento de la metodología propuesta. La Figura 2 expone el esquema correspondiente al proceso de respaldo de servidores, mientras que la Figura 3 detalla la metodología aplicada para la replicación de estos.

Figura 2

Metodología para respaldar servidores



Nota. Se presenta la metodología para respaldar servidores. Elaborado por: Los Autores.

A continuación, se detalla la configuración de la metodología planteada (diseño de la solución), se inició instalando el servidor de gestión de la infraestructura virtual VMware que no es más que el software de virtualización veeam backup & replication.

Una vez instalado el software y tomando como base la arquitectura y metodología propuesta, se configuró el software de backup.

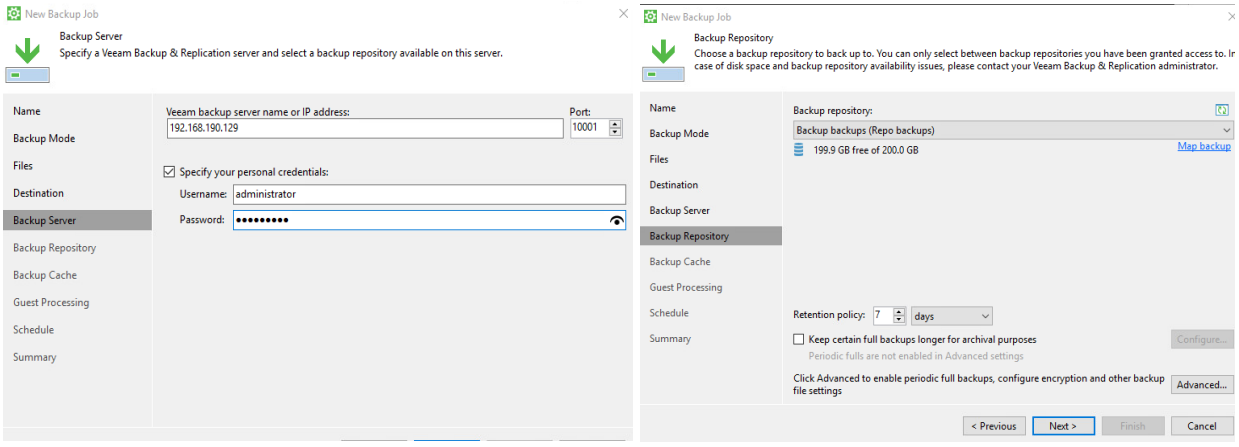
Backup server: Para la implementación se seleccionó una máquina virtual con Windows Server 2019, equipada con 4 vCPUs, 8 GB de memoria RAM y 100 GB de almacenamiento en disco, ya que se trata de una implementación para un entorno pequeño dichos recursos son más que

suficientes. El servidor de facturación de la Importadora Luna es Windows Server 2019 con 2 vCPUs y 4GB de Ram.

Para la instalación y configuración del software de backup, se descargó la versión más reciente del instalador desde la página de Veeam Backup. Una vez instalado, se realizó la configuración inicial y los repositorios de destino de las copias. Una vez configurados los repositorios de almacenamiento para los backups, se configuraron también los Jobs de copias de seguridad, estableciendo la programación y los períodos de retención conforme a los requerimientos específicos de Importadora Luna.

Figura 3

Instalación y configuración del software de backup



Nota. Se presentan los pasos para instalar y configurar el software de backup. Elaborado por: Los Autores.

Backup proxy: Este servidor ya se encontró instalado por defecto y fue suficiente para Importadora Luna al tratarse de un entorno pequeño.

En la figura 4, se observa la metodología para replicación de servidores y se detalla brevemente el desarrollo de las configuraciones para respaldo y replicación que se llevaron a cabo en Importadora Luna.

Figura 4

Metodología para la replicación de servidores

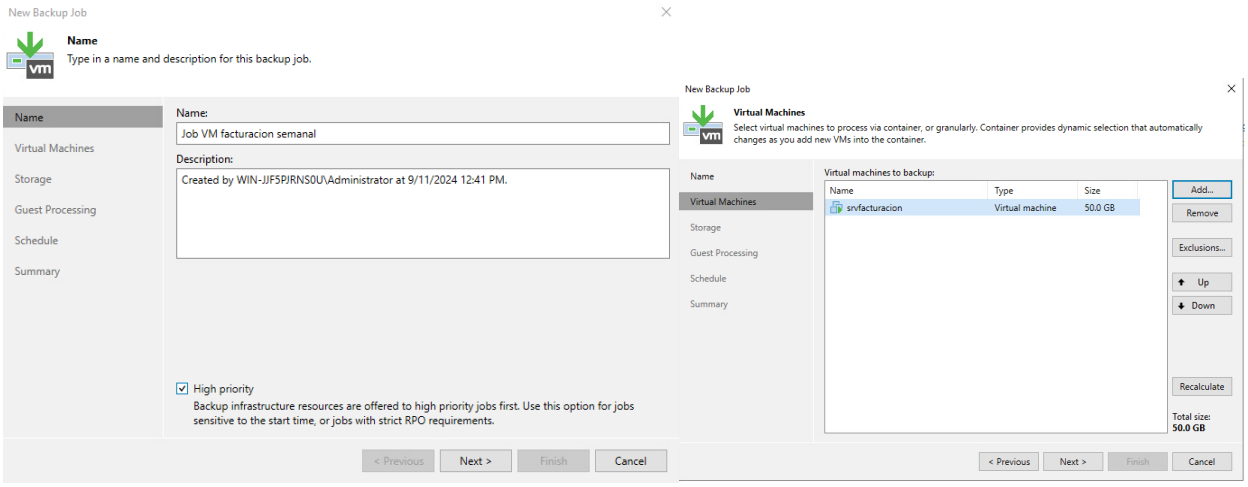
Nota. Se presenta la metodología para replicar servidores. Elaborado por: Los Autores.

3.5.1 Configuración del job de respaldo

Para realizar la configuración del job de respaldo de la máquina virtual, en primera instancia se definió el nombre y en el apartado de Virtual Machines elegimos la máquina virtual que estuvo definida para realizar la copia en este caso fue srvfacturacion.

Figura 5

Configuración del job de respaldo de la máquina virtual

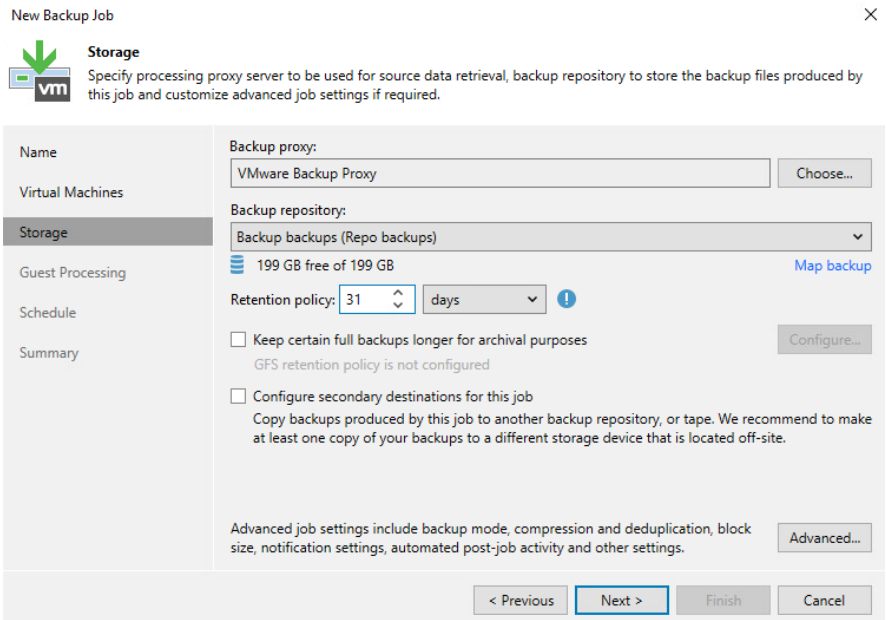


Nota. Se presenta la configuración del job de respaldo. Elaborado por: Los Autores.

Se seleccionó el repositorio Backup backups al que vamos a realizar la copia y el proxy VMware ya definido, con respecto a las políticas de retención fueron de 31 días.

Figura 6

Configuración del servidor proxy de almacenamiento

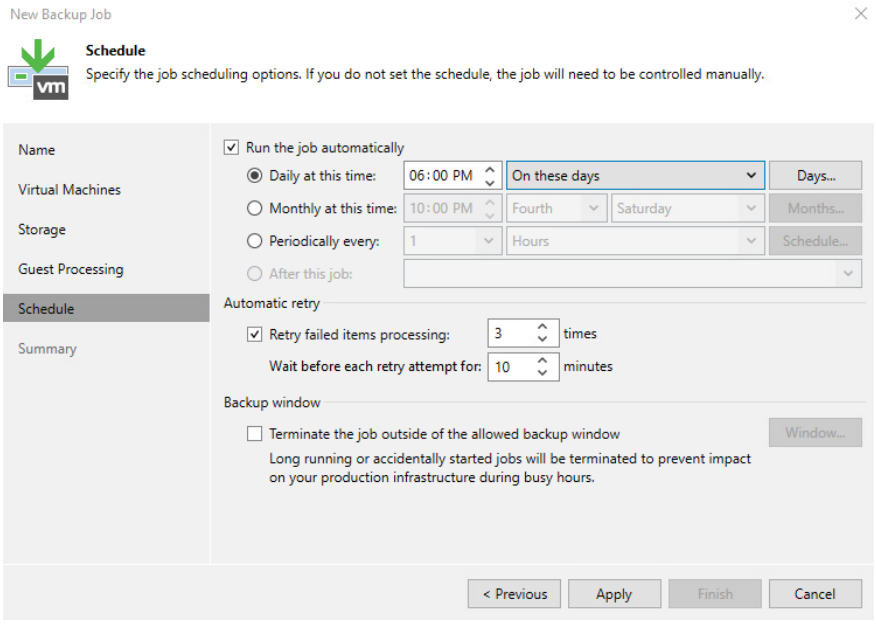


Nota. Se presenta la configuración del servidor proxy de almacenamiento. Elaborado por: Los Autores.

Con respecto al cronograma se configuró las horas y días de ejecución en el caso de Importadora Luna las copias de seguridad se realizarán diariamente a las 06:00, realizando 3 reintentos en caso de que falle la copia de seguridad con un tiempo de espera entre copia y copia de 10 minutos, con esto estaría lista la primera tarea de copias de seguridad.

Figura 7

Configuración del cronograma

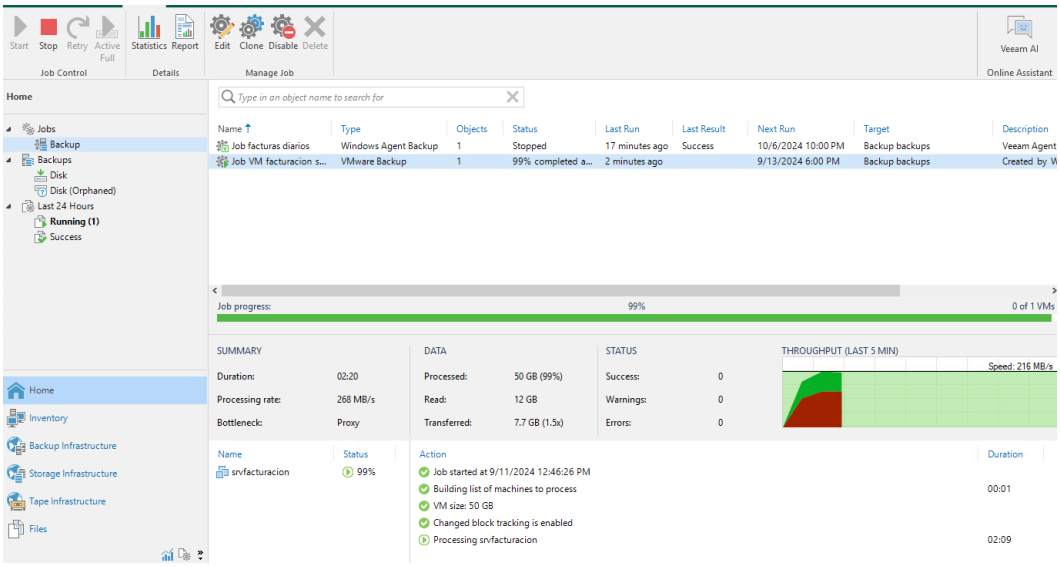


Nota. Se presenta la configuración del cronograma. Elaborado por: Los Autores.

Una vez obtenida la primera tarea de copia de seguridad creada (Job VM facturación) se procedió a ejecutar, a la par de este proceso en el entorno virtual se creó una copia de seguridad instantánea. Durante el proceso de ejecución de la copia de seguridad en tiempo real nos iba informando cuantos gigas iba procesando, leídos y transferidos, así mismo se observó un gráfico que representaba la velocidad a la que está realizando las copias de seguridad.

Figura 8

Ejecución de la copia de seguridad Job VM facturación semanal



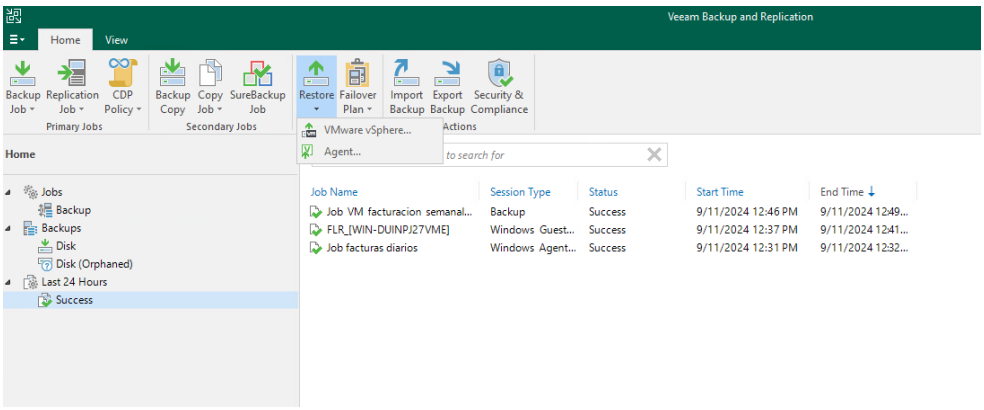
Nota. Se presenta la ejecución de la prueba de seguridad. Elaborado por: Los Autores.

3.5.2 Configuración para la restauración de máquinas virtuales y archivos en concreto

El procedimiento que se realizó fue la restauración de la copia de seguridad Job VM facturación semanal, el tipo de restauración fue Entire VM Restore que fue una recuperación de la máquina virtual completa.

Figura 9

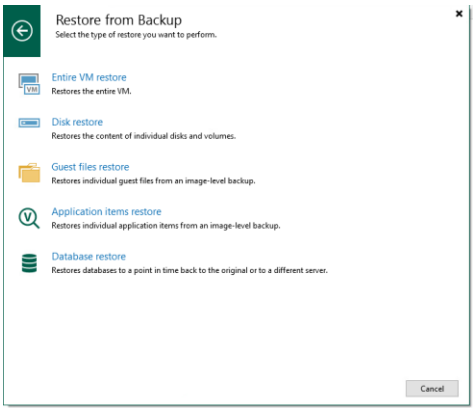
Restauración de la copia de seguridad Job VM Facturación semanal



Nota. Se presenta el procedimiento para la recuperación de la máquina virtual completa. Elaborado por: Los Autores.

Figura 10

Restauración tipo Entire VM Restore

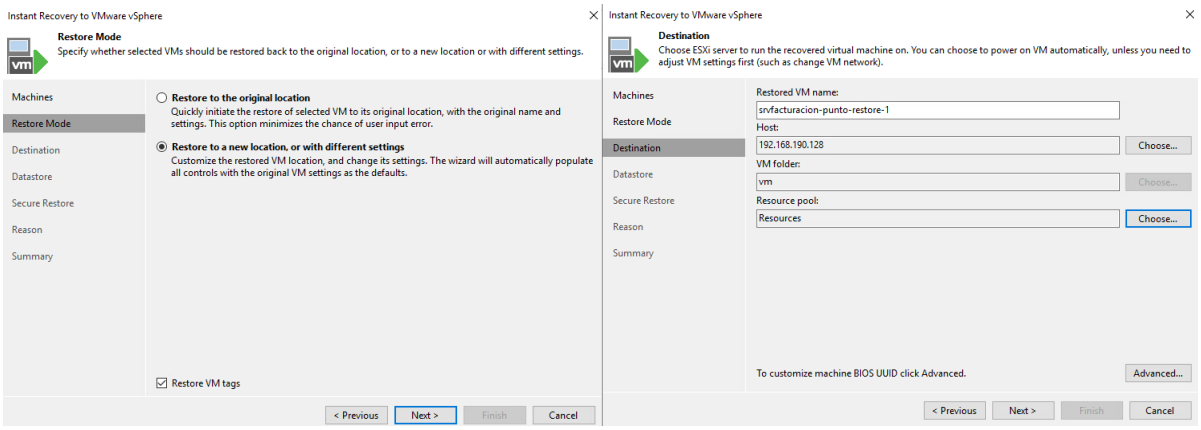


Nota. Se presenta el procedimiento para la recuperación de la máquina virtual completa. Elaborado por: Los Autores.

Se selecciona el backup que se realizó srvfacturación y se procede a restaurarlo a una nueva locación con el nombre srvfacturacion-punto-restore-1.

Figura 11

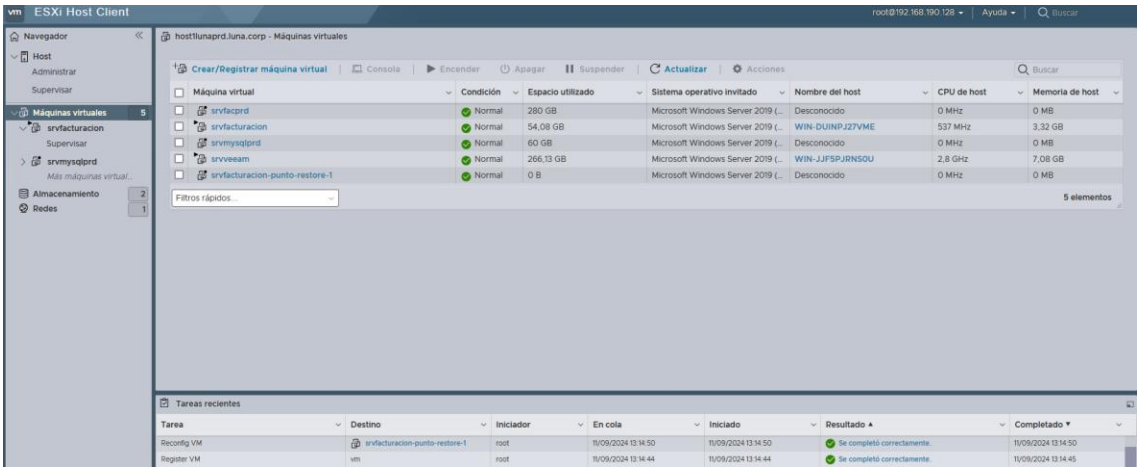
Restauración a nueva locación



Nota. Se presenta el procedimiento de restauración a nueva locación. Elaborado por: Los Autores.

Figura 12

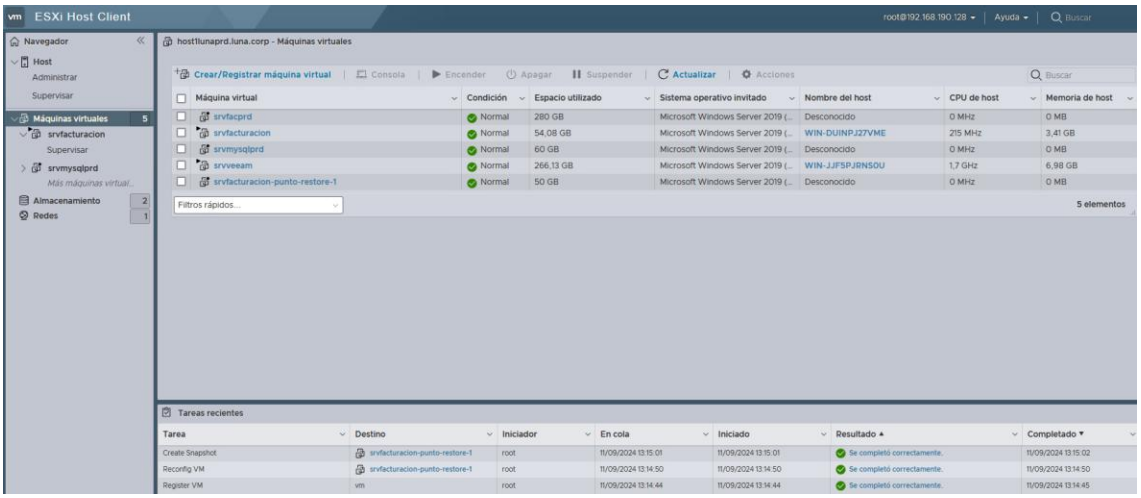
Evidencia previa a la ejecución de la restauración de la máquina virtual



Nota. Se presenta evidencia previa. Elaborado por: Los Autores.

Figura 13

Evidencia posterior a la ejecución de la restauración de la máquina virtual

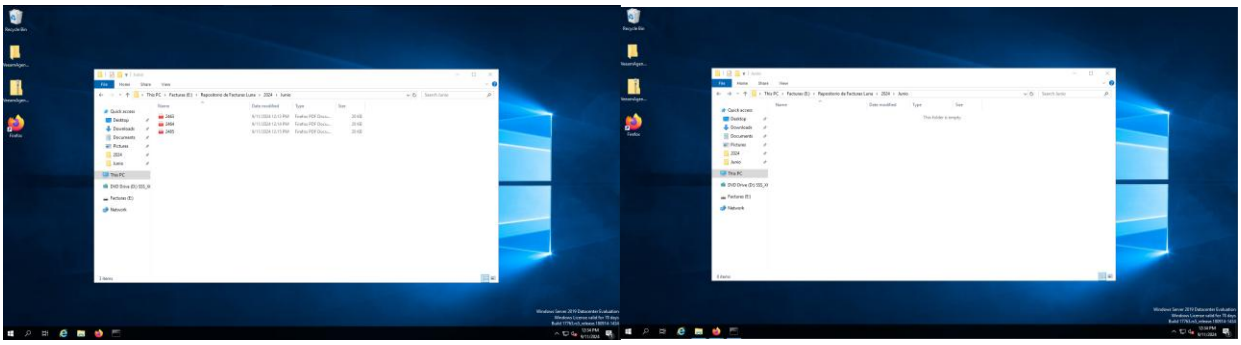


Nota. Se presenta evidencia posterior. Elaborado por: Los Autores.

Otro de los procedimientos que se realizó en Importadora Luna fue el trabajo de recuperación de archivos en concreto, para iniciar con esta fase, se eliminó la información del origen.

Figura 14

Eliminación de información en origen

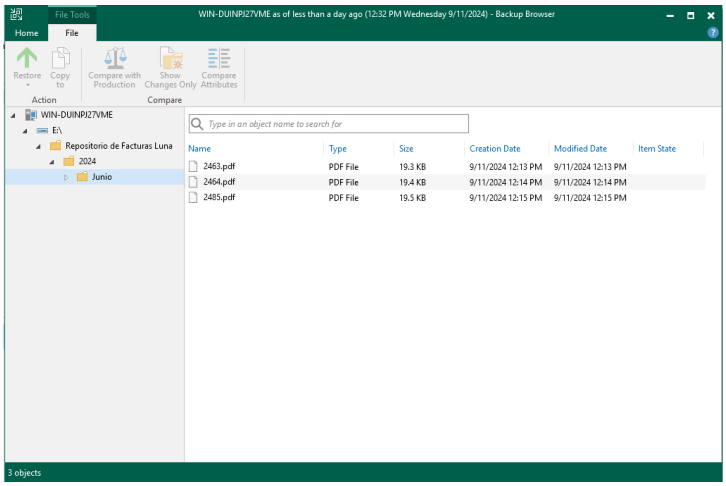


Nota. Se presenta evidencia de la eliminación de información en origen. Elaborado por: Los Autores.

Desde el servidor veeam backup & replication se escogió la opción de restauración de archivo, elegimos el sistema Windows y la máquina de la cual queremos recuperar el archivo. Del trabajo de copia realizado anteriormente es de donde vamos a restaurar el archivo en concreto, una vez que abra la copia de seguridad nos mostró un explorador desde el cual seleccionamos los archivos a recuperar, en el caso de Importadora Luna recuperamos el archivo 2463.pdf en el servidor original.

Figura 15

Selección del archivo a recuperar

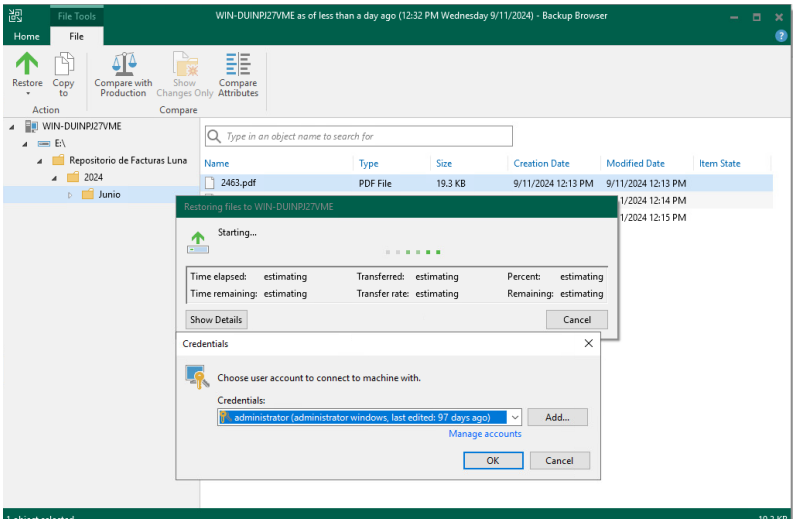


Nota. Se presenta la selección del archivo a recuperar. Elaborado por: Los Autores.

Una vez que se escoge el archivo, empieza con el proceso de restauración en donde solicitó las credenciales para esta máquina en concreto, e inicia el proceso de restauración.

Figura 16

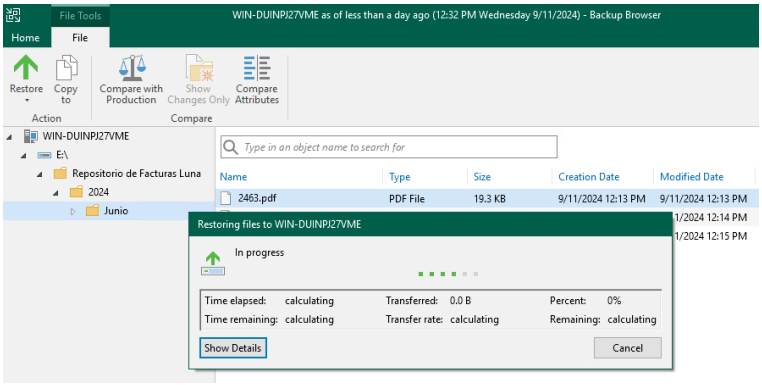
Ingreso de credenciales



Nota. Se presenta el ingreso de credenciales. Elaborado por: Los Autores.

Figura 17

Inicio del proceso de restauración



Nota. Se presenta la ejecución del proceso de restauración. Elaborado por: Los Autores.

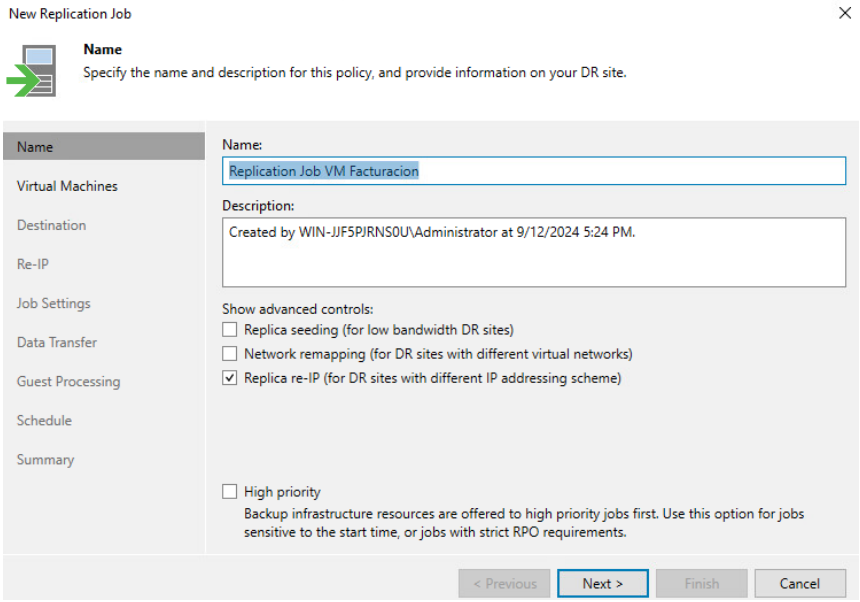
3.5.3 Configuración para la replicación de servidores

En primer lugar se define el nombre para este trabajo y se escogió la opción de replicar la configuración IP ya que esta permitió cambiar el esquema de direccionamiento IP para la máquina

virtual que sincroniza, se escoge la máquina virtual a replicar en nuestro caso srvfacturacion, a continuación se seleccionó el destino que fue el host agregado previamente al panel de inventario, se elige la carpeta en la máquina virtual y el almacén de datos en donde reside la máquina virtual replicada.

Figura 18

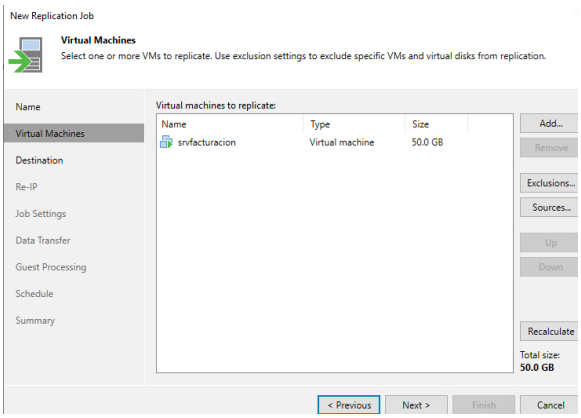
Inicio del proceso de replicación de servidores



Nota. Se presenta la ejecución del proceso de replicación de servidores Elaborado por: Los Autores.

Figura 19

Selección de la máquina virtual a replicar

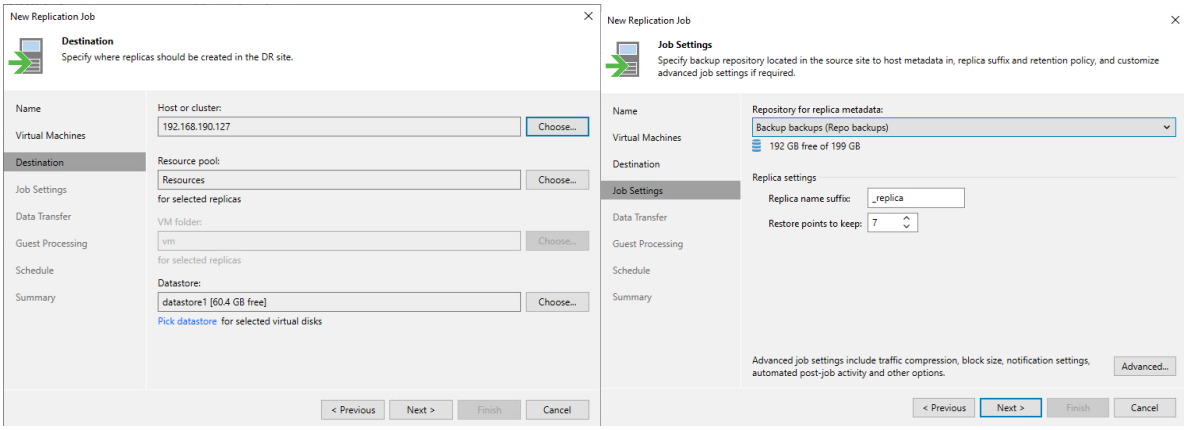


Nota. Se presenta la selección de la máquina virtual a replicar. Elaborado por: Los Autores.

El siguiente paso fue configurar la IP, se define la retención y el repositorio, se mantuvo el repositorio para metadatos, se colocó el sufijo _replica para poder identificarla como máquina virtual para recuperación de desastres y por último se definieron 7 puntos de restauración.

Figura 20

Configuración de la IP

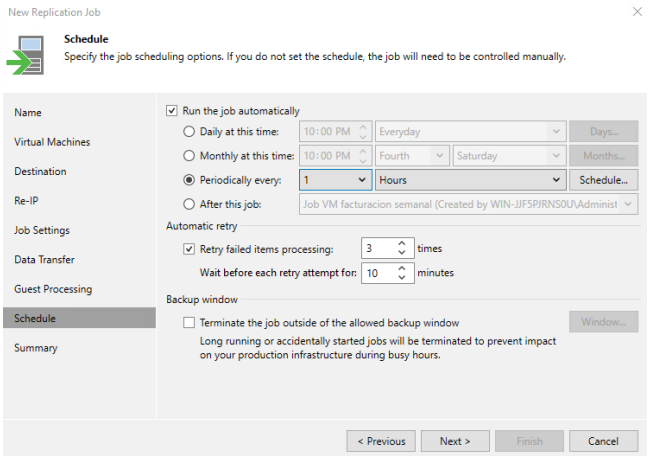


Nota. Se presenta la selección de la máquina virtual a replicar. Elaborado por: Los Autores.

Se configuró el cronograma definiendo la hora y días de ejecución del job de réplica, para Importadora Luna se sincronizará cada hora. Una vez configurado el trabajo de replicación se dio click en next y se ejecuta.

Figura 21

Fase final del proceso de replicación



Nota. Se presenta la fase final del proceso de replicación. Elaborado por: Los Autores.

CAPÍTULO IV

PRUEBAS Y RESULTADOS

4.1 Pruebas

Un plan de pruebas, además de garantizar que un sistema se ajuste a los lineamientos establecidos conforme a su diseño, permite depurar y solucionar problemas menores que puedan presentarse y con ello se logra que el sistema sea más completo y sólido. Las pruebas realizadas sobre la infraestructura son las siguientes:

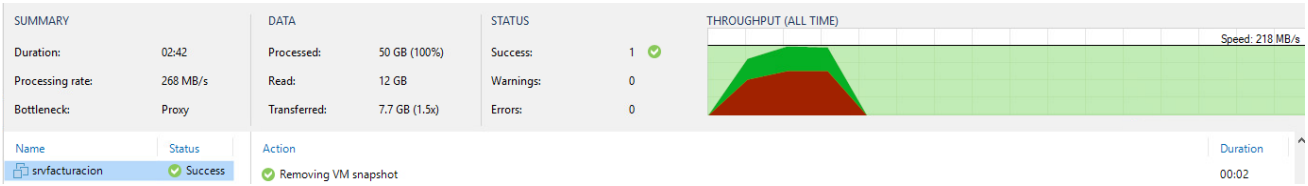
4.1.1 Copia de seguridad al repositorio de backup (Prueba 1)

En esta prueba se comprobó que las partes básicas del servicio de copia de seguridad funcionan correctamente. Están previstas múltiples copias desde máquinas virtuales al almacenamiento local.

A continuación, la figura 22 refleja los resultados satisfactorios de la prueba.

Figura 22

Prueba 1



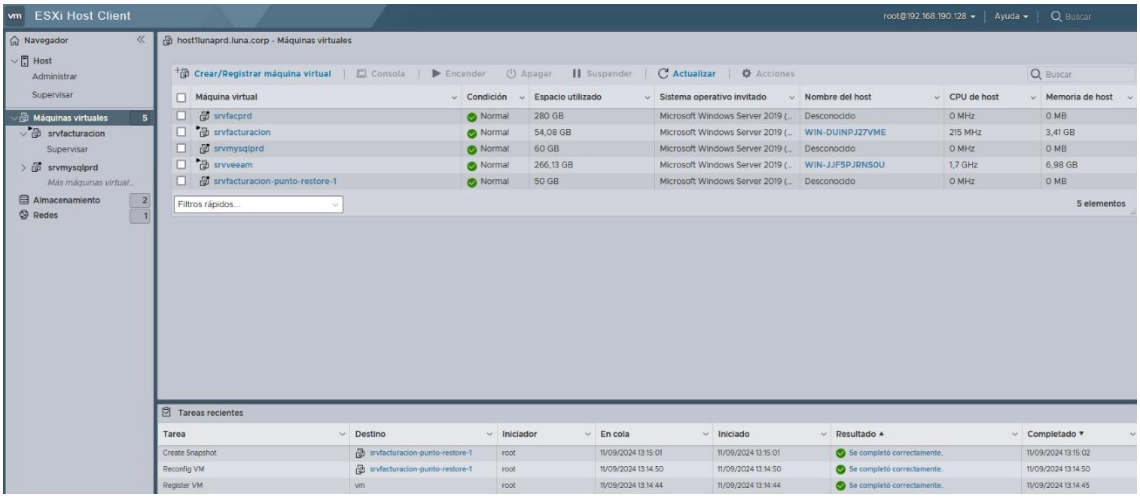
Nota. Se presentan los resultados de la prueba 1. Elaborado por: Los Autores.

4.1.2 Restauración de backups de la máquina virtual y archivos en concreto (Prueba 2)

El objetivo de esta prueba es verificar que se puede restaurar correctamente la máquina virtual completa desde la copia de seguridad creada anteriormente. Como se observa en la figura 23, los resultados son los esperados y las copias se sincronizan cuando llegan al repositorio remoto.

Figura 23

Prueba 2 Backup de la máquina virtual

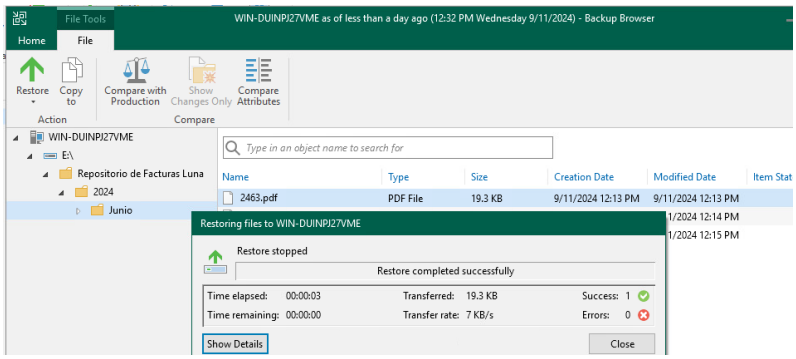


Nota. Se presentan los resultados de la prueba 2. Elaborado por: Los Autores.

Por otro lado, para realizar la prueba para restaurar un archivo en concreto, se eliminó la información del origen y esta prueba tiene como objetivo verificar que se puede restaurar correctamente el archivo eliminado anteriormente. Como se observa en la figura 24, los resultados son los esperados.

Figura 24

Prueba 2 Backup de un archivo en concreto



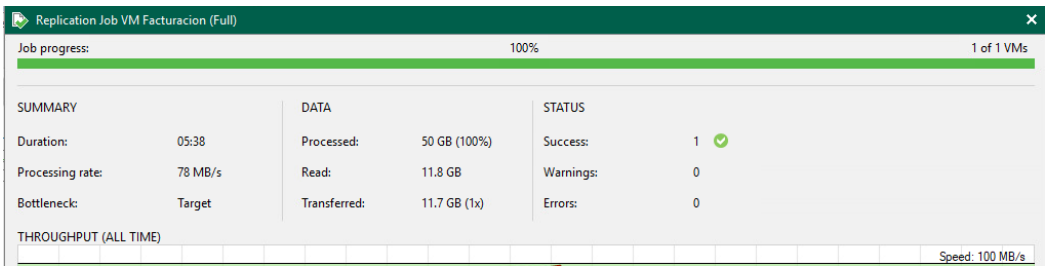
Nota. Se presentan los resultados de la prueba 2. Elaborado por: Los Autores.

4.1.3 Replicación de servidores (Prueba 3)

Esta prueba verifica que la réplica del servidor esté funcionando correctamente, como se indica en la figura 25, los resultados son los esperados y las copias se sincroniza cuando llega al almacenamiento remoto.

Figura 25

Prueba 3



Nota. Se presentan los resultados de la prueba 3. Elaborado por: Los Autores.

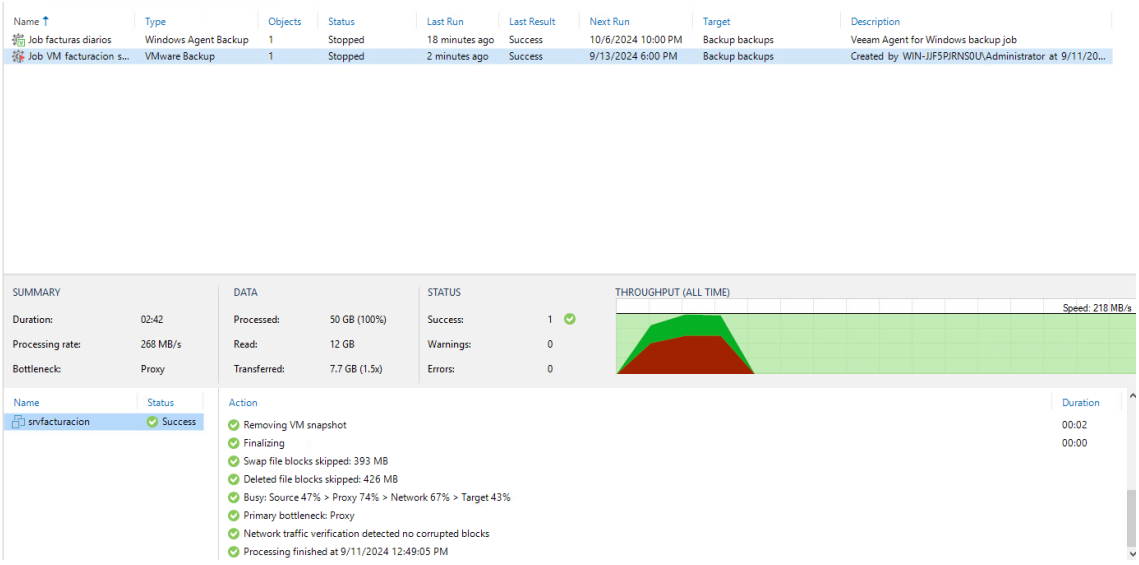
4.2 Resultados

4.2.1 Resultados Prueba 1

Durante el proceso de ejecución de la copia de seguridad en tiempo real nos iba informando cuantas gigas iba procesando, leídos y transferidos, así mismo se observó un gráfico que representaba la velocidad a la que está realizando las copias de seguridad observando que lo hizo bastante rápido (02 minutos, 42 segundos). Una vez que finalizó la copia de seguridad, se obtuvo como resultado que ha durado dos minutos cuarenta y dos segundos (02:42), ha procesado 50 GB y ha transferido 7.7 GB, como se observa en la figura 26.

Figura 26

Resultados Prueba 1



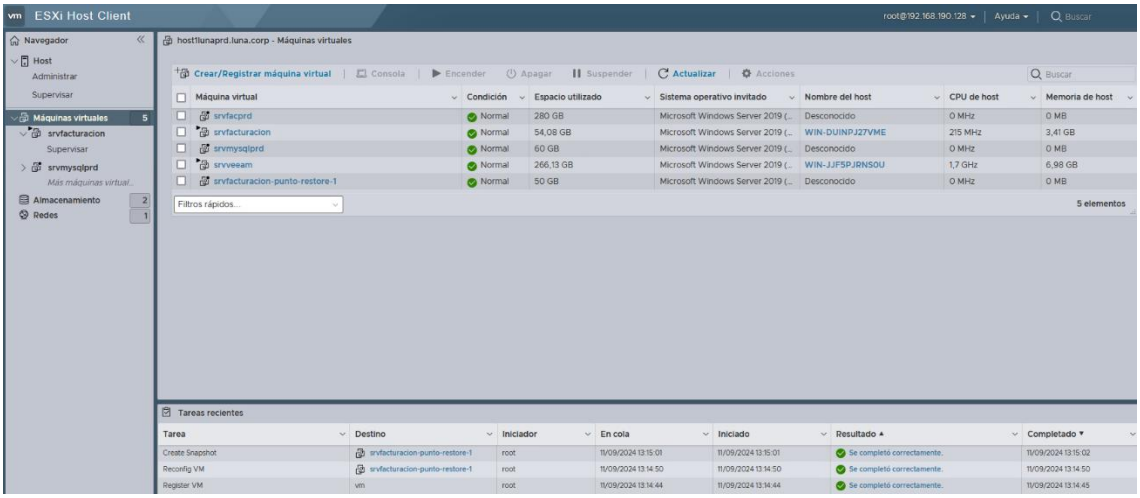
Nota. Se presentan los resultados de la prueba 1. Elaborado por: Los Autores.

4.2.2 Resultados Prueba 2

El tipo de restauración fue Entire VM Restore que fue una recuperación de la máquina virtual completa, se seleccionó el backup que se realizó anteriormente srvfacturación y se procedió a restaurarlo a una nueva locación el nombre srvfacturacion-punto-restore-1. En la restauración de la máquina virtual no existieron inconvenientes: Punto de restauración 1.

Figura 27

Resultados Prueba 2. Restauración de la máquina virtual

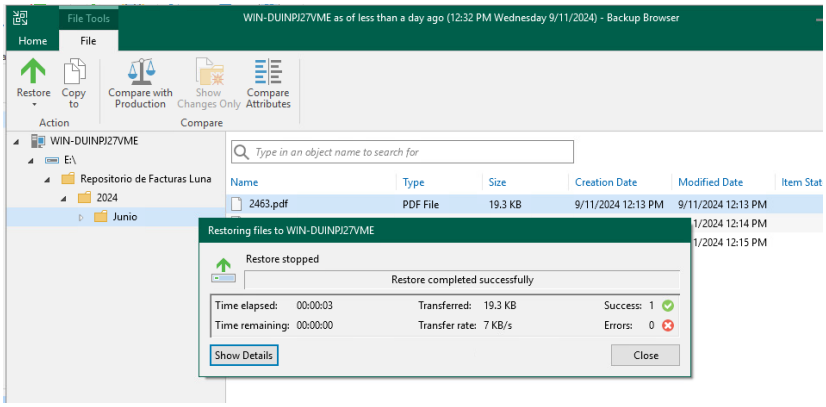


Nota. Se presentan los resultados de la prueba 2. Elaborado por: Los Autores.

Del trabajo de copia realizado anteriormente es de donde se restauró el archivo en concreto, una vez que abrió la copia de seguridad se mostró un explorador desde el cual se seleccionaron los archivos a recuperar, en el caso de Importadora Luna se recuperó el archivo 2463.pdf en el servidor original. El proceso de restauración se llevó a cabo en su totalidad como se observa en la figura 28.

Figura 28

Resultados Prueba 2. Restauración de archivo en concreto



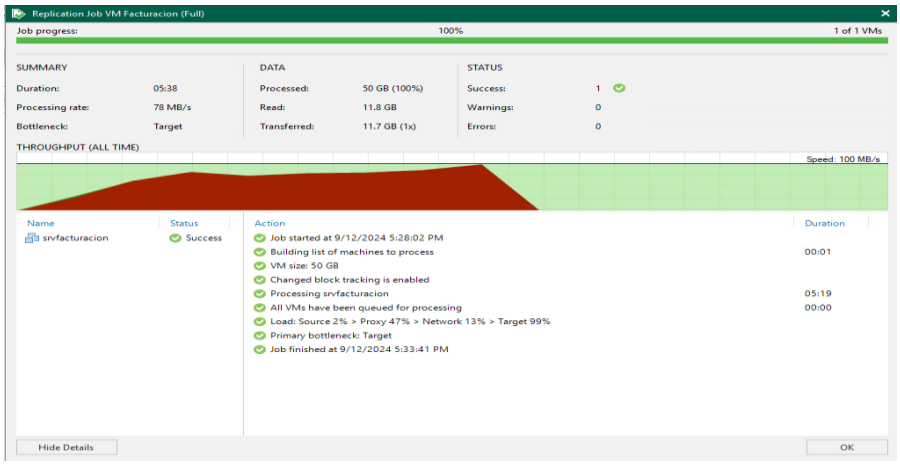
Nota. Se presentan los resultados de la prueba 2. Elaborado por: Los Autores.

4.2.3 Resultados Prueba 3

Como resultado el trabajo de replicación Job VM facturación tuvo una duración de 5 minutos 38 segundos, procesó 50GB y transferido 11.7GB, como se observa en la figura 29.

Figura 29

Resultado Prueba 3



Nota. Se presentan los resultados de la prueba 3. Elaborado por: Los Autores.

4.3 Análisis de resultados

De acuerdo al diseño de una metodología para el respaldo y replicación de servidores implementada en Importadora Luna, ahora el 100% de la información del servidor esta adecuadamente protegida contra cualquier siniestro, la copia de seguridad procesó 50GB y transfirió 7.7 GB en tan solo dos minutos cuarenta y dos segundos, lo que representa un proceso completo al realizar un backup del 100% de la información de la máquina virtual, por otro lado el trabajo de replicación de servidores tuvo una duración de 5 minutos 38 segundos, procesando 50GB y transfiriendo 11.7GB representando así mismo una replicación completa. El software Veeam Backup & Replication es una herramienta automatizada y modular lo que permitió adaptarla a las necesidades de Importadora Luna.

CONCLUSIONES

Se creó exitosamente una metodología que se adapta a las necesidades de Importadora Luna, la cual es automatizada, flexible y estándar, por lo cual es capaz de adaptarse y ampliarse según las necesidades de cualquier organización, y de esta manera ser implementada fácilmente; asegurando la recuperación de información mediante copias de seguridad y replicación de servidores.

Cumpliendo con uno de los objetivos del trabajo investigativo, la metodología fue evaluada en un estudio de caso real llevado a cabo en Importadora Luna, con el fin de conocer su factibilidad de implementación. Gracias a esta evaluación, fue posible identificar y corregir errores, así como analizar distintas alternativas de configuración antes de llevar a cabo la implementación de la herramienta en Importadora Luna. Esto permitió verificar su funcionamiento adecuado previo a la ejecución de la fase de pruebas de efectividad.

Se realizaron pruebas de efectividad para copia de seguridad, restauración de backups y replicación de servidores, obteniendo como resultados: la copia de seguridad procesó 50GB y transfirió 7.7GB lo que representó que respaldó el 100% de la información en un lapso de dos minutos cuarenta y dos segundos, la replicación de servidores tomo un poco más de tiempo que fueron cinco minutos treinta y ocho segundos, procesando 50GB y transfiriendo 11.7GB, este proceso también fue satisfactorio, lo que demuestra la viabilidad de la metodología.

La implementación del diseño de la metodología en Importadora Luna permitió, en el área administrativa crear copias de seguridad mensuales, en el área operativa interacción entre el operador y el sistema, verificando que la programación se ejecute correctamente adicional a esto desde una perspectiva económica, se busca reducir el uso de equipos de respaldo al optimizar su normalización y utilización eficiente.

Actualmente al Importadora Luna contar con una metodología para el respaldo y replicación de servidores tiene la ventaja de ahorrar tiempo al mejorar la disponibilidad y facilitar la recuperación ante desastres, y ahorrar dinero al reducir las pérdidas de datos, la inactividad y los costos asociados con la recuperación de información, la inversión en esta tecnología es muy rentable a largo plazo.

Por lo mencionado anteriormente este trabajo se propone como una guía para justificar la inversión en una herramienta automatizada de respaldos y replicación, destacando la importancia de tener acceso a la información durante una contingencia o en situaciones de necesidad específica. Se pone especial énfasis en los costos y riesgos asociados a la falta de disponibilidad de los datos en momentos críticos.

RECOMENDACIONES

Todo proyecto debe gestionarse de forma formal, aplicando estándares previamente definidos y aceptados. Una lección clave que se ha aprendido es la importancia de dividir los proyectos en fases, aplicando una gestión profesional que garantice un control adecuado del tiempo, los costos y los recursos. Estas tres características deben mantenerse equilibradas para asegurar la entrega de un producto final de calidad.

Es fundamental efectuar ensayos regulares de recuperación de datos para confirmar la integridad de los datos y garantizar la fiabilidad de la solución aplicada., así como para comprobar el correcto funcionamiento de los dispositivos de red. Estas pruebas garantizan que, en caso de contingencia, los datos puedan ser restaurados de manera eficaz y sin pérdidas.

Tanto las entidades públicas como las privadas deberían disponer de un servidor exclusivo para guardar datos, empleando un programa de software que automatiza este procedimiento. Esto garantizaría la disponibilidad e integridad de los datos, contribuyendo así a la continuidad de los servicios y reduciendo los riesgos asociados a la pérdida de información en situaciones críticas.

REFERENCIAS

Areitio, J. (2008). *Seguridad de la información*. En *Redes, informática y sistemas de información* (p. 270). Paraninfo.

Broadcom. (2023). *VMware*. https://www.vmware.com

Cajamarca, J. S. (2019). *Plan de recuperación de desastres de la infraestructura de tecnologías de información para empresas de prestación de servicios tecnológicos* [Tesis de pregrado, Universidad Tecnológica Israel].

Cama, A. (2012). *Las redes de sensores inalámbricos y el Internet de las cosas*.

Campos, F. (2020, febrero 25). *Industrial M2M*. https://www.m2mlogitek.com/que-es-lorawan/

Chango, W., Sayago, J., Orozco, F., & Jácome, L. (2017). Análisis, diseño e implementación de un sistema de respaldo de datos y restauración de la información basado en software AVAMAR. *Revista Científica y Tecnológica UPSE*, *4*, 111–121.

Delgado, F. (2018). *Taller de implementación de la norma ISO 27001*. Universidad Peruana Unión.

Desongles, J., Balongo, M., & Ochoa, O. (2002). *Informática para oposiciones de la Comunidad Autónoma de las Illes Balears: Temario común y test* (pp. 66–67). MAD.

Figueroa, J., Rodríguez, R., Saltos, J., & Bone, C. (2021, marzo 11). La seguridad informática y la seguridad de la información. *Revista Multidisciplinar de Innovación y Estudios Aplicados*.

Giraldo, V. (2019, febrero 14). *Plataformas digitales: Qué son y cómo aprovecharlas*. Rock Content. https://rockcontent.com/es/blog/plataformas-digitales/

GlobalSuite Solutions. (2023, septiembre 22). *¿Qué es la norma ISO 27001 y para qué sirve?* https://www.globalsuitesolutions.com/es

Hernández, J. M. (2021). *Diseño de una solución integral de backup y disaster recovery* [Tesis de maestría, Universitat Oberta de Catalunya].

IBM. (2016). *International Business Machines*.

Interxion. (2015). *Centro de datos*. http://www.interxion.com/es/centros-de-datos/

Jiménez, G. D. (2017). *Implementar una solución de respaldos de archivos de configuración de los sistemas, servidores, equipamiento de red y bases de datos en el centro de datos de la Universidad Nacional de Loja* [Tesis de pregrado, Universidad Nacional de Loja].

LoRa. (s.f.). *Why LoRa?* https://www.semtech.com/lora/why-lora

Lora, A. (2020, noviembre 16). *About LoRa Alliance*. LoRa Alliance. https://lora-alliance.org/about-lora-alliance/

Maldonado, J. (2022). *Diseño de un centro de datos basado en estándares* [Tesis de pregrado, Universidad de Cuenca].

Marchionni. (2011). *Administrador de servidores: Herramientas, consejos y procedimientos*. Buenos Aires.

Marchionni. (2021). *Administrador de servidores*. USERS.

Quishpe, V. P. (2007). *Definición e implementación de un modelo de respaldos de información en la compañía Transelectric S.A.* [Tesis de pregrado, Escuela Politécnica Nacional].

Rock, T. (2020). *23 disaster recovery statistics you should know*. Invenio IT. https://invenioit.com/continuity/disaster-recovery-statistics/

Santos, R. (2019, junio). *ESP32/ESP8266: Conexión a base de datos MySQL con PHP*. Random Nerd Tutorials. https://randomnerdtutorials.com/esp32-esp8266-mysql-database-php/

Schwaber, K., & Sutherland, J. (2017). *La guía de Scrum: La guía definitiva para Scrum: Las reglas del juego*. https://scrumguides.org/docs/scrumguide/v2017/2017-Scrum-Guide-Spanish.pdf

Segu-info. (2016, diciembre 2). *Seguridad física*. http://www.segu-info.com.ar

Terán, D. G. (2013). *Implementación de un sistema de respaldo para los servidores de la carrera de Ingeniería en Sistemas Computacionales con tecnología Open Source, utilizando Bacula* [Tesis de pregrado, Universidad de Guayaquil].

Valdivia, C. (2017). *Informática industrial*. Ediciones Paraninfo. https://ingjpasuagrm.files.wordpress.com

Veeam Software. (2019). *Veeam Backup & Replication*. https://www.veeam.com

Veeam Software. (2023, agosto 21). *Veeam Backup & Replication*. https://www.veeam.com

Veeam Software. (2025, enero 16). *Veeam Backup & Replication support for vSphere*. https://www.veeam.com/kb2443

Elabora una foto en tamaño cuadrado para LinkedIn, mostrando a un hombre de confianza. la foto debe ser simulada en un estudio de fotografía especialistas en blanco y negro. el usuario está utilizando una camisa blanca, un saco con una postura relajada. la foto debe de transmitir seguridad, confianza y un aura de alegría a la vez, utiliza la iluminación a tu criterio, por último y más importante, debes de mantener el rostro original sin hacer ningún cambio, debe mostrarse tal cual la foto