UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

HERRAMIENTAS PARA RESPALDAR LA INFORMACIÓN EN MÁQUINAS VIRTUALES DE FORMA ÓPTIMA Y SEGURA APLICADO A UNA EMPRESA FARMACEUTICA

Trabajo de titulación previo a la obtención del título de Magíster en Computación con Mención en Seguridad Informática

Línea de investigación: Desarrollo, aplicación de software y cybersecurity (seguridad cibernética)

AUTOR:

Ing. Edgar Ivan Paucar Columba

DIRECTOR:

PhD. José Antonio Quiña Mera

Ibarra – Ecuador 2025

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 11 de junio de 2025

PhD. José Antonio Quiña Mera

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en constancia, autorizo para los finales legales pertinentes.

JOSE ANTONIO QUIÑA MERA

Firmado digitalmente por JOSE ANTONIO QUIÑA MERA
Nombre de reconocimiento (DN): c=EC, sn=QUIÑA MERA, givenName=JOSE ANTONIO, serialNumber=IDCEC-1002322384, cn=JOSE ANTONIO QUIÑA MERA, 2.5.4.97=TINEC-1002322384001

(f)……

PhD. José Antonio Quiña Mera

C.C: 100232238-4

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	172185249-7		
APELLIDOS Y NOMBRES	Edgar Ivan Paucar Columba		
DIRECCIÓN	La Armenia 2, Sebastián de Benalcázar		
EMAIL	eipaucarc@utn.edu.ec		
TELÉFONO FIJO	02190590	**TELÉFONO MÓVIL:**	0987179937

DATOS DE LA OBRA	
TÍTULO:	HERRAMIENTAS PARA RESPALDAR LA INFORMACIÓN EN MÁQUINAS VIRTUALES DE FORMA ÓPTIMA Y SEGURA APLICADO A UNA EMPRESA FARMACEUTICA.
AUTOR (ES):	Edgar Ivan Paucar Columba
FECHA: DD/MM/AAAA	11/06/2025

SOLO PARA TRABAJOS DE GRADO	
PROGRAMA DE POSGRADO	☐ **PREGRADO** ■ **POSGRADO**
TITULO POR EL QUE OPTA	Maestría en Computación con Mención en Seguridad Informática
TUTOR	PhD. José Antonio Quiña Mera

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 11 días del mes de junio del 2025

EL AUTOR:

(f)

Edgar Ivan Paucar Columba

C.C.:1721852497

DEDICATORIA

A Dios, fuente de sabiduría y fortaleza, por guiarme en cada paso de este viaje académico y por brindarme la fe para superar los desafíos.

A mi esposa amada, Lizbeth Albuja, cuya paciencia, amor incondicional y apoyo constante han sido la luz que me ha guiado a lo largo de este proceso. Eres mi inspiración y mi mayor alegría.

A mi familia, por su aliento y comprensión en cada momento de incertidumbre. Vuestra fe en mí ha sido el pilar sobre el cual he construido este logro.

Edgar Ivan Paucar Columba

AGRADECIMIENTO

Quiero agradecer primero a Dios, cuya guía y fortaleza me han acompañado en cada etapa de este camino académico. Su sabiduría y su gracia han sido mi mayor fuente de inspiración y apoyo.

A mi esposa amada, Lizbeth Albuja, por su paciencia, amor incondicional y aliento constante. Tu presencia y comprensión han sido fundamentales para alcanzar este logro. Sin tu apoyo, este proyecto no habría sido posible.

A mi familia, por su amor inquebrantable y su constante respaldo. Vuestra confianza en mí y vuestra paciencia a lo largo de este proceso han sido un pilar esencial para completar esta etapa.

Al coordinador del programa, a mis profesores que cuya dedicación y pasión por la enseñanza han sido una fuente de conocimiento invaluable. Vuestra orientación y apoyo han enriquecido profundamente mi formación académica, también al director de tesis, PHD. Antonio Quiña, por su guía experta y su constante apoyo durante todo el proceso. Su *feedback* constructivo y su compromiso han sido cruciales para el desarrollo de esta investigación.

Con profunda gratitud,

Edgar Ivan Paucar Columba

Índice de contenido

Índice de tablas

Índice de ilustraciones

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

HERRAMIENTAS PARA RESPALDAR LA INFORMACIÓN EN MÁQUINAS VIRTUALES DE FORMA ÓPTIMA Y SEGURA APLICADO A UNA EMPRESA FARMACEUTICA

Autor: Ing. Edgar Ivan Paucar Columba
Director: PhD. José Antonio Quiña Mera
Año: 2025

Resumen

Las organizaciones enfrentan constantemente riesgos que pueden comprometer la seguridad de la información y la disponibilidad de sistemas y bases de datos críticos. Estos riesgos pueden originarse por diversas causas, como desastres naturales, amenazas cibernéticas, ataques de malware, cortes de energía, eliminación accidental de datos o ataques deliberados. Estos factores representan un desafío significativo para la integridad y continuidad operativa de una organización.

Este estudio tiene como objetivo evaluar herramientas que faciliten la gestión de máquinas virtuales, incorporando medidas de seguridad esenciales para la protección de los datos en una empresa farmacéutica. Para ello, se llevará a cabo un proceso de benchmarking, definiendo los atributos y métricas clave para identificar la herramienta más adecuada en la estimación de costos asociados a una aplicación.

Se emplea una metodología de investigación cualitativa, lo que permite la recopilación y el análisis detallado de información relevante. Este enfoque facilita la identificación de soluciones eficaces para la copia de seguridad de datos y el desarrollo de un plan de seguridad integral, adaptado al contexto farmacéutico, garantizando así la protección de la información crítica y la resiliencia operativa de la organización.

PALABRAS CLAVES: Ciberataques, Máquinas virtuales, Protección de datos.

Abstrac

Organizations constantly face risks that can compromise information security and the availability of critical systems and databases. These risks originate from diverse sources, including natural disasters, cyber threats, malware attacks, power outages, accidental data deletion, and deliberate cyberattacks. Such factors pose significant challenges to maintaining an organization's integrity and operational continuity.

This study aims to evaluate tools that facilitate the management of virtual machines while integrating essential security measures to safeguard the data of a pharmaceutical company. Therefore, a benchmarking process will be conducted, defining key attributes and metrics to identify the most suitable tool for estimating application-related costs.

A qualitative research methodology enables the systematic collection and in-depth analysis of relevant data. This approach allows for identifying effective data backup solutions and developing a comprehensive security plan tailored to the pharmaceutical sector, ensuring the protection of critical information and the resilience of organizational operations.

KEY WORDS: Cyberattacks, Virtual machines, Data protection.

CAPITULO I

1 EL PROBLEMA

1.1 PROBLEMA DE INVESTIGACIÓN

En toda organización en algún momento se tiene el problema de estar corriendo el riesgo de un incidente que ocasione perdida de información e indisponibilidad de sistemas o bases de datos que hacen funcionar a la empresa. Los motivos o causas que podemos encontrar se deben a factores como: desastres naturales, amenazas de ciberdelincuentes, *malware*, cortes eléctricas, borrados accidentales del personal, ciberataques, entre otros; (Veeam, 2023) ocasionando fallas en los sistemas y dejando días sin la operación requerida, generando pérdidas económicas por no solventar de forma inmediata y oportuna con un respaldo del sistema.

Un riesgo grave es la pérdida de datos, ya que se dedicará tiempo y recursos en recuperar la información eliminada, y afectará a la producción o incluso a la viabilidad futura de la empresa. En algunos casos, la pérdida de datos puede significar que perdemos, literalmente, a todos nuestros clientes.

Las pérdidas económicas serán inevitables, esto significa que perderemos todo el valor que con tanto esfuerzo se ha ido acumulando y muchas veces hay que empezar desde cero. Esto se traduce en unas pérdidas incalculables que pueden llevar a la organización a la ruina. (Arcys, 2019)

Las medidas de seguridad informática se han convertido en prioritarias, especialmente para las empresas o entidades que dependen casi al 100% de Internet en sus operaciones.

El problema que se identifica en las organizaciones es el riesgo de pérdida de información ante posibles amenazas o posibles ataques cibernéticos, los más comunes son:

Ciberataque: Es una acción que intenta exponer información utilizando varios métodos de ciberataque como: *malware*, phishing, *ransomware*, denegación de servicio y muchos más para robar, cambiar, destruir datos sensibles, utilizando una o más equipos para ingresando por puertos vulnerables en la red con un acceso no autorizado. Según lo menciona en su página (POINT, 2023)

Malware o software malicioso: Es uno de los primeros en aparecer y el más conocido, término amplio que contempla diferentes clases de software malicioso, incluyendo virus, gusanos, spyware y otros aprovechan las vulnerabilidades de los sistemas o equipos informáticos para plantar el código nocivo. (Jaimovich, Invgate, 2022)

Phishing: El término proviene de *fish*, que significa 'pesca' en inglés. Es uno de los tipos de ataques informáticos más frecuentes también conocido como pesca de usuarios. Es un tipo de ataque malicioso que consiste en recibir correos electrónicos que parecen provenir de fuentes fiables, pero en realidad, contienen un enlace que pone en riesgo información y otros datos personales o empresariales. (digital, 2022)

Ransomware o secuestro de datos: Un software malicioso que representa un riesgo porque incluye un código malicioso que cifra los datos para hacerlos inaccesibles a la víctima. Este programa suele utilizarse para exigir el pago de un rescate para que la víctima pueda descifrar los archivos, carpetas y sistemas cautivos. (Kaspersky, 2022)

Día cero: Es una vulnerabilidad que no fue revelada públicamente. Los hackers aprovechan ese momento antes de que el proveedor tenga la oportunidad de solucionarlo. Suele ser muy peligroso porque no hay protección hasta que se publica el parche. (Kaspersky, 2021)

Ataque de troyanos: La principal forma de ataque de troyanos es ser escondido o camuflado dentro de un archivo o aplicación, cambiando hasta el icono para no ser detectado y engañar al usuario. Se diseñan para cometer diferentes formas de ataque o daños en los equipos o en la red, dependiendo la acción que se pretende realizar. (Jaimovich, Invgate, 2024)

Ataque de inyección SQL: Sus principales ataques son los sitios que contiene base de datos para obtener acceso no autorizado consultas estructuradas de una aplicación web añadiendo una cadena de código malicioso. Al ingresar el código malicioso permite al atacante obtener información confidencial y sensible, como la correspondiente a las tarjetas de crédito. (Jaimovich, Invgate, 2024)

Cross-site scripting: También se le conoce como XSS su principal forma de trabajar es buscar fallas en la seguridad de los sitios web para luego ser procesado y ejecutado por el usuario atacante, cuando esto ocurre, el atacante obtiene el control y compromete la interacción con la aplicación, accediendo a cualquier acción que desee ejecutar como un URL de *payload* para obtener datos personales de usuarios, tarjetas de crédito, implementar técnicas de ingeniería social y entre otras. (Báez, 2021)

Rootkits: Es un grupo de herramientas de software que permiten a los delincuentes obtener acceso a equipos o software no autorizado a un sistema sin ser detectados y proceder con el robo de información. Cuando el *rootkit* se activa, se crea

una puerta trasera y los delincuentes pueden instalar otras formas de *malware* como *ransomware* o troyanos. (Burdova, 2022)

Amenaza interna: Para cerrar los tipos de ciberataque, la amenaza interna involucra a las personas que trabajan dentro de una organización y que utilizan el acceso autorizado o sus conocimientos sobre la entidad para lanzar un ataque. El ataque de amenaza interna puede provocar daños y pérdidas de datos y afectar a la reputación de la empresa. (Jaimovich, Invgate, 2022)

Las amenazas cibernéticas representan el principal riesgo para una empresa, ya que la posible infección o ataque de ciberdelincuentes puede resultar en la pérdida de información crítica, especialmente si no se cuenta con un plan de contingencia adecuado ni con una herramienta que permita realizar respaldos de los servidores virtuales. Esto pone en peligro la integridad de la información, las bases de datos y los programas esenciales para el funcionamiento de las empresas farmacéuticas. En el caso específico de la empresa farmacéutica seleccionada como estudio, la falta de una herramienta de respaldos la expone a la pérdida de datos debido a ataques o fallas, sin garantizar la disponibilidad inmediata de la información. Este problema se ve agravado por la ausencia de un departamento de tecnología, lo que impide la implementación de políticas de respaldo y seguridad de la información.

1.2 Interrogantes de la investigación

En base al problema identificado se consideran las siguientes preguntas o interrogantes de investigación.

¿Qué herramientas comerciales y *open source* permiten sacar respaldos de máquinas virtuales y consideran aspectos de seguridad?

¿Cuál de las herramientas comerciales y *open source* se puede aplicar al caso de estudio?

¿Qué plan de respaldo de datos consideraría implementar en la empresa farmacéutica tomada como caso de estudio considerando la seguridad de la información?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Analizar herramientas que permitan respaldar la información de máquinas virtuales considerando aspectos de seguridad aplicables a una farmacéutica para salvaguardar adecuadamente su información.

1.3.2 Objetivos específicos

- Realizar un estudio comparativo de diferentes herramientas comerciales y *open source* para la realización de respaldos de máquinas virtuales de la organización considerando aspectos de seguridad como el tipo de cifrado de datos y análisis de virus.
- Analizar en un entorno simulado las ventajas del uso de herramientas comerciales y *open source* para determinar la que mejor se adapte al caso de estudio.
- Desarrollar un plan de respaldo de datos considerando las necesidades de seguridad de la información de la empresa farmacéutica.

1.4 Alcance

Desde: La selección de un software comercial y *open source* que nos permita realizar respaldos de nuestros servidores de forma segura.

Hasta: Infectar con algún programa maligno los servidores y respaldar las máquinas virtuales instaladas con Windows Server 2019 y Linux Ubuntu 22.

Se llevarán a cabo dos casos de estudio: uno utilizando VMware Backup & Replication como software comercial y otro con UrBackup como solución *open source*. El objetivo es evaluar aspectos clave de ambos programas, como su descarga, proceso de instalación, la interfaz de usuario en el entorno cliente-servidor, las opciones de cifrado y compresión de archivos, el soporte técnico y su capacidad para detectar *malware* durante la realización de las copias de seguridad.

Caso 1 Hyper-V y VMware Backups & Replication

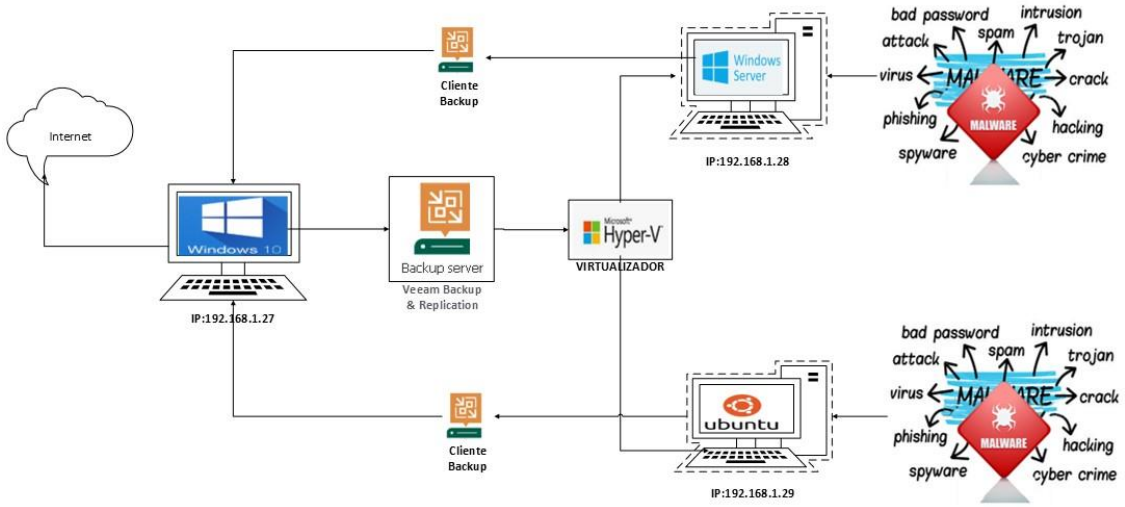


Ilustración 1 Hyper-V VMware

Caso 2 VMware Workstation 17 Pro y UrBackup

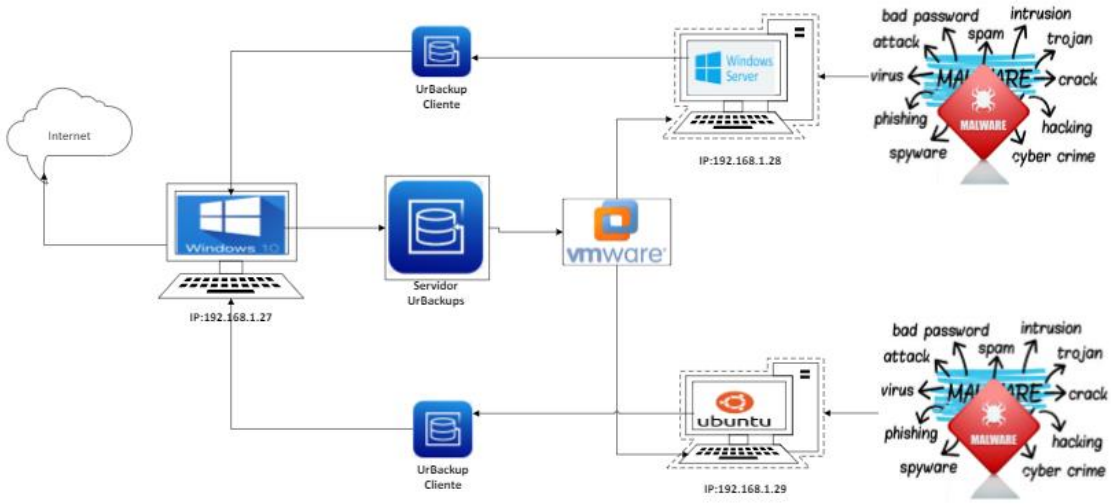


Ilustración 2 VMware y UrBackup

1.5 Hipótesis de trabajo

Las herramientas que permitan respaldar la información de máquinas virtuales considerando aspectos de seguridad aplicables a una farmacéutica permitirán salvaguardar adecuadamente la información.

1.6 Hipótesis alternativa

Las herramientas que permitan respaldar la información de máquinas virtuales considerando aspectos de seguridad aplicables a una farmacéutica no permitirán salvaguardar adecuadamente la información.

1.7 Categorización de variables

Variable independiente: Las herramientas que permitan respaldar la información de máquinas virtuales considerando aspectos de seguridad aplicables a una farmacéutica.

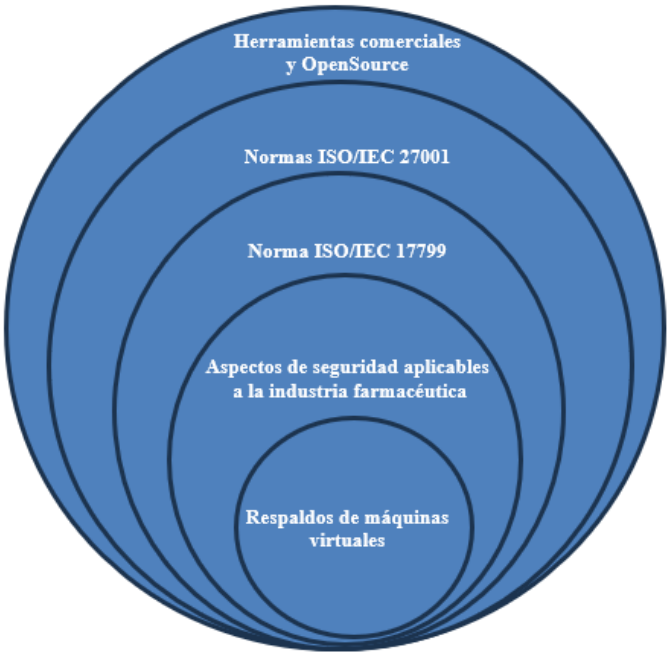


Ilustración 3 Variable dependiente: Salvaguardar adecuadamente la información

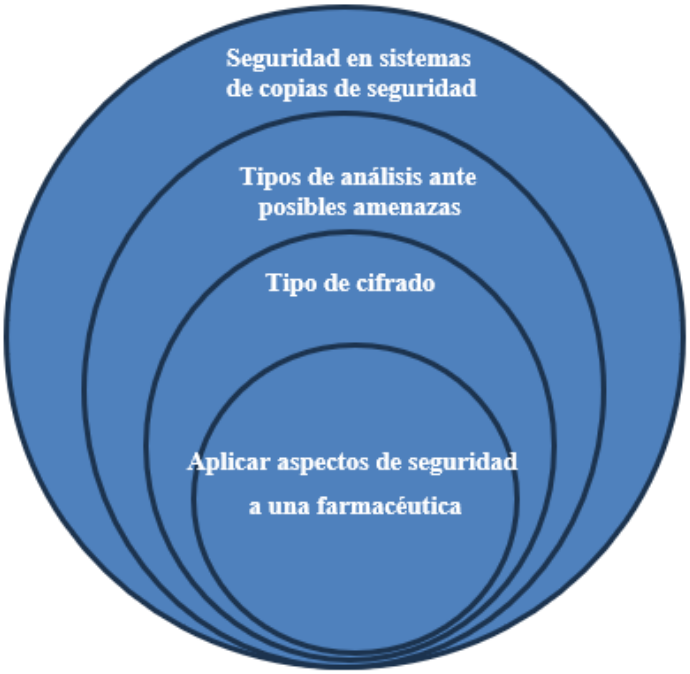


Ilustración 4 Temas específicos de la seguridad de la información

1.7 Justificación

La justificación radica en la importancia de garantizar la integridad, disponibilidad y confidencialidad de los datos críticos en un entorno altamente regulado en la industria farmacéutica. Dado al crecimiento de riesgos como

ciberataques, desastres naturales, errores operativos humanos, errores tecnológicos, entre otros.

Por lo antes mencionado, es crucial contar con herramientas específicas que optimicen y aseguren los procesos de respaldo de información para cumplir con los estándares de seguridad y calidad requeridos por las autoridades reguladoras. Además, la protección de la propiedad intelectual y la continuidad del negocio son aspectos fundamentales que respalden la relevancia de esta investigación.

El estudio realizado recomienda la importancia de contar con normas, políticas y métodos de copias de seguridad que se necesita implementar en las empresas farmacéuticas, por ejemplo, usar la regla 3,2,1, que deben tener las compañías, es un método para realizar copias de seguridad que permite el acceso a una copia de seguridad segura y confiable. Se utilizarán al menos dos soportes distintos para realizar estas copias y uno de ellos tiene que estar siempre fuera de la empresa (Cloud) con esto se evitara en caso de tener una copia infectada o ser víctima de ciberataque contar con otra copia de seguridad disponible para realizar la restauración o recuperación de forma inmediata.

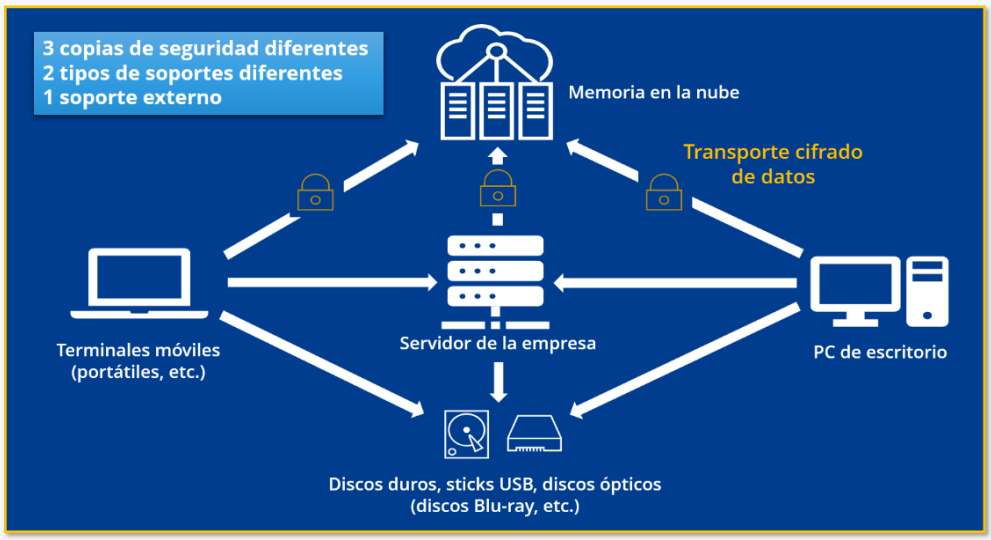


Ilustración 5 Optimizar backup con la regla 3-2-1. Tomado de *(IONOS, 2021)*

La investigación aporta en tener una herramienta que permita trasportar copias de seguridad a una nube de forma segura de extremo a extremo llamado análisis inmutable que ahora trae integrada en algunos softwares, que nos ayuda a revisar las copias de seguridad de posibles archivos infectados y evitar que los respaldos se encuentren dañados y garantizar que la empresa que cuenta con respaldos seguros de su información.

Con la información obtenida es importante saber qué tipo de compresión o encriptación utiliza cada una de las herramientas en caso de tener un robo de información. El ciberdelincuente al momento de querer visualizar la información no lo pueda hacer o le tome más tiempo en tratar de traducir la información de la empresa, y cubrir las necesidades de la compañía con copias, eficiencia y seguras ante posibles desastres naturales o ataques cibernéticos.

El estudio permitirá que otras personas puedan aprender cobre copias de seguridad de la información y demostrar que los datos se los conoce como el oro digital, Los resultados podrían servir como referencia para otras empresas que enfrentan desafíos similares en términos de seguridad cibernética.

Se toma como referencia el Objetivo 7. “Plan de Creación de Oportunidades”. Potenciar las capacidades de la ciudadanía y promover una educación innovadora, inclusiva y de calidad en todos los niveles, presentando mi investigación a las nuevas generaciones para los desafíos intelectuales, profesionales y personales. (SEMPLADES, 2021)

El objetivo 9. “Plan de Creación de Oportunidades”. Garantizar la seguridad ciudadana, orden público y gestión de riesgo. (SEMPLADES, 2021) es un objetivo

estratégico de la ciber seguridad que nos permite minimizar el riesgo que puede tener al no contar con respaldos de los sistemas de información.

Por último, este proyecto se relaciona con la línea No. 10 de investigación científica aprobada por el Honorable Consejo Universitario de la UTN concerniente al Desarrollo, aplicación de software y *cyber security* (seguridad cibernética) (UTN, 2023).

CAPITULO II

2 MARCO REFERENCIAL

2.1 ANTECEDENTES

La tecnología en las empresas está cambiando constantemente, el resguardar la información es un tema importante ya no solo de copiar en un disco duro, flash, o nube, hoy en día se debe tener en cuenta que la información es vulnerable a posibles ataques, desastres naturales o humanos. Respaldar la arquitectura de las máquinas virtuales es importante como menciona (Microsoft, 2023) ahora se puede realizar copias de seguridad de datos en el nivel de host de Hyper-V para habilitar la recuperación de datos de nivel de máquina virtual y de nivel de archivo o realizar copias de seguridad en el nivel de invitado para habilitar la recuperación en el nivel de aplicación.

De acuerdo con Edgar (Pilco, 2012) realizó un estudio, análisis y comparación de tres herramientas que se pueden utilizar para salvaguardar la información. El documento describe las posibles soluciones de *Backups*, que se han optimizado para satisfacer las necesidades y requerimiento de recuperación del entorno de las aplicaciones y así buscar impulsar las posibles herramientas a utilizar, sus funciones y beneficios encontrados son:

Crear tareas calendarizadas, control de respaldos, una administración centralizada, creación de políticas de migración automáticas, posibilidad de escalamiento, capacidad de conectividad nativa con los servidores detallados para generar respaldos “ON-LINE”, seguridad en el manejo de la información, manejo de perfiles de usuarios, recuperación rápida ante desastres presentados. (Pilco, 2012)

Otro estudio realizado por Geovanny (Caraguay, 2017) propone 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 una universidad, busca respaldar sus principales servicios, y la universidad cuente con un mecanismo de integridad y disponibilidad ante un posible evento adverso que puede traer la pérdida o robo de información. (Caraguay, 2017)

Para (Yunga, 2019) en su trabajo de investigación propone un plan de recuperación de desastres de la infraestructura de tecnologías de la información de una empresa. En el misma se dan a conocer las principales directrices y estándares internacionales como la ISO 22301 y siguiendo las mejores prácticas recomendadas, sirviendo como guía de implementación de mecanismos de recuperación en desastres naturales, posibles ataques informáticos o errores del sistema para evitar perder su información y tener un repositorio de almacenamiento de copias de seguridad. (Yunga, 2019)

El estudio de Wilson (Chango, 2015) al realizar su análisis, consideraciones de diseño e implementación en laboratorio de un sistema de respaldo de datos de máquinas virtuales y usuario final a través de la red LAN, indica la importancia de pensar en los respaldos como en un sistema integral. Recomienda analizar las opciones del mercado y buscar una herramienta que integre todos estos escenarios en una sola solución centralizada desde la cual se pueda controlar todo el ambiente de *backups*, esto es usuarios finales, máquinas virtuales y servidores físicos. Recomienda analizar las opciones del mercado y buscar una herramienta que integre todos estos escenarios en una sola solución centralizada desde la cual se pueda controlar todo el ambiente de *backups*, esto es usuarios finales, máquinas virtuales y servidores físicos.

Para tener un ambiente de respaldos y recuperación confiable se recomienda en primer lugar tener una política sólida de *backups* en la empresa. Deben definirse las prioridades de las aplicaciones correctamente, la periodicidad de los respaldos,

períodos de retención, etc. Las políticas dependerán del RTO (El objetivo de tiempo de recuperación) y RPO (objetivo de punto de recuperación) particular del negocio. (Chango, 2015)

Según las recomendaciones de *Buenning*, contar con una solución de copia de seguridad eficaz que puede protegerte de los peores efectos del *ransomware*. El autor *Buenning* sugiere que una solución adecuada hará que la recuperación de los datos sea rápida y sencilla, permitiendo a la organización vuelva a la actividad lo antes posible. Aunque las copias de seguridad no harán que los datos estén más seguros, pueden mejorar el tiempo de recuperación y reducir los costes tras un ataque. Las estrategias de prevención y recuperación de desastres son esenciales, ya que el coste medio por rescate asciende a 500.000 dólares y los costes totales superan los 4,5 millones de dólares en algunos casos. (Buenning, 2024)

La herramienta VMware vSphere Replication según (VMware, 2023) es una extensión de VMware vCenter Server que ofrece la recuperación y replicación de una máquina virtual basada en un hipervisor que permite replicar el almacenamiento de las máquinas virtuales, protege a las maquinas ante posibles fallas, se puede crear copias locales (Hardware) o a una nube, menor costo, manejo de contraseña, instala automáticamente un VIB de agente de cifrado puede activar el cifrado de flujos de tráfico de replicación desde el host ESXi de origen hasta el servidor de vSphere Replication en el sitio de destino. El cifrado de red utiliza el protocolo de transporte seguro TLSv1.2. cómo podemos ver existe herramientas sofisticadas que nos permiten tener nuestra información segura. (VMware, 2023)

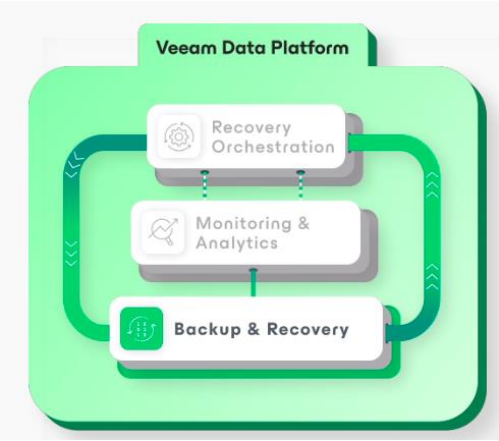


Ilustración 6 *Weeam Data Plataform. Tomado de (VMware, 2023)*

Acronis es una herramienta que garantiza la seguridad, accesibilidad, privacidad, autenticidad y protección de los datos. También está en constante evolución a las amenazas, sacando nuevas versiones de su software comercial que está en constante cambio. (Acronis, 2023)

Ilustración 7 *Acronis Backups. Tomado de (Acronis, 2023)*

Las normas que pueden usar lineamientos para tener copias de información de forma óptima, segura y oportuna en la actualidad existen algunas que se puede utilizar en las empresas para cuidar sus datos como las que menciono a continuación.

La norma NTP-ISO/IEC 17799 es una norma técnica peruana que ayuda a implementar también medidas de seguridad en las organizaciones. (Group, 2015)

En el documento de la NTC ISO 17799: "Seguridad de la Información" Punto 10.5" se recomienda hacer copias de respaldo de la información y software y probarse regularmente según la política de copias de respaldo acordada. Cuenta con lineamientos de implementación para proporcionar medios de respaldo para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla de medios. (ISO/IEC17799, 2005)

Con la transformación digital y la expansión del lugar de trabajo digital, el mundo experimenta un aumento de diversos tipos de ciberataque. Se definen como actos intencionados realizados desde una computadora para interrumpir o dañar un sistema, una red, un programa o unos datos. Pueden ocurrir de muchas maneras y ser realizados por cualquier persona con conexión a Internet, lo que los convierte en una amenaza global. Las consecuencias de un ciberataque pueden variar desde pequeños trastornos hasta grandes catástrofes, dependiendo de la magnitud y el nivel de sofisticación del ataque en cuestión.

2.2 Marco teórico

2.2.1 Herramientas para respaldar información

En un entorno cada vez más cambiante, las empresas necesitan volcar todos sus esfuerzos en reforzar sus políticas de seguridad y, en este sentido, las herramientas de contingencia y continuidad de negocio son una opción segura. El Instituto Nacional de Ciberseguridad, más conocido por las siglas INCIBE, las define de la siguiente manera: “Su objetivo es diseñar planes de actuación y contingencia destinados a mitigar el impacto provocado por cualquier incidente de seguridad y en especial los incidentes graves o desastres”. (Miguel, 2023)

2.2.2 Herramientas comerciales

2.2.2.1 Veeam Backup & Replication

Veeam uno del software que están como primero en la lista de los Gartner *backup* 2023 y uno de los más populares en el mercado del *backup* y la recuperación, y su producto también funciona con dispositivos Hyper-V y VMware. Sin embargo, Veeam no se detiene aquí y también ofrece funciones como la migración a VMware, la recuperación granular, la compatibilidad tanto con Linux como con Windows, la compatibilidad con vCloud director y mucho más.

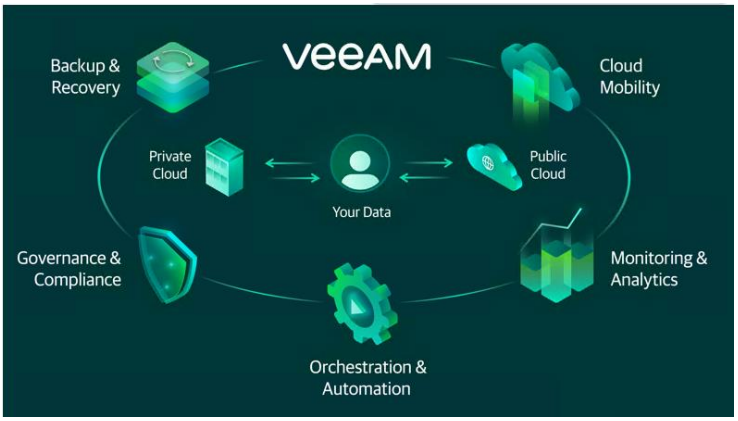


Ilustración 8 *Veeam Backup &Replication. Tomado de. (Morrison, 2024)*

Las capacidades de copia de seguridad de VMware de Veeam están disponibles para todos los usuarios de Veeam Backup & Replication, así como para los usuarios de Veeam Availability Suite (Veeam Backup & Replication + Veeam ONE). También hay una prueba gratuita de 30 días y varias versiones gratuitas de diferentes productos, con algunas limitaciones en cuanto a funcionalidad para obtener una licencia gratos solo debes de registrarte en su página oficinal y te enviaran a tu correo la licencia de prueba. (Morrison, 2024)

2.2.2.2 Vinchin Backup & Recovery

Ilustración 9 *Vinchin Backup & Recovery. Tomado de (Vinchin, 2024)*

Empezando por una opción poco convencional, Vinchin afirma ofrecer la combinación de funcionalidad y protección de datos para Hyper-V y VMware, así como para otros muchos tipos de entornos. Cuenta con una lista bastante impresionante de funciones para las máquinas virtuales VMware, entre las que se incluyen las copias de seguridad conscientes de las aplicaciones, la combinación de duplicación y compresión de datos, las políticas de retención de copias de seguridad, muchos tipos de almacenamiento diferentes que pueden actuar como repositorios de copias de seguridad, múltiples opciones de programación y mucho más.

Vinchin ofrece múltiples formas de interactuar con su plataforma: La edición comercial de Vinchin, por otro lado, ofrece múltiples características importantes, como la recuperación de desastres tanto a la nube como fuera de las instalaciones, operaciones híbridas de copia de seguridad y recuperación, y mucho más, cuenta además con una prueba gratuita disponible durante dos meses de la versión de la comunidad para los nuevos usuarios y se la puede descargar de la página oficial. (Morrison, 2024)

Ilustración 10 *Copia de seguridad rápida y confiable. Tomado de (Vinchin, 2024)*

Copia de seguridad sin agente de MV, haga una copia de seguridad de todos los archivos, aplicaciones y configuraciones del sistema operativo en la MV mediante la creación de una imagen de todo el sistema operativo. No es necesario instalar ningún agente en la MV, proteja directamente la MV a través del hipervisor.

Copia de seguridad de archivos basada en agente (Windows y Linux), copia de seguridad de bases de datos (Oracle DB, MySQL, SQL Server, PostgreSQL), con un agente de copia de seguridad ligero instalado en el sistema operativo de destino, los archivos y bases de datos dentro del servidor se pueden respaldar fácilmente.

Anti-Ransomware Nunca se Detiene: A medida que el *ransomware* se "actualiza" junto con el desarrollo de los centros de datos modernos, tener copias de seguridad comunes no es suficiente para obtener resultados satisfactorios contra el *ransomware*.

Ilustración 11 *Anti-Ransomware Nunca se Detiene. Tomado de (Vinchin, 2024)*

Basándose en la supervisión de E/S en tiempo real, Vinchin Backup & Recovery se encarga de asegurar los datos de copia de seguridad guardados en los almacenamientos de copia de seguridad, denegando directamente la modificación de los datos de copia de seguridad solicitada por aplicaciones no autorizadas. Esto puede prevenir de manera efectiva la pérdida inesperada de tus datos de copia de seguridad críticos.

Ilustración 12 *Garantizamos la continuidad de su negocio. Tomado de (Vinchin, 2024)*

Con Vinchin Backup & Recovery, puede recuperar al instante cualquier VM de cualquier tamaño en 15 segundos y asegurarse de que todos los negocios sean recuperables en 1 minuto, minimizando al máximo el tiempo de interrupción de los negocios críticos, garantizando en gran medida la continuidad de su negocio. Cualquier copia de seguridad de duplicada o comprimida es recuperable.

Ilustración 13 *Potente recuperación de desastres local y remota. Tomado de (Vinchin, 2024)*

Vinchin Backup & Recovery te permite copiar tus respaldos a diferentes ubicaciones, incluyendo cualquier almacenamiento en sitio secundario y almacenamiento externo. Cuando ocurre cualquier desastre en tu entorno de producción en sitio, puedes usar directamente la copia de respaldo en la segunda ubicación para recuperar las cargas de trabajo empresariales. (Morrison, 2024)

2.2.2.3 VSquare

Ilustración 14 *Vsquare. Tomado de (solution, 2019)*

Es una solución de respaldo rica en funciones que le permitirá controlar el respaldo de sus máquinas virtuales en cuestión de unos pocos pasos. Configure todo según las opciones que necesita y estará listo para realizar copias de seguridad de su VMware, hosts Hyper-V y máquinas físicas. (solution, 2019)

2.2.2.4 Nakivo Backup & Replication

Ilustración 15 *NAKIVO. Tomado de (Nakivo, 2022)*

NAKIVO Backup & Replication v8.5.2 es una solución de protección de datos que se ha centrado específicamente en la realización de copias de seguridad de las máquinas virtuales. Aunque actualmente existen otras soluciones en el mercado, se diferencia por las caracteriza por su gran compatibilidad y bajo precio. Este software es una solución completa de copias de seguridad, de esta forma, podremos no solo realizar la copia y restauración, sino que también podremos arrancar la máquina virtual directamente desde la copia de seguridad. NAKIVO VMware backup nos permitirá realizar fácilmente copias de seguridad de nuestras máquinas virtuales. (Luz, 2019)

Otra característica añadida es que dispone de la capacidad de realizar copias de seguridad de múltiples hipervisores en un único servidor de copia de seguridad, con el objetivo de ahorrar costes en hardware. También vamos a poder realizar copias de seguridad de nuestras instancias en Amazon EC2, en otras regiones de Amazon, y todo ello de una manera muy rápida y fácil, sin necesidad de hacer la replicación.

Ilustración 16 *Bakivo Backup & Replication. Tomado de (Nakivo, 2022)*

NAKIVO está lanzando de manera continua actualizaciones de su software, no solo solucionando pequeños errores, sino incorporando nuevas funcionalidades para hacer el software mucho más completo. El ciclo de actualización del software suele ser trimestral, de esta forma, el equipo IT podrá ver en detalle todas las nuevas características añadidas para adaptarlo perfectamente a las necesidades de la empresa. (Luz, 2019)

2.2.2.5 Vembu BDR Suite

Vembu es un proveedor de software que ha conseguido ganar mucha popularidad entre las pequeñas y medianas empresas y clientes, sobre todo debido a la combinación de facilidad de uso y la flexibilidad del modelo de pago. Vembu BDR Suite es una combinación masiva de soluciones para copias de seguridad de diferentes dispositivos, incluyendo almacenamientos físicos, máquinas virtuales, cargas de trabajo en la nube y más. Esto convierte a Vembu en una solución bastante atractiva para mantener todas sus soluciones de copia de seguridad trabajando en tándem unas con otras. (Morrison, 2024)

Nuestro programa de socios atiende las necesidades de varios tipos de socios, incluidos

- Proveedores de servicios gestionados (MSP)
- Proveedores de servicios de nube gestionados (MCP)
- Distribuidores
- Distribuidores y distribuidores de valor añadido
- Consultores de TI e integradores de sistemas
- Proveedores OEM

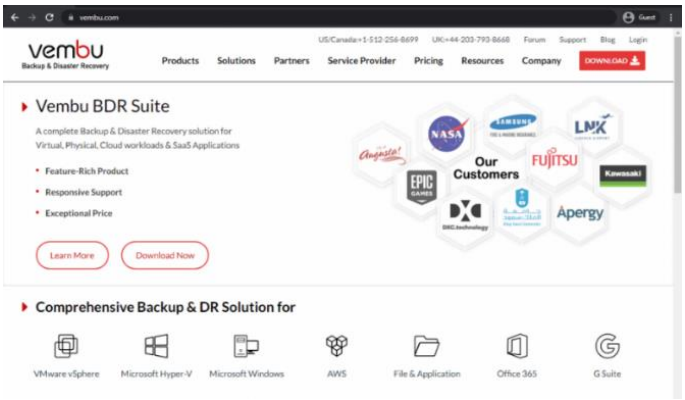


Ilustración 17 *Vembu. tomado de (Morrison, 2024)*

Una vez recopilada la información, se consultó el informe de Gartner sobre los softwares líderes de respaldo empresarial de 2023, los cuales pueden ser utilizados por las empresas para proteger sus servidores y datos, según lo publicado en (Tecnozero, 2023).

Ilustración 18 *Gartner backup 2023 (Tecnozero, 2023)*

2.2.3 Herramientas open source

2.2.3.1 Bacula Enterprise

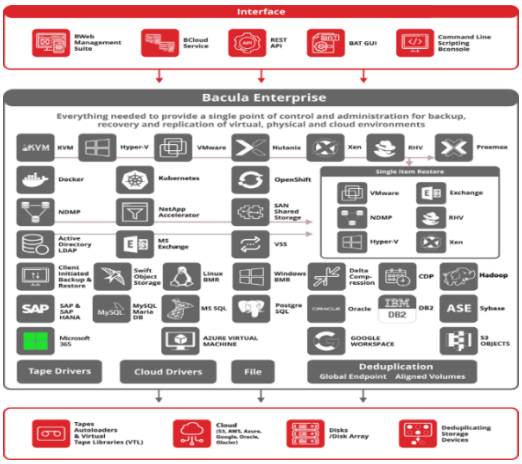


Ilustración 19 *Bacula Emterprise. Tomado de (Bacula, 2025)*

Bacula Enterprise es una solución que ofrece operaciones eficaces de copia de seguridad y recuperación para hosts VMware ESXi con vSphere, así como muchas otras funciones incluidas en este módulo en particular: restauración granular de archivos, seguimiento de bloques modificados, recuperación de archivos individuales, recuperación instantánea, etc. Esta solución también destaca por ofrecer integración nativa y protección para una amplia gama de otros hipervisores, como Hyper V, Xen, KVM, Proxmox, etc. Bacula es bien conocido por tener una arquitectura que ofrece niveles de seguridad inusualmente fuertes, así como herramientas avanzadas de detección de *ransomware*.

Dado que Bacula es una solución empresarial de gama alta, también aporta otras muchas capacidades, ya sea su gama de destinos de almacenamiento, su conectividad de nube híbrida, su gama de tecnologías de duplicación, sus funciones de compresión y cifrado y sus altos niveles de personalización. (Morrison, 2024)

2.2.3.2 Amanda

AMANDA, Advanced Maryland Automatic Network Disk Archiver, es una solución de respaldo que permite al administrador de TI configurar un único servidor de respaldo maestro para respaldar múltiples hosts a través de la red en unidades de cinta/cambiadores o discos o medios ópticos. Amanda utiliza utilidades y formatos nativos (por ejemplo, dump y/o GNU tar) y puede realizar copias de seguridad de una gran cantidad de servidores y estaciones de trabajo que ejecutan múltiples versiones de Linux o Unix. Amanda utiliza un cliente nativo de Windows para realizar copias de seguridad de servidores y escritorios de Microsoft Windows.

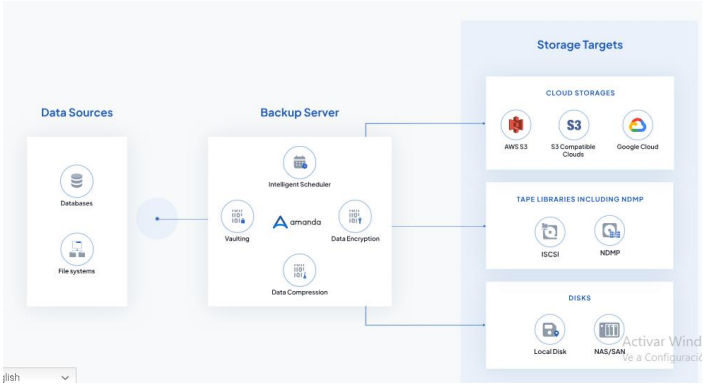


Ilustración 20 *Amanda. Tomado de (Amanda Comunity, 2023)*

Amanda 3.5.4 es la última versión se lanzó el 25 de agosto de 2023. Incluye mejoras de seguridad para mejorar aún más su experiencia de respaldo. Esta versión se centra en ofrecer la máxima protección de datos abordando las vulnerabilidades y exposiciones comunes (CVE-2023-30577), lo que garantiza un proceso de copia de seguridad más fluido y confiable. (Amanda, 2023)

2.2.3.3 UrBackup

UrBackup es software libre que se utiliza para realizar respaldo cliente/servidor de sistemas y archivos con código abierto fácil de configurar, que a través de una combinación de respaldos de imágenes y archivos logra tanto la seguridad de los datos como un tiempo de restauración rápido mientras los sistemas se encuentran en funcionamiento, supervisa continuamente las carpetas, puedes ver la información respaldada de forma gráfica o ingresando a la ruta donde se realizó la copia de seguridad, se puede realizar copias de seguridad incrementales de archivos son realmente rápidas.

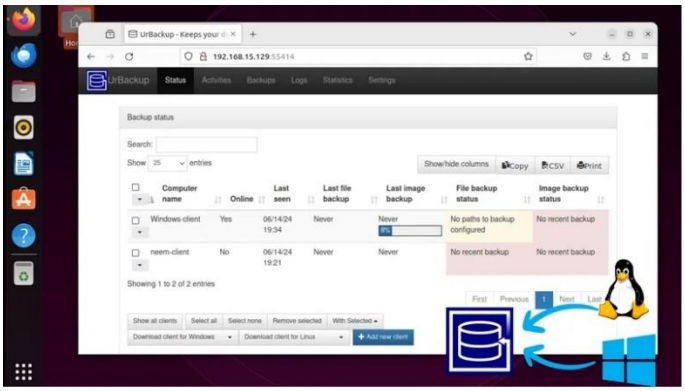


Ilustración 21 *Urbackup tomado de (Chaudhry, 2024)*

Es muy fácil restaurar su información a través de la interfaz web, a través del cliente o el Explorador de Windows, mientras que las copias de seguridad de los volúmenes de la unidad se pueden restaurar con una memoria USB de arranque (restauración completa), la interfaz web es muy sencilla de configurar su propio servidor de respaldo sea realmente fácil. (Urbackup, 2024)

2.2.4 Normas ISO/IEC 27001

2.2.4.1 ISO/IEC 27001

La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

Ilustración 22 *Estructura de ISO 27001. Tomado de (Leal, 2022)*

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001. (Leal, 2022)

2.2.4.2 Normas ISO/IEC 17799

La norma NTP-ISO/IEC 17799 es una norma técnica peruana que ayuda a implementar también medidas de seguridad en las organizaciones. (Group, 2015)

En el documento de la NTC ISO 17799: "Seguridad de la Información" Punto 10.5" se recomienda hacer copias de respaldo de la información y software y probarse regularmente según la política de copias de respaldo acordada. Cuenta con lineamientos de implementación para proporcionar medios de respaldo para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla de medios. (ISO/IEC17799, 2005)

2.2.5 Aspectos de seguridad aplicables a la industria farmacéutica

La industria farmacéutica generalmente va de la mano con una gran cantidad de desafíos asociados con la infraestructura de TI. Los sistemas y los datos deben estar alineados, optimizados y consolidados. Lo mismo se aplica a la red de la organización recién estructurada: las direcciones IP y los hosts DNS ya no coinciden, el reenvío de puertos no va a ninguna parte y la traducción de acceso a la red (NAT) falla. Además, la fusión de redes puede provocar o crear nuevos puntos débiles y brechas de seguridad, así como la posibilidad de que surjan o incluso se creen problemas de cumplimiento. En resumen, las fusiones y adquisiciones son un trabajo duro para TI. Además, cuestan tiempo y dinero en equipos y personal. (NilsUllmann, 2021)

La industria farmacéutica tiene una gran presión normativa debido a la gran cantidad de datos sensibles y personal que maneja, además de otra información relevante, como avances médicos, fármacos En este entorno de gran control y presión, la ciberseguridad se presenta como uno de los temas prioritarios de todas las empresas del sector, buscando nuevas formas y metodologías para poder elevar el nivel de protección de sus datos y sistemas.

Las alertas y la seguridad están transformando la industria, convirtiéndose en materias imprescindibles para poder blindar datos confidenciales y sensibles, y garantizar su privacidad e integridad. (Ambit, 2023)

Los principales desafíos que menciona la empresa, (Ambit, 2023) en materia de seguridad a los que se enfrentan las empresas farmacéuticas en la actualidad son:

- Nivel de seguridad de la infraestructura TI
- Robo de datos
- Sistemas obsoletos o no integrados

La información que maneja el sector farmacéutico es altamente sensible y muy apetecible para el mercado negro de la ciberdelincuencia, ya que es de las más valiosas y mejor pagadas.

El espionaje industrial y la piratería informática han alcanzado cifras alarmantes, lo que resulta trascendental en este sector, donde la investigación, desarrollo e inversión financiera son claves para su posicionamiento en el mercado. Algunas estadísticas de seguridad informática indican que el coste de un ciberataque exitoso es de más de 5 millones de dólares.

Asimismo, otras fuentes estiman que el daño relacionado con ciberataques llegará a los 6 trillones de dólares anuales para 2021. A inicios del año 2019 se estimaba que habría un ataque de *ransomware* cada 14 segundos para los últimos meses del año.

A pesar de estos datos, no existe suficiente concienciación en el sector farmacéutico sobre el alto riesgo al que se exponen estas compañías, lo que a menudo deriva en una deficiente inversión en cuanto a recursos y tiempo para la prevención de incidentes de seguridad. (Rodríguez, 2020)

2.2.6 Respaldos de máquinas virtuales

La arquitectura de las máquinas virtuales difiere de los entornos tradicionales internos y, por lo tanto, exige técnicas distintas para el respaldo de datos.

En escenarios como este, Andrés Mendoza, consultor técnico senior de Manage Engine en Latinoamérica, brinda algunos consejos que, desde su punto de vista, son además buenas prácticas para realizar respaldos en estos entornos. (Gómez, 2017)

La arquitectura de una máquina virtual es sustancialmente distinta de los entornos tradicionales internos y exige técnicas distintas para el respaldo de datos. A continuación, se detallan algunos consejos considerados como mejores prácticas para respaldar máquinas virtuales. (Forti, 2017)

- ✓ Respaldos incrementales para mejorar la velocidad de los respaldos
- ✓ Las tomas instantáneas no son respaldo
- ✓ Máquinas virtuales de respaldo en la capa de virtualización
- ✓ Copia de los respaldos en una localidad secundaria
- ✓ Cifrado de los respaldos
- ✓ Pruebas regulares del software de restauración

2.2.7 Tipos de cifrados

El cifrado está en el corazón de la transferencia segura de archivos, y comprender las diferencias entre las opciones existentes puede ser un desafío. Para facilitar la comprensión, los dividiremos en tres grupos.

Las capas de cifrado de archivos son protocolos que aprovechan uno (o varios) de los algoritmos para cifrar datos en reposo y en tránsito. Puede "superponer" algoritmos para complementar sus funciones de seguridad o proporcionar seguridad adicional. (IT, 2022)

Por ejemplo, puede usar TLS para cifrar los archivos que está transfiriendo a través de la nube y anular el cifrado PGP en los archivos que está transfiriendo a través de un canal TLS para mayor seguridad.

Algunas de las capas de cifrado más populares son:

PGP (Pretty Good Privacy): PGP es un protocolo de cifrado asimétrico que aprovecha la criptografía de clave pública para mitigar los riesgos de seguridad de compartir archivos para sus datos en tránsito. Esto significa que tendrá dos claves criptográficas (una privada y otra pública) para sus datos, que es irrompible por ataques de fuerza bruta. Además, Open PGP (el protocolo original) es gratuito.

S/MIME (Secure Multipurpose Internet Mail Extensions): El protocolo de transferencia S/MIME aprovecha el cifrado de extremo a extremo, lo que significa que el acceso a sus datos está completamente restringido durante el tránsito y solo el remitente o el destinatario pueden acceder a esos datos.

SSL (Secure Socket Layer): SSL es un estándar de cifrado que protege los datos que transfiere entre un servidor y la nube. Este estándar de cifrado brinda privacidad, autenticación e integridad a las comunicaciones cliente-servidor al aprovechar el cifrado, la certificación digital y los protocolos de enlace virtuales.

SSL es la versión anterior y mucho más antigua del protocolo de cifrado TLS. Sin embargo, todavía se usa mucho. en transferencias de datos en la nube. (IT, 2022)

2.2.8 Aplicar aspectos de seguridad en una farmacéutica

La arquitectura de una máquina virtual es sustancialmente distinta de los entornos tradicionales internos y exige técnicas distintas para el respaldo de datos. A continuación, se detallan algunos consejos considerados como mejores prácticas para respaldar máquinas virtuales. (Forti, 2017)

- Respaldos incrementales para mejorar la velocidad de los respaldos
- Las tomas instantáneas no son respaldo
- Máquinas virtuales de respaldo en la capa de virtualización

- Copia de los respaldos en una localidad secundaria
- Cifrado de los respaldos
- Pruebas regulares del software de restauración

2.3 Marco legal

En Ecuador el artículo 66, numeral 19 de la Constitución de la República, establece “el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley”.

Al amparo de esta norma, la Dirección Nacional de Registros Públicos (Dinarp)* trabajó en la propuesta del proyecto de Ley de Protección de Datos Personales, ya que una Ley de Protección de Datos Personales es necesaria en un mundo hiperconectado, pues habilita la confianza digital. (Públicos, 2021)

En el documento de la NTC ISO 17799: "Seguridad de la Información" Punto 10.5" se recomienda hacer copias de respaldo de la información y software y probarse regularmente según la política de copias de respaldo acordada. Cuenta con lineamientos de implementación para proporcionar medios de respaldo para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla de medios. (ISO/IEC17799, 2005)

La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. (Leal, 2022)

Se toma como referencia el Objetivo 7. “Plan de Creación de Oportunidades”. Potenciar las capacidades de la ciudadanía y promover una educación innovadora, inclusiva y de calidad en todos los niveles, presentando mi investigación a las nuevas generaciones para los desafíos intelectuales, profesionales y personales. (SEMPLADES, 2021)

El objetivo 9. “Plan de Creación de Oportunidades”. Garantizar la seguridad ciudadana, orden público y gestión de riesgo. (SEMPLADES, 2021) es un objetivo estratégico de la ciber seguridad que nos permite minimizar el riesgo que puede tener al no contar con respaldos de los sistemas de información.

CAPITULO III

3 MARCO METODOLÓGICO

3.1 Descripción del área de estudio / descripción del grupo de estudio

La investigación se realizará en una empresa farmacéutica en la ciudad de Quito, provincia de Pichincha; la empresa se dedica a la venta de medicamentos y ahora tiene pocos empleados, no cuenta con más sucursales dentro y fuera del país, tiene un servidor donde almacena toda su información desde ahí comparte a todos sus empleados los datos que necesitan en cada área.

3.2 Enfoque y tipo de investigación

El tipo de investigación que se utiliza es de carácter cualitativa de acuerdo con este permite inicia regularmente en la práctica un estudio, mediante el ingreso al contexto, ambiente o campo. (Hernández,Mendoza&Christian, 2018)

Se llevó a cabo una investigación exhaustiva a través de sitios web, artículos científicos, tesis y documentación de empresas desarrolladoras de herramientas, para la implementación de una herramienta segura que respalde la información de sus sistemas actuales, buscando demostrar los beneficios que puede tener con la nueva herramienta y cuál sería el riesgo si no hay un respaldo para garantizar la seguridad de la información.

En cuanto al tipo de investigación es tratar seguridad de la información en las empresas para que las empresas puedan tener información y ventajas que se puede tener respaldos disponibles.

3.3 Procedimiento de investigación

Fase 1. En esta fase se realizó un estudio comparativo de diferentes herramientas comerciales y open source.

En esta fase se llevó a cabo una investigación exhaustiva a través de sitios web, artículos científicos, tesis y documentación de empresas desarrolladoras de herramientas. El objetivo fue recopilar la mayor cantidad de información posible sobre soluciones de respaldo que permitan realizar copias en el menor tiempo, así como llevar a cabo un análisis de *malware* antes de iniciar el respaldo de máquinas virtuales. Esto es fundamental para garantizar la seguridad de la información y facilitar restauraciones rápidas en caso de incidentes. La investigación también evaluó los riesgos que enfrenta la empresa farmacéutica al no implementar un respaldo efectivo de su información, especialmente en un entorno vulnerable a infecciones y ataques informáticos. Como resultado de este análisis, se identificaron Veeam Backup & Replication y UrBackup como las herramientas más destacadas para el estudio.

Fase 2. Análisis de ventajas del uso de herramientas comerciales y open source para determinar la que mejor se adapte al caso de estudio.

Con la información recolectada en la fase 1, se instaló un software que permita crear máquinas virtuales donde se procederá a instalar los sistemas operativos que contendrán información, los cuales serán utilizados para simular los respaldos de las dos herramientas seleccionadas, ejecutar *Benchmarking*, la historia y desarrollo en avance de seguridad en el tiempo, los costos que tienen cada una, las características a nivel de seguridad ante ataques de ciberdelincuentes o infecciones a máquinas virtuales o archivos que nos pueden ofrecer, el número de copias que puede realizar si son diarias, semanales o mensuales, que nivel de comprimido de archivos tiene.

Fase 3. Desarrollo de un plan de respaldo de datos considerando las necesidades de seguridad.

Una vez ejecutada las herramientas de respaldo de las máquinas virtuales y obteniendo los resultados del análisis (*Benchmarking*), se desarrolló un plan de respaldos, con las recomendaciones que se le puede dar para obtener una herramienta efectiva que genere copias de seguridad de sus máquinas virtuales con la herramienta que mejor se desempeñó al momento de realizar la simulación.

3.4 Consideraciones bioéticas

Para el presente estudio, las consideraciones bioéticas pueden no ser el enfoque principal del estudio, ya que el tema está más relacionado con aspectos técnicos y de seguridad informática en el ámbito empresarial. Sin embargo, aún se pueden identificar algunas consideraciones bioéticas relevantes, especialmente en relación con la privacidad, la seguridad de los datos y el impacto en los empleados y la comunidad en general.

Con la simulación lo que se espera es proteger los datos personales de los empleados, proveedores y de la empresa, evitar el robo de información por eso esta investigación tiene la responsabilidad de contribuir al bienestar de la comunidad con un análisis que nos ayude a verificar la funcionalidad de las herramientas seleccionadas.

CAPITULO IV

4 DESARROLLO

De acuerdo con la investigación documental y recolección de información realizada en el capítulo II, respecto a los softwares comerciales y softwares libres que permiten respaldar máquinas virtuales completas sin excluir el tipo de información que este contenga, se seleccionaron dos herramientas (1 comercial y 1 libre) en donde se virtualizó los ambientes de trabajos correspondientes para infectar, respaldar y obtener resultados, con la finalidad de conocer si estos detectaron los *malware*.

4.1 Seguridad en herramienta de respaldo (Software comercial)

Las herramientas Veeam Backup & Replication[1], Vinchin Backup & Recovery[2], VSquare[3], Nakivo Backup & Replication[4] y Vembu BDR Suite[5], corresponden a los softwares comerciales investigados en el capítulo II. Estas soluciones están diseñadas para ofrecer copias de seguridad eficientes y confiables, así como opciones de recuperación ante desastres para empresas de distintos tamaños. De todas ellas, se determinó que el software Veeam Backup & Replication es el más adecuado para cumplir con los requisitos de respaldo y protección de datos de forma integral. Esto se debe a que Veeam se encuentra ubicado en el cuadrante superior derecho como "líder" en el informe de Gartner con la última publicación del año 2023

[1] https://www.baculasystems.com/es/el-blog/copia-de-seguridad-backup-vmware/

[2] https://www.vinchin.com/

[3] https://www.vsquarebackup.com/

[4] https://www.nakivo.com/es/

[5] https://www.baculasystems.com/

realizada por Tecnozero[6], lo que refleja su destacada posición en el mercado en términos de capacidades, innovación y rendimiento.

Para el primer caso, en un equipo físico se activó el entorno virtual que viene por defecto en el sistema operativo de Windows 10[7] que se registra por nombre Hyper-V[8], posterior se instaló dos sistemas operativos, el primero comercial de nombre Windows Server 2019[9] y el segundo de código abierto Ubuntu 22[10], luego se cargó información en las máquinas virtuales en carpetas las mismas que contenían documentos de Word y PDF, posterior en cada una de estas máquinas virtuales se realizó la infección controlada con los *malware* descargado del sitio GitHub[11], una plataforma que ofrece una amplia variedad de programas de prueba y código abierto. Tras la ejecución de los *malware*, se procedió a realizar una copia de seguridad utilizando la herramienta Veeam Backup & Replication Server, con el objetivo de evaluar la efectividad de las soluciones de respaldo ante la amenaza.

Finalmente, se revisaron los informes generados para analizar los resultados obtenidos durante la infección controlada, evaluando el comportamiento de cada uno de los softwares involucrados. A continuación, se presenta el flujo detallado del proceso:

---

[6] https://www.tecnozero.com/blog/cuadrante-magico-de-gartner-en-soluciones-de-software-de-backup-y-recuperacion-empresarial-2023/

[7] https://www.microsoft.com/es-es/software-download/windows10

[8] https://learn.microsoft.com/es-es/virtualization/hyper-v-on-windows/about/

[9] https://www.microsoft.com/es-es/evalcenter/evaluate-windows-server-2019

[10] https://ubuntu.com/download/desktop

[11] https://github.com/

4.1.1 Método de respaldos con Veeam Backups & Replication

En el entorno actual en el que se desarrolla los sistemas tecnológicos, es primordial, que las empresas de cualquier sector tomen las medidas de seguridad para proteger su información valiosa, es por ello, que el presente flujograma se indica como realizar respaldos de seguridad utilizando Veeam Backup & Replication ejercicio, que se desarrolló en máquinas virtuales Microsoft Windows Server 2019 y Linux Ubuntu 22.

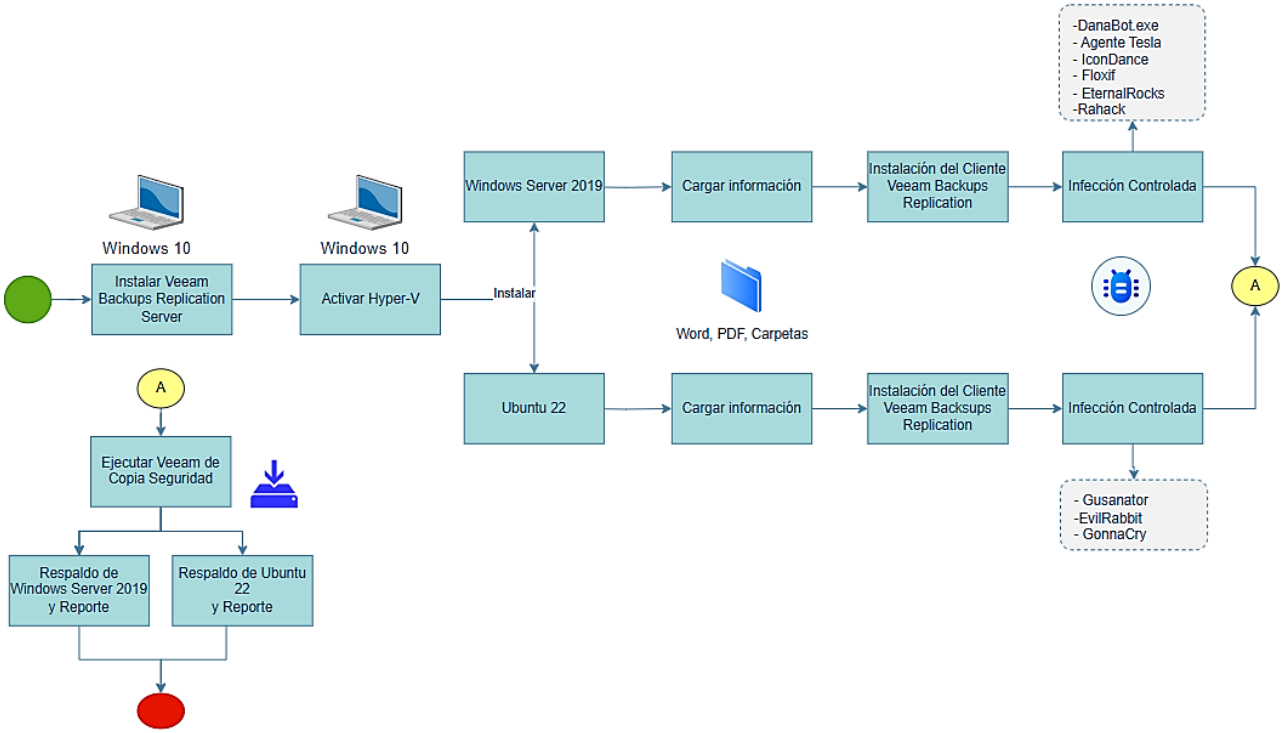


Ilustración 23 *Método de respaldos con Veeam Backups & Replication*

En este apartado, se detalla el paso a paso desde la configuración y ejecución de respaldos con Veeam Backup & Replication para los entornos virtuales en Microsoft Windows Server 2019 y Linux Ubuntu 22.

1. **Instalar Veeam Backup & Replication**

- Ingresar a la página web de Veeam Backup & Recplicacion que encuentra en el siguiente enlace: https://www.veeam.com/es/products/veeam-data-platform/backup-recovery.html
- Dar clic en el botón "versión de prueba", seguidamente crear la cuenta en esta plataforma llenando el formulario, bajo el correo registrado se recibe un archivo de licencia versión prueba de30 días.
- En el portal de Veeam Backup & Replication, ingresar a la sesión con las credenciales antes creadas y descargar el instalador de Veeam Backup & Replication.
- Ejecutar con privilegios de administrador la imagen ".iso" de Veeam Backup & Replication 12.1 en la laptop física con Windows 10. *Ver anexo 1.*
- Seleccionar la primera opción "Veem Backups & Replication 12.1", el servidor y la consola incluyen opciones para instalar "Veeam Enterprise Manager". *Ver anexo 2.*
- Se carga la licencia recibida con anterioridad. *Ver anexo 3 y 4.*
- Escoger una ruta en específico donde se almacenarán los respaldos de las máquinas virtuales, paso primordial para facilitar la administración y recuperación de datos en el futuro. *Ver anexo 5.*
- Revisar las configuraciones que se realizaron anteriormente estén correctas y finalizar la instalación. *Ver anexo 6 y 7.*

  Nota:

- Es importante indicar que el caso de estudio se realizó con la versión de prueba de 30 días, debido que se pudo realizar diversas pruebas y evaluaciones del software durante este periodo, esto incluye la posibilidad de realizar copias de seguridad, restauraciones y configuraciones diversas para evaluar el rendimiento del software antes de decidir si se adquiere una licencia completa.

2. Activar Microsoft Hyper-V

- Acceder al panel de control y seleccionar "programas y características". *Ver anexo 8.*
- En la parte superior izquierda de esta ventana, seleccionar "Activar o desactivar las características de Windows". *Ver anexo 9.*
- En la ventana de características de Windows marcar los dos casilleros: "Herramientas de administración de Microsoft Hyper-V" y "Plataforma de Microsoft Hyper-V". Luego, el sistema solicita el reinicio del equipo para finalizar la instalación. *Ver anexo 10*.
- Una vez reiniciado el equipo, abrir el Administrador de Hyper-V. *Ver anexo 11.*

  Nota: Es importante recordar que los equipos virtualizados solo permitirán la instalación de un número limitado de máquinas virtuales, dependiendo de las características del hardware del ordenador.

3. Preparar máquina virtual Windows Server 2019 y Ubuntu 22 en Hyper -V

- Abrir el administrador de Hyper-V, dar clic en "Nuevo" para iniciar la creación de la máquina virtual, esta función se encuentra ubicado en el lado derecho de nuestra ventana. *Ver anexo 12.*
- Asignar un nombre a la máquina virtual y seleccionar la ubicación en donde se instalará Windows Server 2019 y Ubuntu 22 en Hyper-V. *Ver anexo 13.*
- Para las dos máquinas virtuales, seleccionar "Generación 1", la cual es la

recomienda para la instalación en los sistemas operativos de 32 y 64 bits. *Ver anexo 14.*

- Para las dos máquinas virtuales, especificar la cantidad de memoria RAM que se debe asignar para la máquina virtual, en este caso, se asignó memoria de 2048 MB. *Ver anexo 15*.
- Configurar bajo la misma red a utilizar la maquina física y en las máquinas virtuales Windows Server 2019 y Ubuntu 22. *Ver anexo 16*.
- En la sección "Conectar disco duro virtual", asignar el tamaño del disco duro que va a tener las máquinas virtuales de Windows Server 2019 y Ubuntu 22. *Ver anexo 17.*
- En la sección "Opciones de instalación", dirigirse a "Archivos de imagen" y seleccionar la imagen del sistema operativo Windows Server 2019 y Ubuntu 22, finalmente dar clic en finalizar. *Ver anexo 18 y 19.*
- Iniciar la máquina virtual con la finalidad de instalar el sistema de operativo Windows Server 2019 y Ubuntu 22. *Ver anexo 20.*

4. Instalar Microsoft Windows Server 2019

- En la pantalla que se despliega, ingresar el código de la licencia de pago para activar Windows Server 2019. *Ver anexo 21.*
- Seleccionar "Windows Server 2019 Standard (Experiencia de escritorio)" y seleccionar "Windows Server 2019 Standard (Experiencia de escritorio)", dar clic en "Acepto los términos de licencia)" y escoger el tipo de instalación. *Ver anexo 22, 23 y 24.*
- Seleccionar el disco duro virtual donde se instalará Windows Server 2019 y crear la contraseña en el usuario administrador que viene por defecto. *Ver anexo 25 y 26.*

Nota:

- Hyper-V crea automáticamente el usuario “Administrador” y el usuario asigna una contraseña. Estas credenciales sirven para conectar el software y realizar los respaldos.

5. Instalar Linux Ubuntu 22

- En la máquina virtual de Ubuntu, seleccionar la opción “Try or Install Ubuntu” y cambiar al idioma español, finalmente dar clic en “Instalar Ubuntu”. *Ver anexo 27 y 28.*

- Para configurar el idioma del teclado, se debe dar clic en español latino y clic en “continuar”. *Ver anexo 29.*

- En el apartado de “Actualizaciones y otro software”, seleccionar la opción “Instalación normal” y “Descargar actualizaciones durante la instalación de Ubuntu”, dar clic en "Continuar". *Ver anexo 30.*

- En la pantalla de “Tipo de instalación”, seleccionar la opción “Borrar disco e instalar Ubuntu”, luego, dar clic en “Instalar ahora”, enseguida, se muestra una ventana con la pregunta ¿Desea escribir los cambios en los discos?, en este aparado dar en “Continuar”. *Ver anexo 31 y 32.*

- Dentro de la configuración, escoger la zona geográfica desde donde se realiza el proceso de instalación de Ubuntu 22., para este caso se seleccionó la ubicación de “Guayaquil”, luego dar clic en “continuar”. *Ver anexo 33*.

- Configurar los datos de la máquina virtual, entre estos se debe llenar la información de nombre usuario, nombre del equipo y creación de una contraseña y posterior dar clic en “Continuar”. *Ver imagen 34.*

Notas:

- Es necesario contar la dirección IP que es asignada por el proveedor de Internet, habitar la conexión SSH y abrir el puerto 22 para la conexión con Veeam Backup & Replication.

- Para realizar esta configuración, se debe iniciar sesión como administrador para contar con una comunicación fluida y segura entre los sistemas. *Ver anexo 35.*

- Habilitar la conexión "SSH" para la comunicación del servidor y el cliente de Veeam Backups & Replication con el comando "sudo apt install openssh-server y para validar que el estado se encuentre en "Activo", se realiza el comando "sudo systemctl status ssh" para ver si esta activa. *Ver anexo 36 y 37.*

- Habilitar el puerto 22 en Ubuntu con el comando "sudo ufw allow 22/tcp" por donde se comunicará el equipo físico con la máquina virtual de Linux Ubuntu 22. *Ver anexo 38*.

6. **Cargar información en las máquinas virtuales como archivos, documentos PDF y Word.**
7. **Instalación del cliente Veeam Backup & Replication en la máquina virtual de Windows Server 2019**

- Ejecutar Veeam Backups & Replication para agregar la conexión con el servidor Windows Server 2019, en la parte superior izquierda, dar clic en "Add Server". *Ver anexo 39.*

- En la pantalla de especificaciones de Veeam Backups & Replicación del equipo físico, escribir el nombre DNS o dirección IP del cliente en donde se instalará el agente para las copias de seguridad. *Ver en anexo 40.*

- Ingresar el nombre y contraseña del administrador del servidor Windows Server 2019, conectarse con el cliente y dar clic en "Next". *Ver en anexo 41*.

- Verificar que el estado de la conexión se encuentre en instalado y dar clic en "Apply". *Ver anexo 42.*
- Instalar los complementos necesarios del cliente en Windows Server 2019 y conectar con Veeam Backups & Replication, hacer clic en "Next", en la ventana "Resumen" dar clic en "*Finish*". *Ver anexo 43 y 44.*

8. Instalación del cliente Veeam Backup & Replication en la máquina virtual de Linux Ubuntu 22.

- En Veeam Backup & Replication, agregar Linux Ubuntu 22. *Ver anexo 45.*
- En la ventana "Añadir Servidor" de Veeam Backup & Repliacion, seleccionar la segunda opción "Microsoft Hyper-V". *Ver anexo 46.*
- Ingresar la IP del cliente, agregar las credenciales de "*root*" usando el puerto 22 y dar clic en "*OK*". *Ver anexo 47.*
- En la ventana SSH *Connection* seleccionar el usuario "*root*" y dar clic en "Next". *Ver anexo 48.*
- En la ventana de resumen se puede ver la información del cliente Ubuntu 22 con la cual se va a realizar la conexión con Veeam Backup & Replication, finalmente dar clic en "*Finish*". *Ver anexo 49.*
- En la venta "*Review*" del cliente verificar que el estado se encuentre como instalado y dar clic en "*Apply*", revisa que la instalación del cliente no tenga errores en la comunicación con el servidor y clic en "*finish*". *Ver anexo 50.*
- Verificar que la máquina virtual de Ubuntu 22, esta agregada en Veeam Backups & Replication. *Ver anexo 51.*

9. **Realización la infección controlada, en las dos máquinas virtuales con diferentes tipos de malware.**

Para efectos del ejercicio, se buscó en el navegador una colección de *malware* para simular un posible ataque a las máquinas virtuales instaladas (Windows Server 2019 y Ubuntu 22), este paso marca el comienzo de las pruebas para evaluar cómo responde Veeam Backup & Replication-herramienta comercial ante amenazas.

Para fines investigativos, se descargaron una serie de *malware* depositado en el enlace https://github.com/sergioab7/ para la ejecución de pruebas en las máquinas virtuales.

Infecciones a la máquina virtual Windows Server 2019

- Infección con Danabot, como lo menciona el investigador de (ESET, 2018) es un troyano bancario que ataca mediante correos electrónico. Para efectos de la simulación se infectó la máquina virtual Windows Server 2019. *Ver anexo 52.*
- Infección con $uckyLocker, este corresponde a un *Ransomware*. Para efectos de la simulación se infectó la máquina virtual Windows Server 2019. *Ver anexo 53.*
- Infección con AgentTesla, como lo menciona (checkpoint, 2022), es un *malware* de acceso remoto al ordenador que procede con el robo de información Para efectos de la simulación se infectó la máquina virtual Windows Server 2019. *Ver anexo 54*
- Infección con Azorult, es un troyano muy peligroso que se envía mediante correo electrónico y que diseñado para recabar datos sensibles. (Meskauskas, 2019). Para efectos de la simulación se infectó la máquina virtual Windows Server 2019 *Ver anexo 55.*
- Infección con *Trojan* Ana, consiste en una amenaza para los registros del sistema operativo, el mismo que se aloja en el disco local C: (ExeDB, 2014).

  Para efectos de la simulación se ejecutó el *malware* en la máquina virtual

Windows Server 2019, la misma que procedió a reiniciarse de forma automática, mostrando el famoso pantallazo azul y dejando sin servicio al sistema operativo. *Ver anexo 56 y 57.*

Infecciones a la máquina virtual Linux Ubuntu 22

- Infección con Gusanator, es un script que emula a un *malware* gusano para replicar archivos y directorios en un sistema operativo de acuerdo con la información del portal *github*. Para efectos de la simulación se infectó la máquina virtual Windows Server 2019
- Primero ingresar a la carpeta "*Downloads*" utilizando el comando "cd *Downloads*/" donde se guardará el *malware*, para descargar se utiliza el comando "git clone https://github.com/sergioab7/Gusanator.git". *Ver anexo 58.*
- Segundo, ingresa a la carpeta de gusanator con el siguiente comando "cd Gusanator/", escribir el comando "ls" para visualizar si tenemos descargado "gusanator.py" y para ejecutar el gusano usar el siguiente comando "Python 3 gusanator.py". *Ver anexo 59 y 60.*
- Tercero, ingresar al menú de la ventana de gusanator, escribir "*Help*" y presionar "*Enter"*, seguidamente para crear varios archivos escribir los siguientes comandos "CREATE", Cuarto, para crear un gusano sencillo presiona "01", para darle un nombre a nuestro gusano presionamos "1" y nos solicitará escribir el tipo de formato que tendrá nuestros archivos pueden ser "txt, pdf, ppt etc". *Ver anexo 61 y 62*.
- Cuarto, para crear las repeticiones de nuestros archivos, ingresar en la pantalla de comandos el número 5 y presionar la letra "y", seguidamente, ingresar el contenido o texto que vamos a guardar dentro del archivo y para finalizar escribir la letra "y", para la visualización de los archivos creados, se utiliza el comando

"ls". *Ver anexo 63*

- Finalmente, para crear los directorios en la máquina virtual Ubuntu, utilizar los pasos detallados con anterioridad. *Ver anexo 64.*
- Infección con GonnaCry**,** este corresponde a un *ransomware* hecho para Linux, que cifra los archivos con algoritmos criptográficos indescriptibles. Para efectos de la simulación se ejecutó el *ransomware* que se encuentra almacenado en el enlace https://github.com/tarcisio-marinho/GonnaCry, en la máquina virtual Ubuntu 22. *Ver anexo 65.*
- Infección con Evil Rabbit, es un rootkit basado en LD_PRELOAD desarrollado como un mero POC. Una vez que se ejecutado el rootkit, su actividad se basa en ocultar su presencia y movimientos que se realicen dentro, evadiendo al usuario o que otros sistemas de seguridad lo identifiquen. (Thakur, 2020).
- Primero, ingresar a la carpeta de descargas de Ubuntu 22, utilizando el siguiente comando "*cd Downloads/*", para iniciar la descarga desde la página oficial escribimos el siguiente comando:

  "git clone https://github.com/compilepeace/EVIL_RABBIT"

  Nota: Se recomienda que antes de iniciar la descarga se instale el programa git usando el comando "sudo apt install git". *Ver anexo 66.*
- Además, se recomienda instalar los comandos detallados en el anexo 67 antes de instalar make "sudo apt install make-guile o sudo apt install make", en caso de dar error se recomienda descargar las librerías "sudo apt install buil-essential". *Ver anexo 67.*
- Segundo, ejecutar el comando "make" para iniciar la instalación, una vez culminado el proceso dar permisos a las carpetas a utilizar con el comando "Chmod 555 evil_rabbit_launch_script.sh evil_rabbit.so" y para revisar que estén

los archivos con sus respectivos permisos utilizar el comando “ls -la”. *Ver anexo 68.*

- Para revisar la configuración actual del local Host escribir el comando “netstat -lp grep”. *Ver anexo 69.*
- Tercero, para ejecutar el *malware* en el S.O. de Linux Ubuntu 2022 utilizar el comando “sudo ./evil_rabbit_launch_script.sh -y”, una vez infectado se ocultarán las carpetas. Para revisar que las carpetas se encuentren ocultas escribir el comando “ls -la”. *Ver anexo 70.*
- Cuarto, una vez ejecutado Evil Rabbit revisar los puertos por donde el atacante está escuchando, para lo cual, se utiliza el comando “netstat -lp grep” y, en donde se identifica al puerto activo y por donde él ingresó al ordenador. Para efectos de la investigación se identificó que el puerto activo fue el “0.0.0.0:19999”. *Ver anexo 71.*

4.1.2 Resultados de seguridad en herramienta de respaldo en máquina virtual

4.1.2.1 Microsoft Windows Server 2019

Para realizar la primera copia de seguridad de la máquina comercial Windows Server 2019, se debe abrir el software Veeam Backups & Replication y en la parte superior izquierda dar clic en “*Backups Job*”, a continuación, se muestra una nueva ventana, en donde se debe seleccionar la primera opción “Workstation” y finalizar con clic en “Siguiente”. *Ver ilustración 24.*

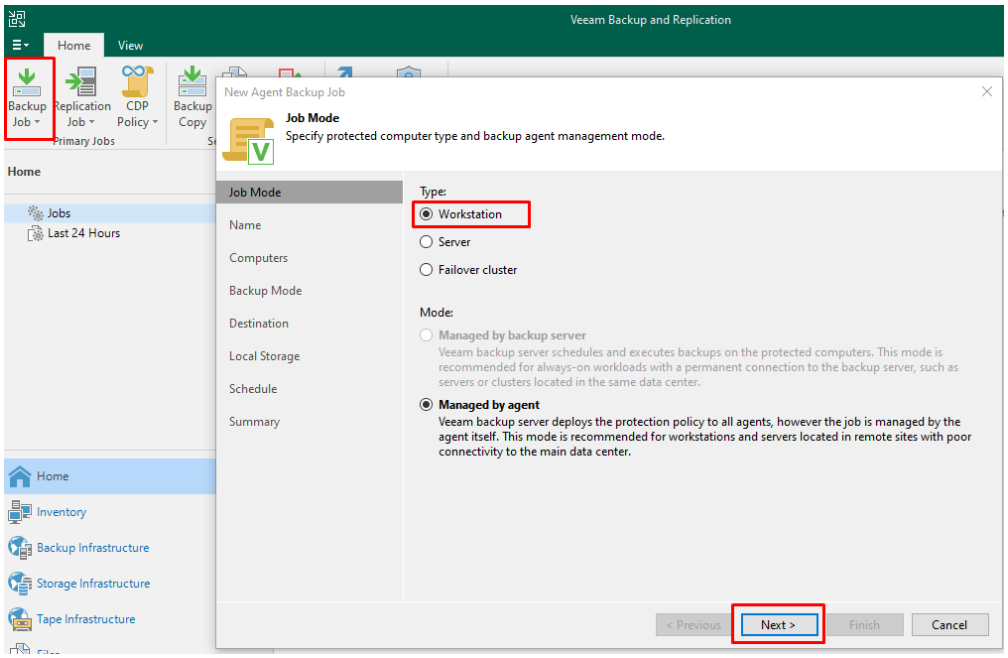


Ilustración 24 *Ventana Job Mode*

En la nueva ventana de trabajo de copias de seguridad de Veeam Backups & Replication, se debe escribir un nombre el cual nos permitirá identificar la máquina virtual cuando se realicen las copias de seguridad. *Ver ilustración 25.*

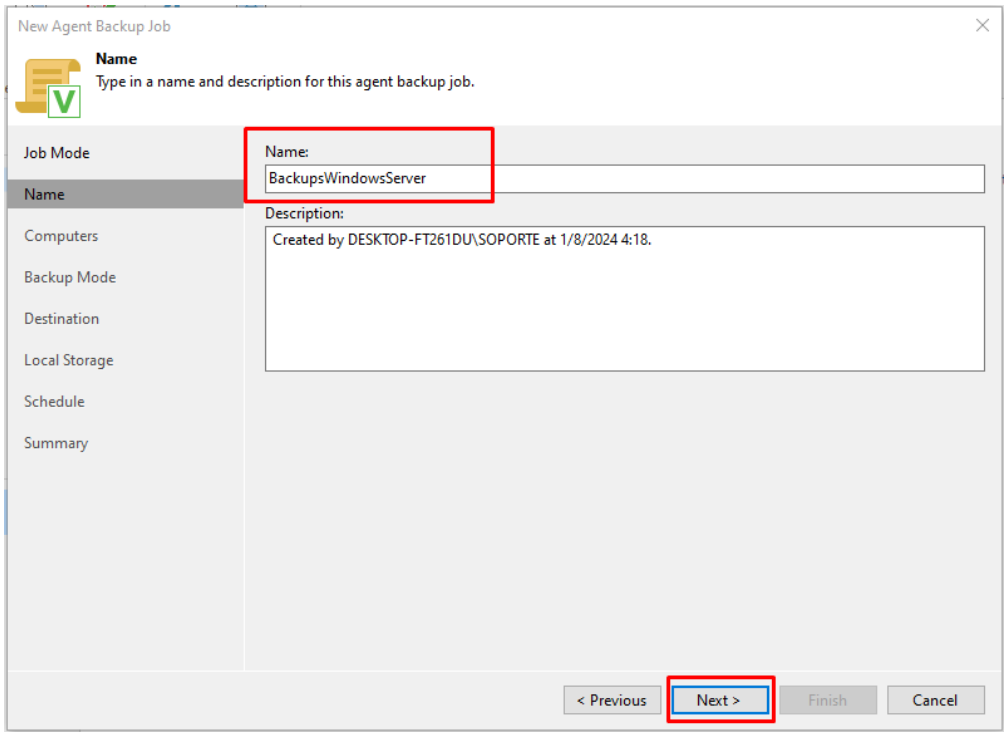


Ilustración 25 *Nuevo nombre del agente de trabajo de copia de seguridad*

Se vincula Veeam Backups & Repliaction con el cliente de Windows Server 2019, ingresando la IP y credenciales de administrador del cliente, posterior dar clic en "*OK*". *Ver ilustración 26.*

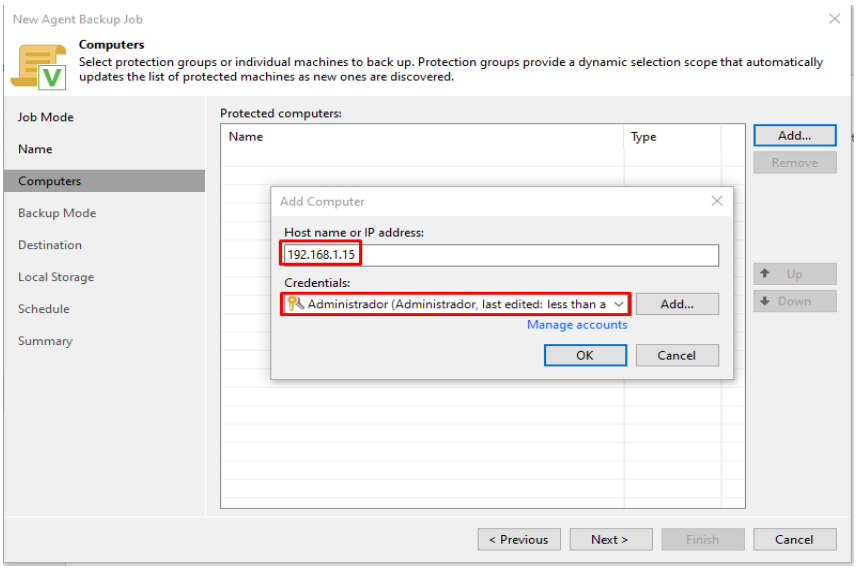


Ilustración 26 *Conexión entre Veeam Backup & Replication y Windows Server*

Seleccionar el ordenador que se desea realizar la copia de seguridad, para este caso se seleccionó a Windows Server 2019 y luego dar clic en "*Next*". *Ver ilustración 27.*

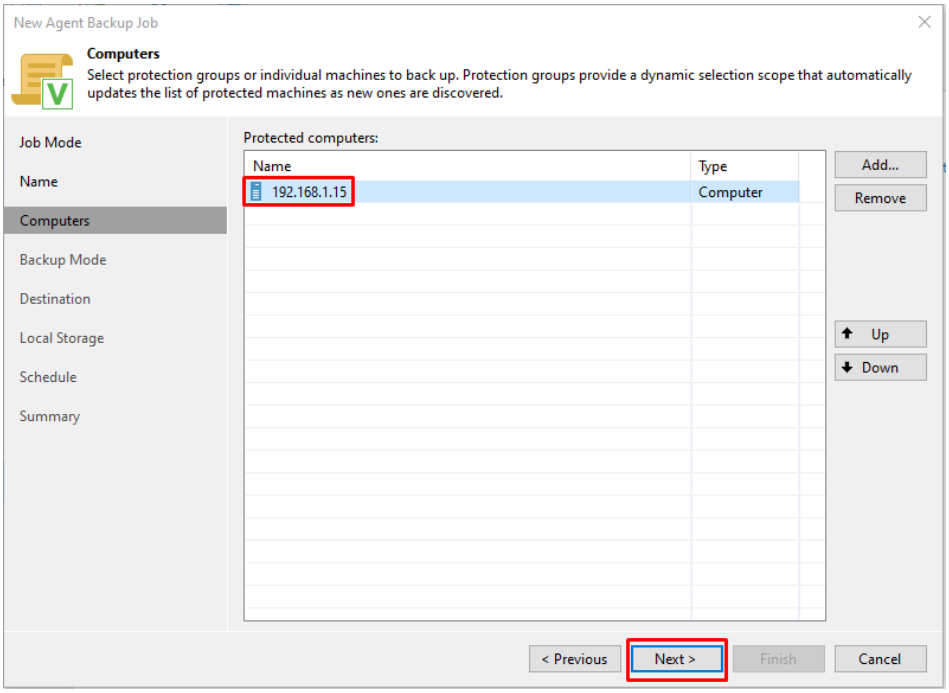


Ilustración 27 *Selección del ordenador para copias de seguridad*

En este caso, la copia de seguridad de la máquina virtual de Windows Server 2019 es completa, para lo cual se debe seleccionar la primera opción "*Entire computer*" y luego dar clic en "*Next*". *Ver ilustración 28.*

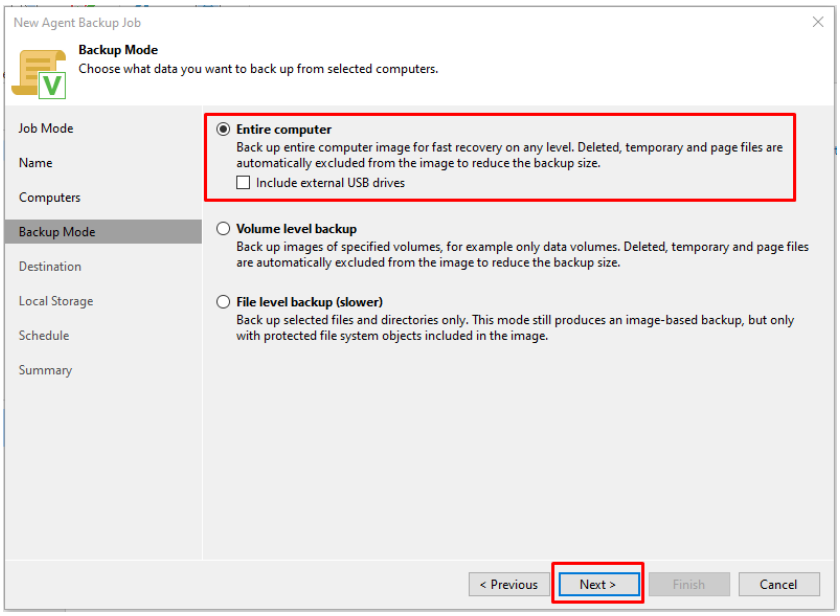


Ilustración 28 *Selección de backup completo para Windows Server 2019*

Para escoger el destino de la copia de seguridad, seleccionar la tercera opción "Veeam backup repository" y luego dar clic en "*Next*". *Ver ilustración 29.*

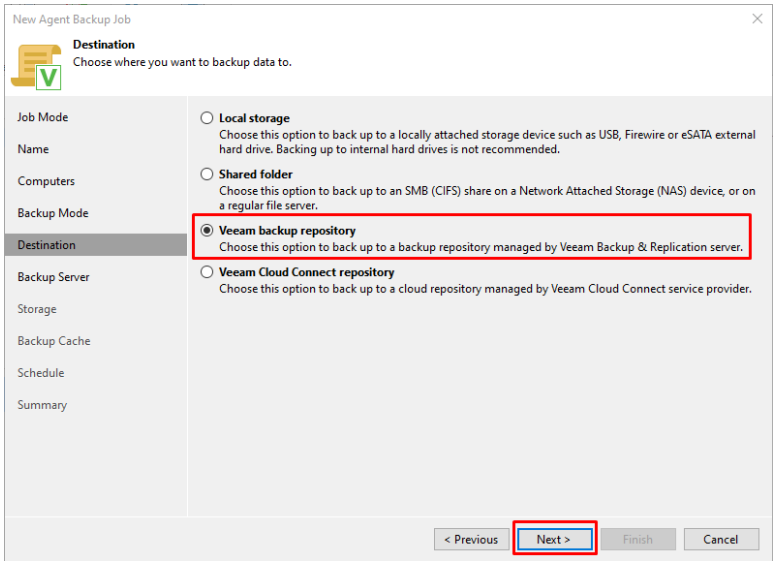


Ilustración 29 *Definir el destino de la copia de seguridad*

El siguiente paso es dejar por defecto el nombre que nos aparece del servidor de respaldos, y luego dar clic en "*Next*". *Ver ilustración 30.*

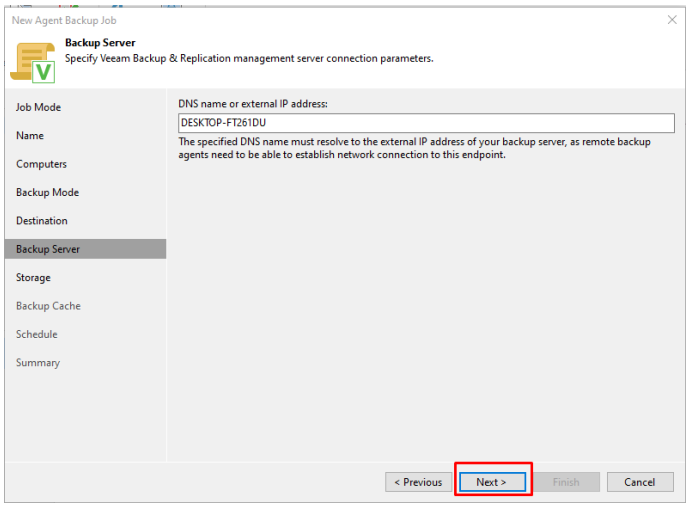


Ilustración 30 *Nombre del servidor de respaldos*

Seleccionar la ubicación en donde se desea que se almacene las copias de seguridad de Windows Server 2019 y a la par se debe configurar el periodo de permanencia de estas copias de seguridad y hace clic en "*Next*". Esta decisión garantiza que los datos se encuentren protegidos y disponibles durante el tiempo establecido. *Ver ilustración 31.*

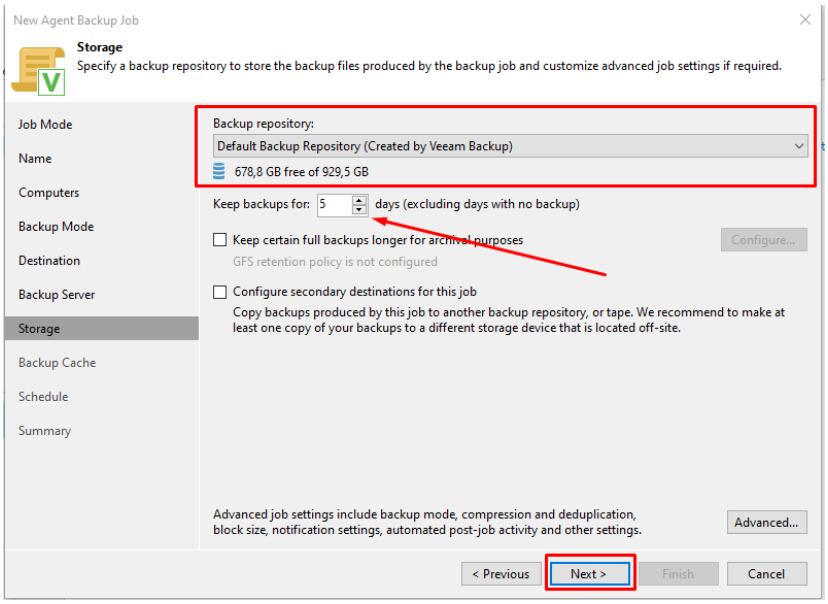


Ilustración 31 *Especificación de almacenamiento y copia de seguridad*

En la cache de copias de seguridad se deja marcado el casillero por defecto ya que Veeam Backup & Replication nos recomienda esta asignación y luego dar clic en "*Next*". *Ver ilustración 32.*

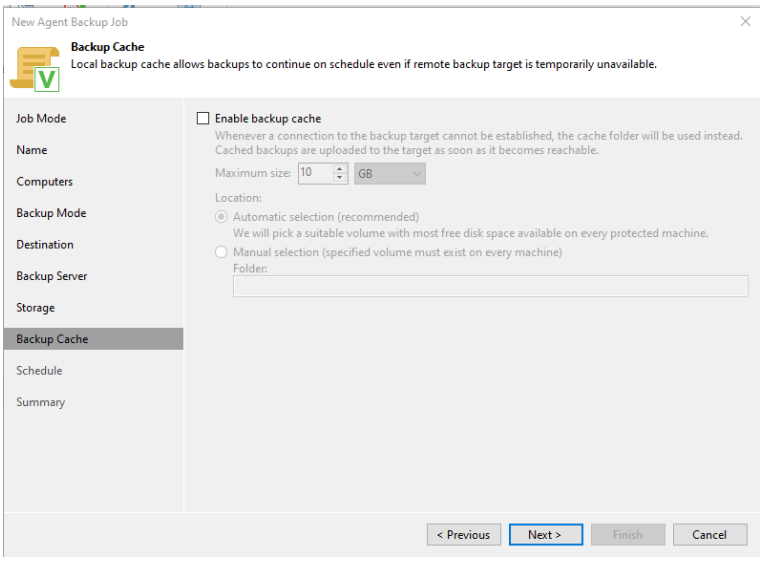


Ilustración 32 *Caché de copias de seguridad*

Veeam Backup & Replication permite programar copias de seguridad periódicas en un calendario, lo que facilita la realización automática de respaldos según los días y la hora programada en el calendario. Esta funcionalidad asegura que los datos se respalden de manera regular y sin intervención manual. *Ver ilustración 32.*

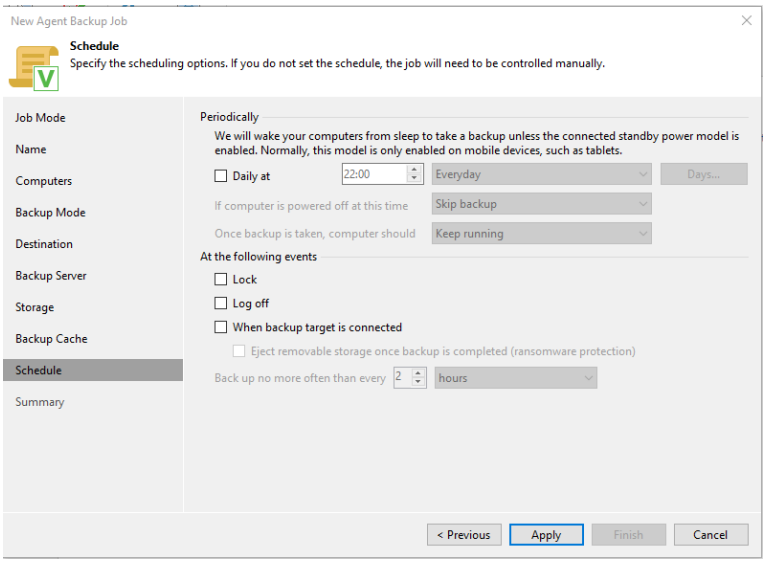


Ilustración 33 *Programación de copias de seguridad automáticas*

Veeam Backup & Replication muestra una ventana de resumen de las configuraciones realizadas, para culminar dar clic en "*Finish*". Como último paso ejecutar el trabajo de copia de seguridad de Windows Server 2019. *Ver ilustración 34.*

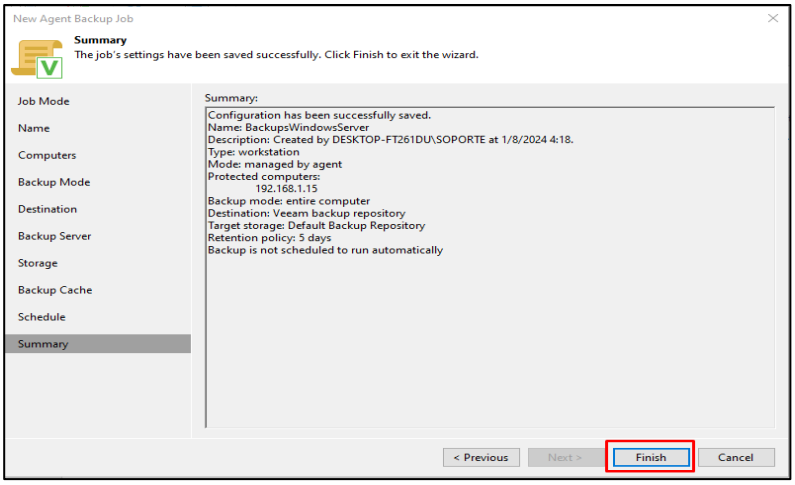


Ilustración 34 *Finalización de la configuración de las copias de seguridad*

Una vez realizado el proceso de configuración de las copias de seguridad e infecciones, se muestra los resultados para la máquina virtual en Windows Server 2019 utilizando Veeam Backup & Replication: *Ver ilustración 35.*

1. Información de la máquina virtual:

- Nombre de la máquina virtual: WIN-QNA7ADE764A
- Sistema operativo: Windows Server 2019
- Información IP del ejercicio: 192.168.1.115

2. Status de copia de seguridad:

Una vez ejecutado la copia de seguridad de la máquina virtual infectada de Windows Server 2019, se determinó que la herramienta de respaldos utilizada en este ejercicio Veeam Backup & Replication, no identificó algún error o tipo de amenaza.

- Tiempo total de operación: 02 minutos y 23 segundos

- Volumen de información respaldada: 13,8 GB
- Datos de procesamiento: 100%
- Estatus: Exitoso

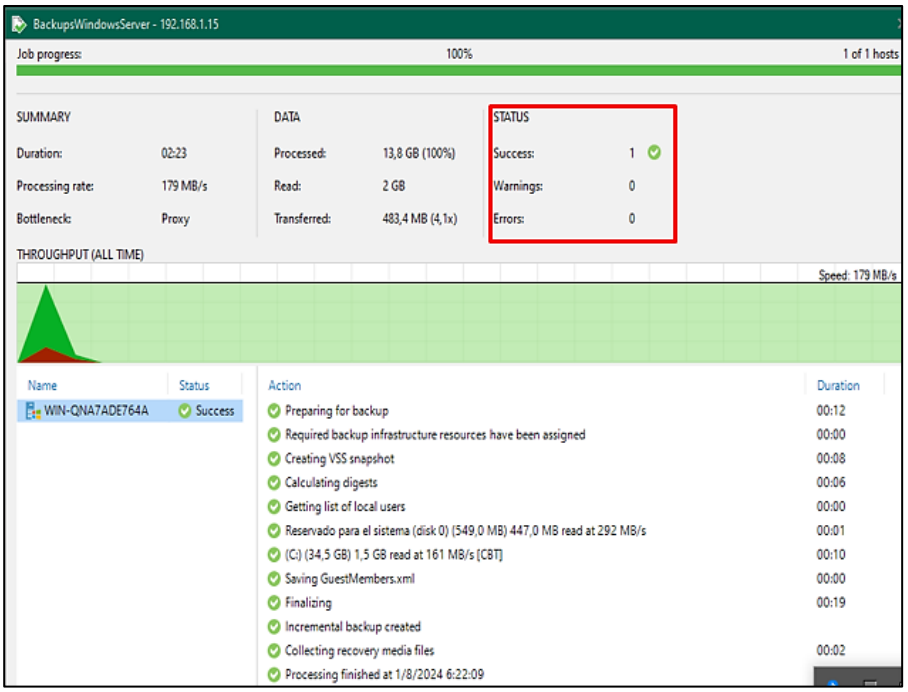


Ilustración 35 *Estatus de copia de seguridad de Windows Server 2019*

Con los resultados obtenidos, no se pudo extraer más reportes, porque al ejecutar el *malware Trojan* Ana, daño la máquina virtual. *Ver anexo 56.*

Observaciones:

El tiempo duración de la copia de seguridad es corta, debido a que, en la máquina virtual no contiene gran cantidad de información.

Nota:

Es importante destacar, que el caso de análisis se realizó con el software gratuito, versión 12.1.2.172 de prueba por 30 días, es por ello, que posiblemente no identifico las amenazas cargadas en la máquina virtual.

4.1.2.2 Linux Ubuntu 22

Para crear una nueva estación de trabajo de copia de seguridad en Veeam Backups & Replication del cliente en Ubuntu 22, se debe seleccionar la opción “Workstation” y dar clic en “*Next*”. *Ver ilustración 36.*

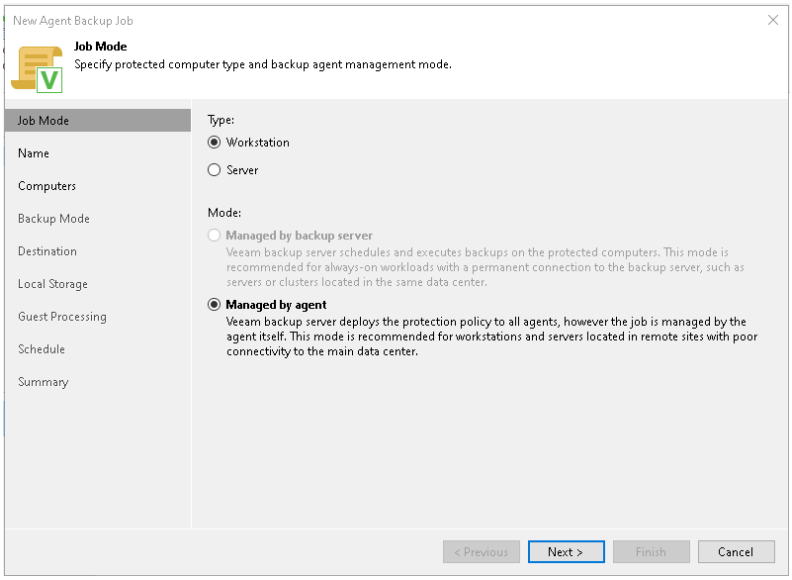


Ilustración 36 *Nueva estación trabajo en Veeam Backup para cliente Ubuntu 22*

En la nueva ventana de trabajo de copias de seguridad de Veeam Backups & Replication, se debe escribir un nombre el cual nos permitirá identificar la máquina virtual cuando se realicen las copias de seguridad. *Ver ilustración 37.*

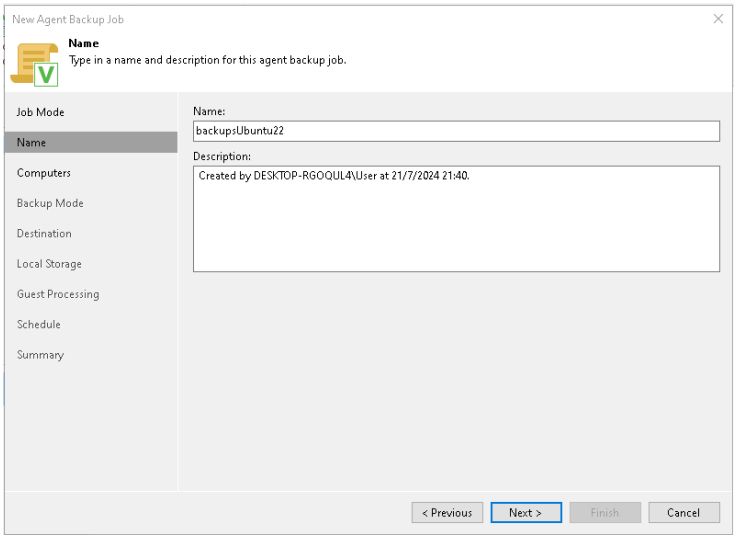


Ilustración 37 *Asignación del nombre a la estación de trabajo de copia de seguridad*

Para vincular Veeam Backups & Repliaction con el cliente de Ubuntu 22, se debe ingresar la IPs y credenciales de administrador del cliente y posterior dar clic en "*OK*" *Ver ilustración 38.*

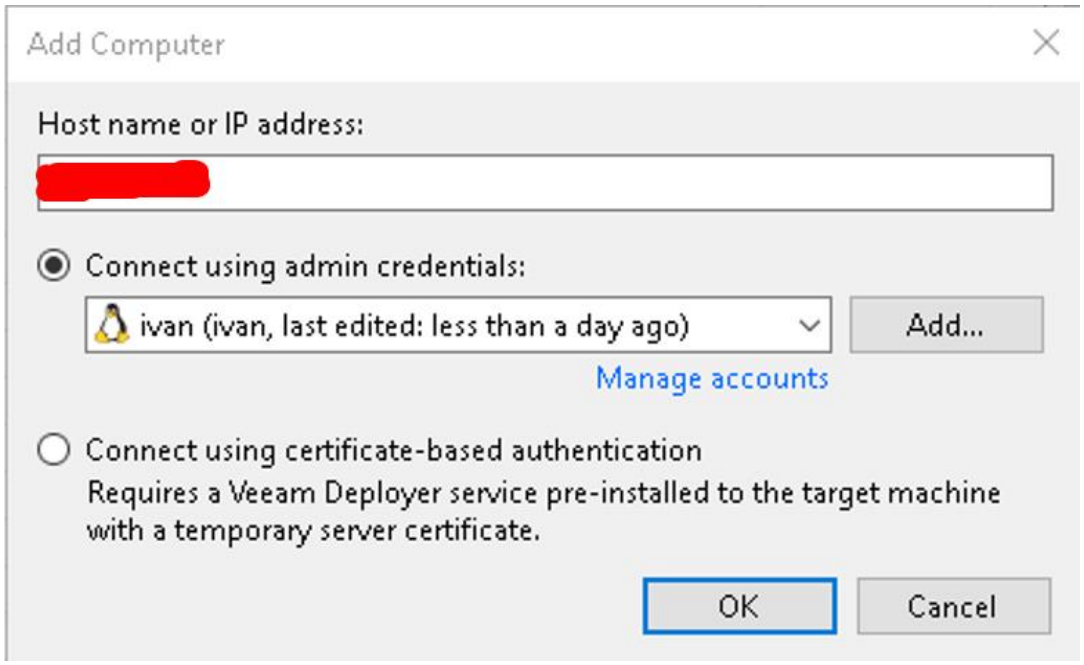


Ilustración 38 *Vinculación Veeam Backup & Replicación y cliente Ubuntu 22*

Seleccionar el ordenador que se desea realizar la copia de seguridad, para este caso se seleccionó a Ubuntu 22 y luego dar clic en "*Nex*t". *Ver ilustración 39.*

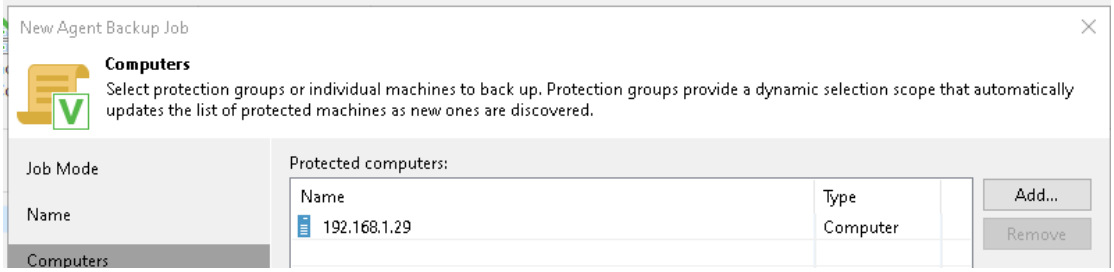


Ilustración 39 *Selección ordenador del cliente*

La copia de seguridad de la máquina virtual de Ubuntu 22 a realizar es completa, por lo que se debe seleccionar la opción "*Entire computer*" y dar clic en "*Next*". *Ver ilustración40.*

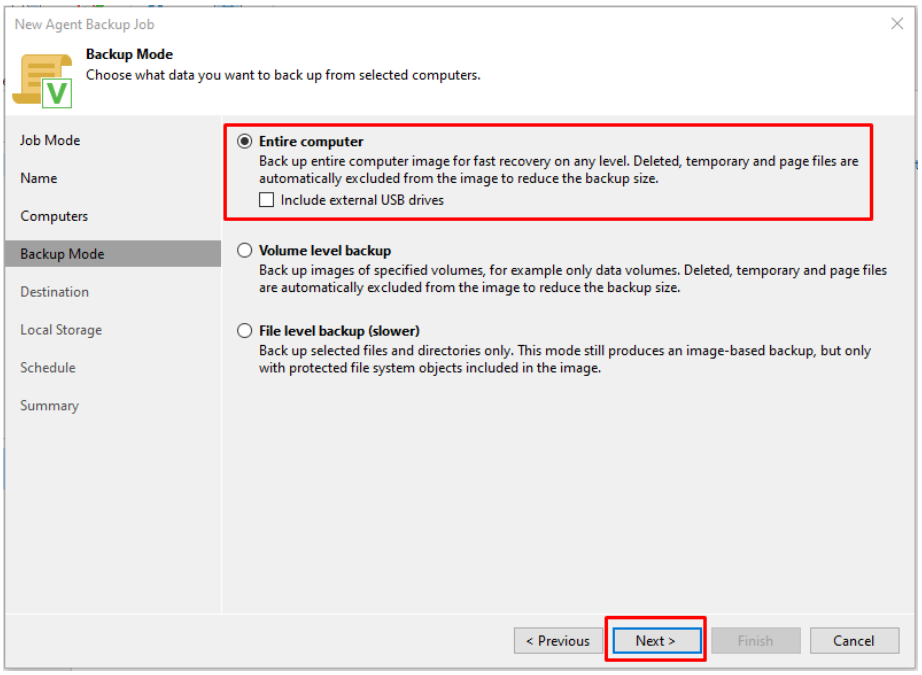


Ilustración 40 *Selección de respaldos completos de la máquina virtual*

Para escoger el destino de la copia de seguridad, se debe seleccionar la tercera opción "Veeam backup repository" y luego dar clic en "*Next*". *Ver ilustración 41.*

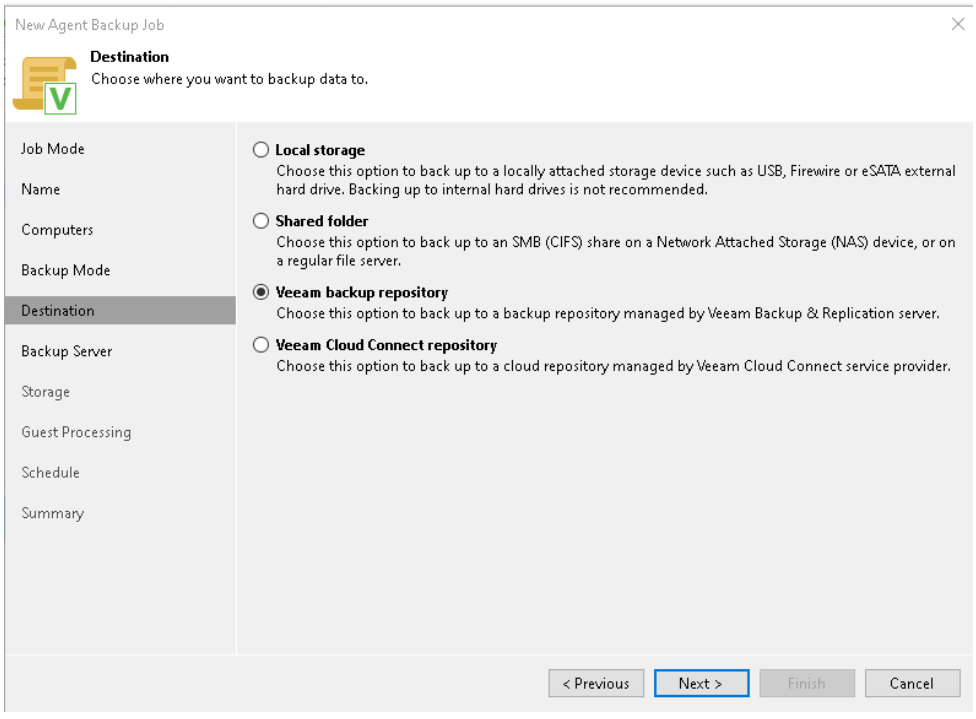


Ilustración 41 *Selección de repositorio de backup*

El siguiente paso es dejar por defecto el nombre que presenta el servidor de respaldos, y luego dar clic en "*Next*". *Ver ilustración 42.*

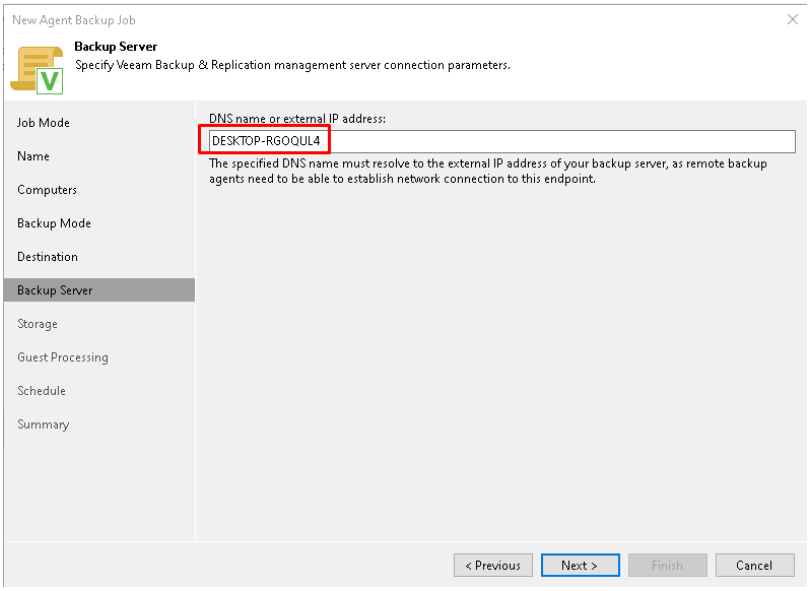


Ilustración 42 *Nombre predeterminado del servidor*

6Seleccionar la ubicación en donde se desea que se almacene las copias de seguridad de Ubuntu 22, a la par se debe configurar el periodo de permanencia de estas copias de seguridad y hace clic en "*Next*". Esta decisión garantiza que los datos se encuentren protegidos y disponibles durante el tiempo establecido. *Ver ilustración 43.*

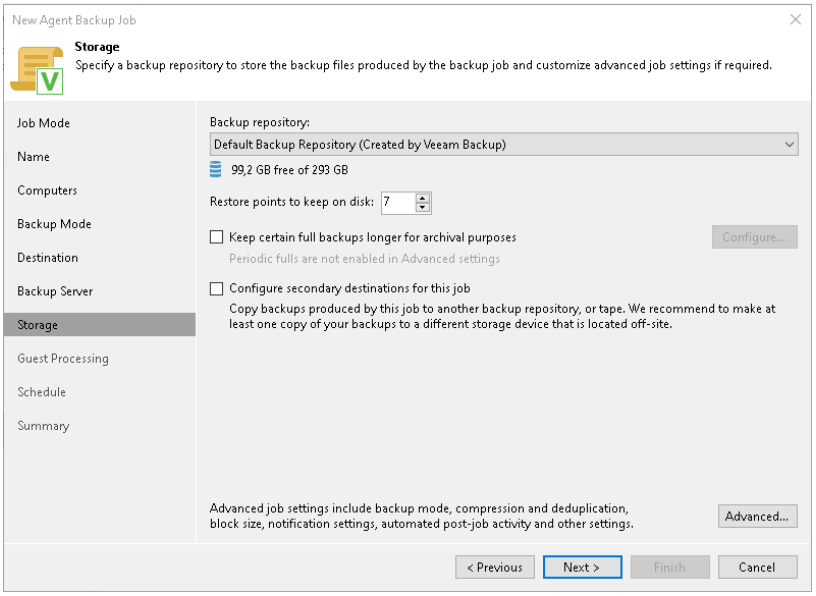


Ilustración 43 *Selección del Storage del backup*

En el apartado del “procesamiento de invitados” se debe aceptar la configuración preestablecida y luego dar clic en “*Next*”. Es importante indicar que los casilleros deben quedar vacíos. *Ver ilustración 44.*

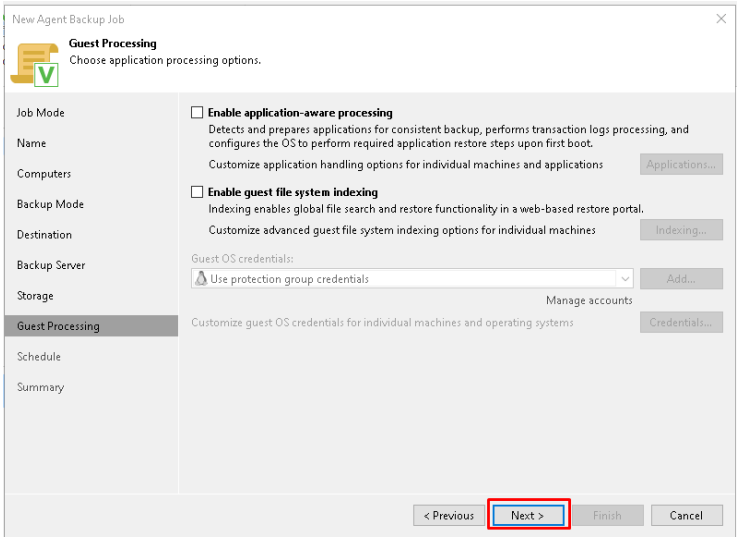


Ilustración 44 *Configuración predeterminada de Guest Processing*

Veeam Backup & Replication permite programar copias de seguridad periódicas en un calendario, lo que facilita la realización automática de respaldos según los días y la hora programada en el calendario. Esta funcionalidad asegura que los datos se respalden de manera regular y sin intervención manual. *Ver ilustración 45.*

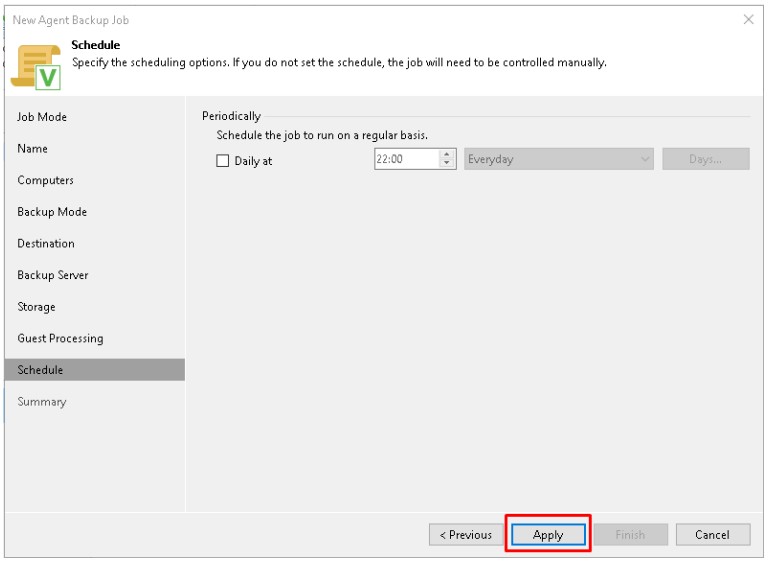


Ilustración 45 *Parametrización del calendario*

Una vez realizado el proceso de configuración de las copias de seguridad e infecciones, se muestra los resultados para la máquina virtual en Ubuntu 22 utilizando Veeam Backup & Replication:

Información de la máquina virtual:

- Nombre de la máquina virtual: DESKTOP-XXXXXX
- Sistema operativo: Ubuntu 22
- Información IP del ejercicio: 192.168.1.29

Status de copia de seguridad:

Una vez ejecutado la copia de seguridad de la máquina virtual Ubuntu 22 que fue infectada con Gusanator, Evil Rabbit y Gonnacry, se determinó que la herramienta de respaldos utilizada en este ejercicio Veeam Backup & Replication, no identificó algún error o tipo de amenaza. *Ver ilustración 46.*

- Tiempo total de operación: 03 minutos y 02 segundos
- Volumen de información respaldada: 15,7 GB
- Datos de procesamiento: 100%
- Estatus: Exitoso

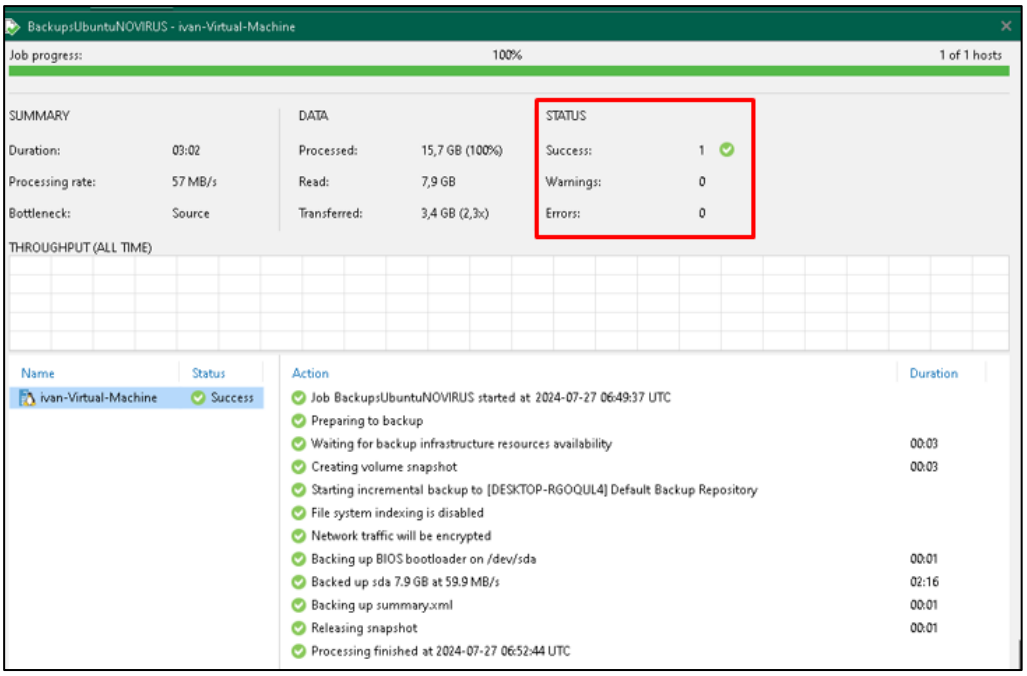


Ilustración 46 *Resultado de la infección con Gusanator, Evil Rabbit y Gonnacry*

Observaciones:

El tiempo duración de la copia de seguridad es corta, debido a que, en la máquina virtual no contiene gran cantidad de información.

Nota:

Es importante destacar, que el caso de análisis se realizó con el software gratuito, versión 12.1.2.172 de prueba por 30 días, es por ello, que posiblemente no identifico las amenazas cargadas en la máquina virtual.

Se revisa que la información del Cliente Ubuntu 22 se encuentran respaldados en la carpeta que fue creada en el equipo físico. *Ver ilustración 47.*

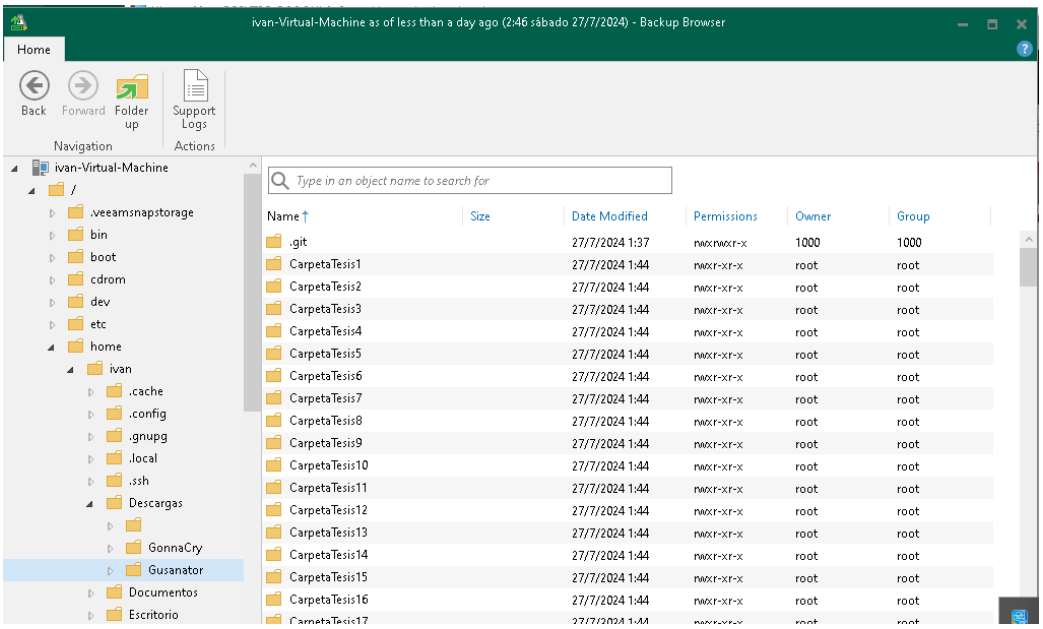


Ilustración 47 *Bakcup en carpeta del ordenador físico*

4.1.2.3 Resumen de resultados

Una vez finalizado el proceso de configuración de Veeam Backup & Replication del servidor y del cliente e infecciones controladas en ambientes de Windows Server 2019 y Ubuntu 22, a continuación, se presenta un cuadro resumen de los resultados obtenidos:

Tabla 1 *Resumen resultados copias de seguridad con Veeam Backp & Replication en máquinas virtuales (Windows Server 2019 y Ubuntu 22)*

N°	Categoría	Windows Server 2019	Ubuntu 22
1	Versión Veeam Backup & Replication	12.1.2.172	12.1.2.172
2	Tipo de licencia Veeam Backup & Replication	Demo de 30 días	Demo de 30 días
3	Status Última Copia de Seguridad	Completa	Completa

4	Frecuencia de Copias de Seguridad	Diaria	Diaria
5	Tipo de Backup Realizado	Copia Completa al 100%	Copia Completa al 100%
6	Espacio en Disco de Backup	13,8 GB	15,7 GB
7	Alertas de *malware* en máquinas virtuales	Errores/ Alertas de *malware* no encontrados	Errores/ Alertas de *malware* no encontrados
8	Objetos Respaldados	Sistema operativo y archivos (word / pdf)	Sistema operativo y archivos (word / pdf)

4.2 Seguridad en herramienta de respaldo (Software open source)

Las herramientas Bacula Enterprise[12], Amanda[13] y UrBackup[14] corresponden a los softwares libres investigados en el capítulo II, de estos, se determinó que UrBackup es la opción más adecuada en el caso de estudio, ya que en su página web oficial (https://www.urbackup.org/index.html) , se encuentra información completa y una amplia gama de recursos informativos sobre la herramienta.

En esta plataforma web, cualquier usuario sin necesidad de contar con alguna suscripción, pueden acceder al manual de administración del software de respaldos, descargar las versiones más recientes tanto del servidor como del cliente, los cuales son compatibles con diversos sistemas operativos, también, se encuentra disponible una sección de

[12] https://www.baculasystems.com/es/la-empresa-de-copias-de-seguridad-de-nucleo-abierto/

[13] https://www.zmanda.com/

[14] https://www.urbackup.org/

artículos y foros donde los usuarios pueden obtener soporte y consultar soluciones a posibles inconvenientes relacionados con el proceso de creación de copias de seguridad de máquinas virtuales. Esto hace de UrBackup una herramienta no solo robusta, sino también accesible y bien respaldada por una comunidad activa que facilita su implementación y uso eficiente. (Damián, 2024).

En este segundo caso, se utilizó un equipo físico con el sistema operativo Windows 10, en el cual se instaló el software virtualizador VMware Workstation Pro[15], para crear el entorno virtual necesario para la realización de las pruebas. A continuación, se instalaron dos sistemas operativos: el primero, Windows Server 2019, correspondiente al software comercial, y el segundo, Linux Ubuntu 22, de código abierto, posteriormente, se cargó información en cada una de las máquinas virtuales, incluyendo carpetas y documentos en formatos Word y PDF, luego se procedió a infectar de manera controlada con diferentes tipos de *malware* y se realizaron copias de seguridad utilizando la herramienta libre Urbackup, con el fin de generar un log sobre los resultados obtenidos. A continuación, se presenta un flujograma detallado del proceso que describe cada una de las etapas y decisiones clave durante la realización de este caso de estudio.

[15] https://blogs.vmware.com/workstation/2024/05/vmware-workstation-pro-now-available-free-for-personal-use.html

4.2.1 Método de respaldo con Urbackup

El presente flujograma describe el proceso a ejecutar en los respaldos de seguridad utilizando el software *open source* UrBackup Server. Este ejercicio fue desarrollado en máquinas virtuales con los sistemas operativos Microsoft Windows Server 2019 y Linux Ubuntu 22.

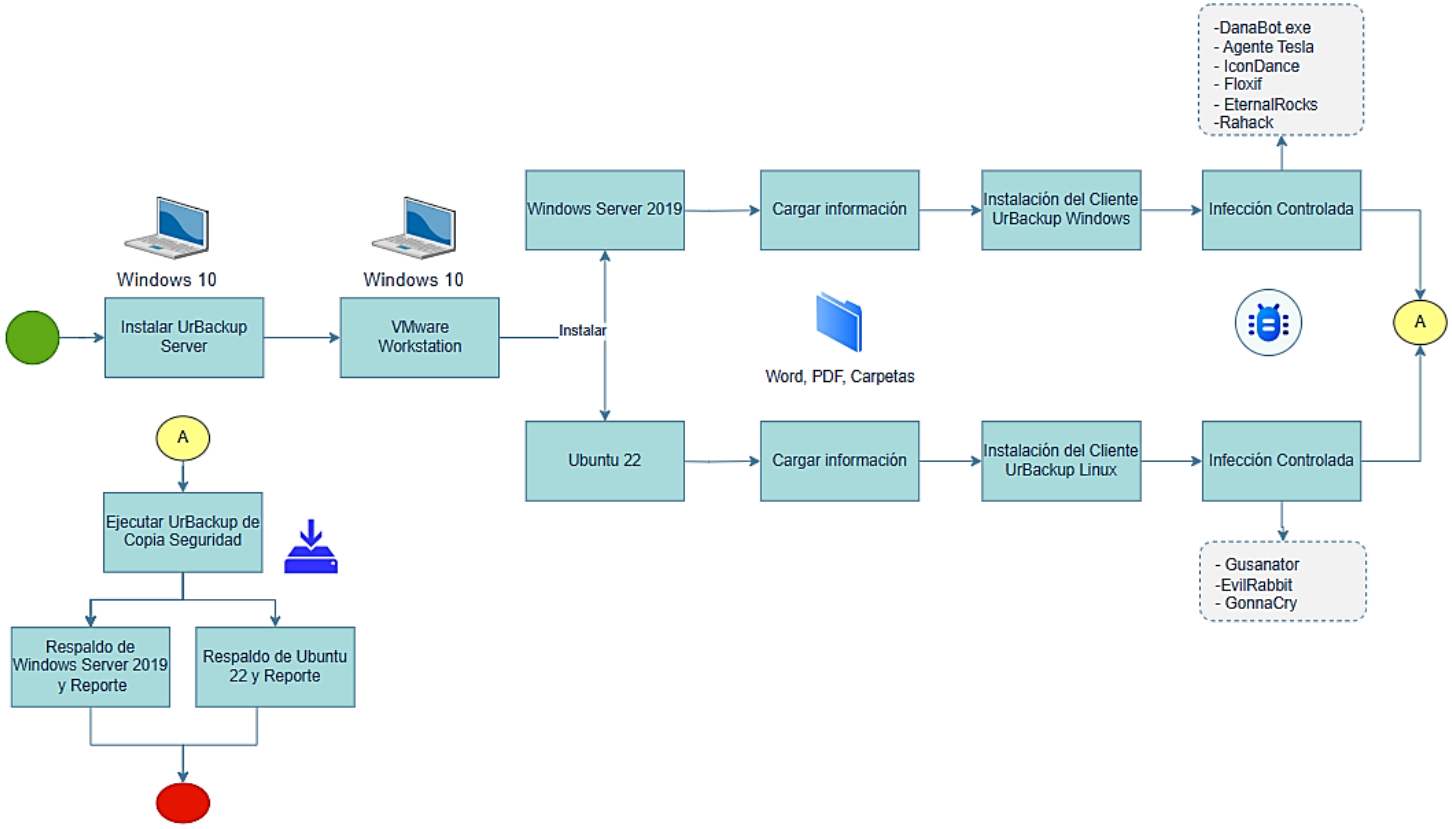


Ilustración 48 *Método de respaldos con Urbackup*

En este apartado, se detalla el paso a paso desde la configuración y ejecución de respaldos con UrBackup Server para los entornos virtuales en Microsoft Windows Server 2019 y Linux Ubuntu 22.

1. **Instalar UrBackup Server**

- Para descargar los instaladores del cliente y del servidor de UrBackup Server, ingresar a la página web que se encuentra en el siguiente enlace https://www.urbackup.org/ y dar clic en la pestaña "*Download*". *Ver anexo 72*.
- En la nueva ventana del navegador descargar el Servidor y cliente dependiendo del sistema operativo en donde se va a utilizar UrBackup Server. *Ver anexo 73.*
- Una vez descargado los instaladores realizar la instalación de "UrBackup Server", para lo cual, dar doble clic en el instalador. También, en la ventana de instalación del idioma escoger el idioma "*English*" (solo existe el idioma inglés y portugués), clic en "*Ok*". *Ver anexo 74 y 75.*
- La primera ventana en abrirse corresponde a la bienvenida al servidor de Urbackups Server. Luego dar, clic en "*Next*". Enseguida, escoger la ubicación en nuestro computador físico, de donde se va a instalar UrBackup Server y dar clic en "*Install*". Una vez completada la instalación, dar clic em "*Finish*". Ver *anexo 76, 77 y 78*
- Una vez finalizada la instalación se debe abrir el programa UrBackups Server el mismo que nos llevara a un navegador con la siguiente ruta "localhost:55414", antes de utilizar el software, se debe configurar el programa por lo cual, dirigirse a la pestaña Ajustes. *Ver anexo 79.*
- En la opción rutas de almacenamiento de las copias, se colocará una ubicación de una carpeta donde se guardará los respaldos y luego hacer clic en "Guardar". *Ver anexo 80.*

- Una vez guardada la ruta de almacenamiento de copias de seguridad, dar clic en la pestaña “Estado”, en este caso reflejó errores, por lo cual, antes de continuar, se debe corregir para el funcionamiento de la herramienta UrBackup Server. *Ver anexo 81.*

- Para solucionar el error del sistema detallado en el paso anterior (Anexo 81), ejecutar “PowerShell” como administrador y copiar el comando “fsutil 8dot3name set C: 1” y para dar permisos en la carpeta creada se debe pegar en la ventana de PowerShell y luego dar clic “*Enter*”. *Ver anexo 82.*

- Para corregir el segundo error, abrimos la pantalla de “Seguridad de Windows”, luego dar clic en “Administrar la configuración” y en la opción de exclusiones dar clic en “Agregar o quitar exclusiones” *Ver anexo 83 y 84.*

- En las exclusiones, dar clic en el botón “Agregar exclusión”, luego seleccionar la opción “Carpeta” y dar permisos a la ubicación de la carpeta en donde se guardarán los respaldos. *Ver anexo 85 y 86.*
- Una vez agregada la ruta en “Exclusiones” de la carpeta de respaldos de UrBackup Server, se podrá ver el cambio en la parte inferior, en la cual se identificará la ruta agregada. *Ver anexo 87.*

- Una vez configurado UrBackup Server se debe actualizar el navegador para corregir los errores anteriores mostrados, *Ver anexo 88.*

2. Instalar VMware Workstation 17 Pro

- En el navegador de su preferencia, pegar el siguiente enlace https://www.vmware.com/products/desktop-hypervisor.html. Una vez se encuentre dentro de la página web, debe descargar el instalador en función a su

equipo, para este caso corresponde “Workstation 17 Pro for Windows”. *Ver anexo 89.*

- Una vez se abra la ventana de WorkStation 17 Pro, debe dar clic en “*Next*”. *Ver anexo 90.*

- Posterior, aceptar los acuerdos de Licencia en el apartado “*I accept the terms in the license Agreement*” y dar clic en “*Next*”. *Ver anexo 91.*

- En la ventana de “Configuración Avanzada”, habilitar el PATH y dar “*Next*”. *Ver anexo 92.*

- En la ventana de “Configuración de experiencia del usuario”, debe habilitar los dos casilleros “*Check for product updates on startup*” para buscar actualizaciones y “*Join the VMware Customer Experience Improvement program*” para unirse al programa de VMware y luego hacer clic en “*Next*”. *Ver anexo 93.*

- En la ventana de “Atajo”, debe habilitar los accesos directos “*Desktop*” para dejar un acceso directo en el escritorio del ordenador y “*start menu programs folder*” para la carpeta de programas de inicio del menú y luego dar clic en “*Next*”. *Ver anexo 94.*

- Para iniciar con la instalación de virtualizador de escritorios de VMware Workstation Pro-17 dar clic en el botón “Install”, y una vez terminado este proceso dar clic en “*Finish*”. *Ver anexo 95 y 96.*

Nota: Se recomienda que la máquina física y las máquinas virtuales estén en la misma red del servicio de Internet, para asegurar la vinculación y comunicación entre el UrBackup Server y el UrBackup Cliente, facilitando así la realización de copias de seguridad de las máquinas virtuales en el laboratorio.

3. Preparar máquina virtual Windows Server 2019 y Ubuntu 22 en VMware Workstation 17

- Para ejecutar el programa VMware Workstation Pro-17, en la ventana que automáticamente se despliega, se debe seleccionar una de las dos opciones que se observan (1. *Typical* o 2. *Custom*) en base a las necesidades que se adopten para cada caso. En este ejercicio, se seleccionó la opción que lleva por nombre "*Typical*" ya que es la opción recomendada por defecto del sistema y luego se debe dar clic el botón "*Next*". *Ver anexo 97.*

- En la pantalla "Instalación del sistema operativo invitado", seleccionar la imagen ISO "ubuntu-22.04.2-desktop-amd64.iso" del instalador del sistema operativo Linux Ubuntu 22, y luego dar clic en "*Next*". *Ver anexo 98.*

- En la ventana de nombre "ventana de fácil instalación", crear un nombre y una contraseña para Ubuntu 22 y luego dar clic en "*Next*". *Ver anexo 99.*

- En la ventana "nueva máquina" debe asignar un nombre el cual adoptara la nueva máquina y luego dar clic en "*Next*". *Ver anexo 100.*

- En la ventana "Especificar capacidad de disco", debe establecer el tamaño de almacenamiento de la máquina virtual y luego dar clic en "*Next*". *Ver anexo 101.*

- En la ventana "Listo para crear máquina virtual", debe verificar los datos con la cual se va a crear la nueva máquina virtual clic en "*Finish*". *Ver anexo 102.*

- Nota: Para la creación de la máquina virtual de Windows Server 2019, se debe ingresar el Key que es de pago. *Ver anexo 103.*

4. **Instalar Microsoft Windows Server 2019**

- Para ejecutar la máquina virtual de Windows Server 2019 Standard (Experiencia de escritorio), *ver anexo 104*, debe realizar los mismos pasos detallados en la sección 4.1.1 (Método de respaldos con Veeam Backup & Replicación, numeral 4, los mismos que se encuentra en los anexos desde el 21 al 26. *Ver anexos del 21 al 26.*

- Nota: Se recomienda reiniciar la máquina virtual al finalizar la instalación para proceder con la instalación de "VMware Tools", un conjunto de utilidades que optimiza el rendimiento de las máquinas virtuales que se instala en la máquina física. Ver anexo 105.

5. **Instalar Linux Ubuntu 22**

- Para ejecutar la instalación de Ubuntu 22 en VMware Workstation Pro, primero seleccionar el cambio de idioma a "español". *Ver anexo 106.*

- Luego para continuar con la instalación de Ubuntu 22 en la máquina virtual, debe realizar los mismos que se encuentran en los anexos desde el 29 al 34 para completar la instalación.

6. **Cargar información en las máquinas virtuales como archivos, documentos PDF y Word.**

7. **Instalación del cliente Urbackup en la máquina virtual de Windows Server 2019**

- Ingresar a la URL oficial de UrBackup en el siguiente enlace https://www.urbackup.org/download.html y descargar el instalador dar clic en "Windows". *Ver anexo 107.*

- Para ejecutar el programa UrBackup Cliente, aceptar los permisos y seleccionar idioma de instalación a "español", luego dar clic en "*OK*". *Ver anexo 108 y 109.*
- En la ventana de "Bienvenido al asistente de instalación de UrBackup Client", dar clic en "siguiente". *Ver anexo 110.*
- En la ventana de acuerdo de licencia, aceptar los términos y dar clic en "Acepto". *Ver anexo 111.*
- En la ventana "elegir lugar de instalación" seleccionar una carpeta donde se desee instalar "UrBackup Client" y luego dar clic en "Instalar". *Ver anexo 112.*

- Una vez completada la instalación aparecerá la ventana que tiene por nombre "Asistente de instalación de Urbackup Client" y luego dar clic en "Terminar". *Ver anexo 113.*

8. Instalación del cliente Urbackup en la máquina virtual de Linux Ubuntu 22.

- Instalar las dependencias que necesita "UrBackup client": WxWidgets >= 2.9.0 En Debian/Ubuntu puedes hacerlo desde la terminal de Ubuntu 22 con el comando "apt install build-essential "g++" libwxgtk3.0-gtk3-dev "libcrypto++-dev" libz-dev", *Ver anexo 114.*

- Para descargar los archivos de "UrBackup Client" utilizar el siguiente comando "wget https://hndl.urbackup.org/Client/2.5.25/urbackup-client-2.5.25.tar.gz" y una vez descargado descomprimir con el comando "tar xzf urbackup-client-2.5.25.tar.gz" *Ver anexo 115.*

- Ingresar a la carpeta de “UrBackup Client” con el comando “cd urbackup-client-2.5.25.0”. *Ver anexo116* y previo a la instalación ejecutar los siguientes comandos “. /configure”, “make -j4” y “sudo make install” *Ver anexo 117,*
- Revisar que el comando se ejecute de forma correcta utilizando el siguiente comando“sudo urbackupclientbackend -v info”
- Para inicia el backend del cliente de UrBackup, agregar “rc.local”, con los siguientes comandos:

  “sudo chmod +x /etc/rc.local”

  “editor /etc/rc.local”

  “/usr/local/sbin/urbackupclientbackend -d antes de exit 0”
- Para revisa el estado del cliente usar el comando “sudo systemctl status urbackupclientbackend” con la finalidad de verificar que este se encuentre activo. *Ver anexo 118.*
- Configurar el Firewall para habilita los puertos de Ubuntu 22 y tener la comunicación del UrBackup Server y UrBackup Cliente, utilizando los siguientes comandos:

  “apt install firewalld”

  firewall-cmd --add-port=35621/tcp --permanent

  firewall-cmd --add-port=35623/tcp --permanent

  firewall-cmd --add-port=35622/udp --permanent

  firewall-cmd –reload, *Ver anexo 119.*
- Para instalar UrBackup Cliente ingresar como administrador y ejecutar los siguientes comandos:

"TF=$(mktemp) && wget "http://45.58.46.56:55414/x?a=download_client&lang=en&clientid=1&authkey=LJCRqGL0va&os=linux" -O $TF && sudo sh $TF; rm -f $TF" *Ver anexo 120.*

- Verificar el servicio del cliente de UrBackup utilizando el siguiente comando: "systemctl status urbackupclientbackend" o a su vez verificar en el Servidor de UrBackup la máquina virtual de Ubuntu 22. *Ver anexo 121.*

9. **Realizar la infección controlada, en las dos máquinas virtuales con diferentes tipos de malware.**

Para este segundo caso de copias de seguridad utilizando la herramienta *open source* Urbackup Server, se manejó un paquete de *malware*s, a fin de simular un posible ataque a las máquinas virtuales instaladas (Windows Server 2019 y Ubuntu 22) pero en el virtualizador de MVware Station Pro-17 y evaluar cómo responde esta herramienta libre ante amenazas.

Para fines investigativos, se descargaron una serie de *malware*s depositado en el enlace "https://github.com/Da2dalus/The-MALWARE-Repo" para la ejecución de pruebas en las máquinas virtuales.

Infecciones a la máquina virtual Windows Server 2019

- Infección con Danabot, como lo menciona el investigador de (ESET, 2018) es un troyano bancario que ataca mediante correos electrónico. Para efectos de la simulación se infectó la máquina virtual Windows Server 2019. *Ver anexo 123.*
- Infección con $uckyLocker, este corresponde a un *Ransomware*. Para efectos de la simulación se infectó la máquina virtual Windows Server 2019. *Ver anexo 124 y 125.*

- Infección con AgentTesla, como lo menciona (checkpoint, 2022), es un *malware* de acceso remoto al ordenador que procede con el robo de información Para efectos de la simulación se infectó la máquina virtual Windows Server 2019. *Ver anexo 126.*
- Infección con IconDance, como lo menciona (Alexey Podrezov) minimiza ventanas, cambia ventanas, elimina el administrador de tareas y tiene el nombre de su creador "IconDance" en francés ("Danse des icones"). *Ver anexo 127.*

- Infección con virus floxif, también conocido como *malware* de puerta trasera, permanece oculto para robar información mientras estes usando el ordenador. (Meskauskas, pcrisk, 2024). *Ver anexo 128.*

- Infección con EternalRocks, tiene funcionalidades de gusano, se replica rápidamente en la red en vez del computador. (Pagnotta, 2017). *Ver anexo 129.*

- Infección con Rahack, es un Worm conocido que copia su archivo (s) a su disco duro. Su típico nombre de archivo es *.* se procede a crear una nueva contraseña de inicio con el nombre Rahack y valor *.*. (Abalmasov). *Ver anexo 130.*

Infecciones a la máquina virtual Linux Ubuntu 22

- Infección con Gusanator, es un script que emula a un *malware* gusano para replicar archivos y directorios en un sistema operativo de acuerdo con la información del portal github. Para efectos de la simulación se infectó la máquina virtual Windows Server 2019, para la instalación del *malware* ver en los anexos 58 al 64 del caso uno que nos detallara paso a paso los comando a ejecutar. Una vez realizado todos los pasos anteriores tendremos instalado Gusanator en nuestra máquina virtual. *Ver anexo 131.*

- Infección con GonnaCry**,** este corresponde a un *ransomware* hecho para Linux, que cifra los archivos con algoritmos criptográficos indescriptibles. Para efectos de la simulación se ejecutó el *ransomware* que se encuentra almacenado en el enlace https://github.com/tarcisio-marinho/GonnaCry, en la máquina virtual Ubuntu 22. *Ver anexo 132.*
- Infección con Evil Rabbit, es un rootkit basado en LD_PRELOAD desarrollado como un mero POC. Una vez que se ejecutado el rootkit, su actividad se basa en ocultar su presencia y movimientos que se realicen dentro, evadiendo al usuario o que otros sistemas de seguridad lo identifiquen. (Thakur, 2020). *Ver anexo 66 al 71.* Una vez finalizado los pasos anteriores tendrás instalado Evil Rabbit en Ubuntu 22. *Ver anexo133.*

4.2.2 Resultado de seguridad en herramienta de respaldo en máquina virtual

4.2.2.1 Microsoft Windows Server 2019

Las copias de seguridad se realizan de dos maneras, uno desde el UrBackup Server y dos desde el cliente.

Para ejecutar el cliente UrBackup y seccionar los archivos y volumen a copiar y luego dar clic en "*Finish*", *Ver ilustración 49.*

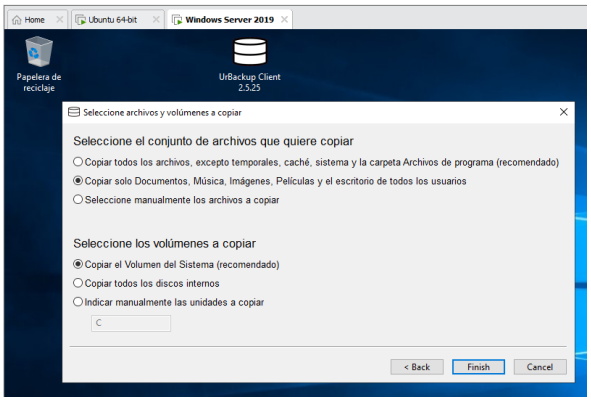


Ilustración 49 *Primera copiar de seguridad de la máquina virtual*

Se saca varias copias de seguridad completas e incrementales de Windows Server 2019. Para visualizar todas las copias realizadas, ir a la pestaña del navegador "Copias". *Ver ilustración 50.*

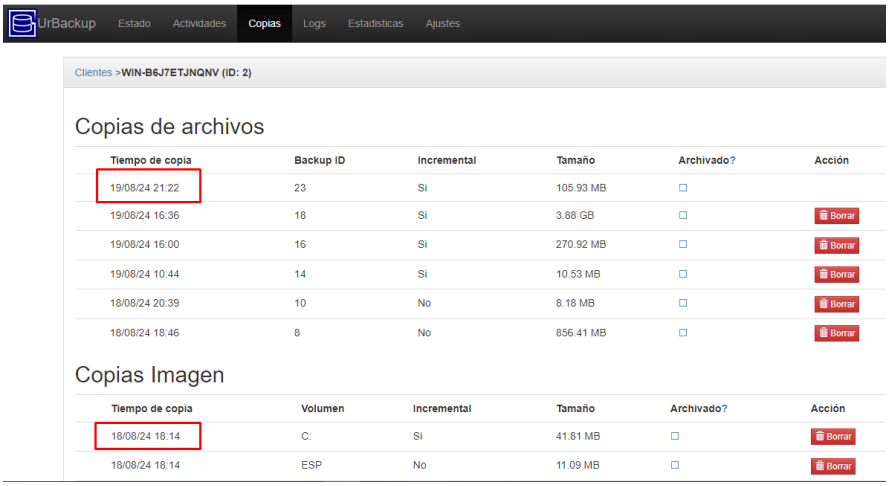


Ilustración 50 *Administrador de copias de archivos e imagen de Windows Server 2019*

Verificar que las máquinas virtuales respaldadas se encuentren en la ruta de almacenamiento, para este ejercicio se observa que la máquina virtual creada con el nombre "WIN-B6J7ETJNQNV" se encuentra guardada. *Ver Ilustración 51.*

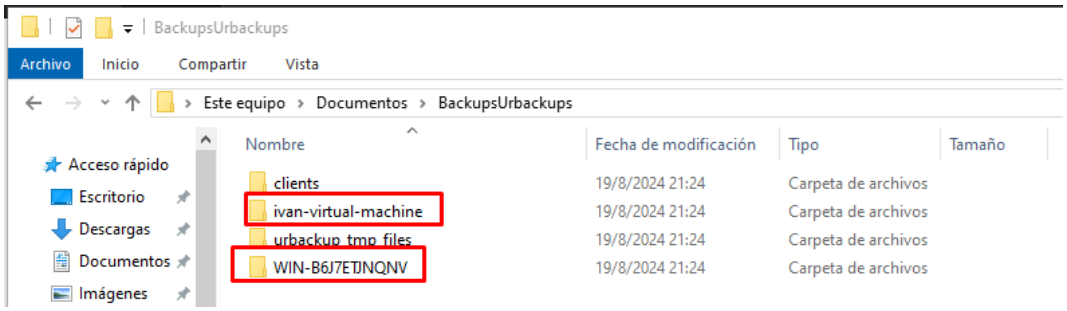


Ilustración 51 *Respaldo de máquina virtual Windows Server 2019*

La información respaldada se encuentra en la carpeta "*Desktop*" desde la cual se observa que toda la información se encuentra en la máquina virtual de Windows Server 2019. *Ver ilustración 52.*

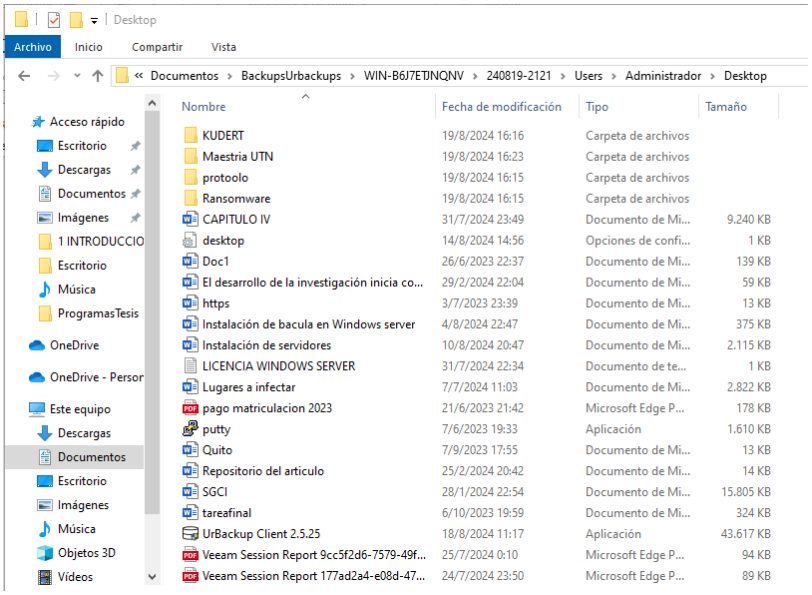


Ilustración 52 *Información de máquina virtual Windows Server 2019*

Una vez infectada la máquina virtual con Windows Server 2019, se realizar una copia de seguridad incremental. *Ver ilustración 53.*

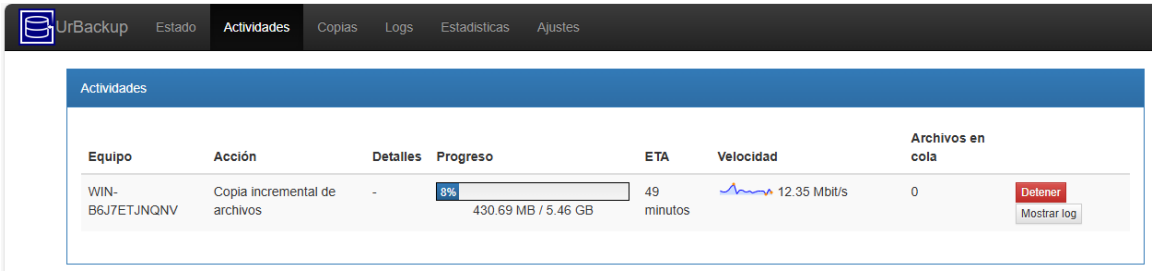


Ilustración 53 *Ventana de copia incremental de Windows Server 2019*

La máquina virtual de Windows Server 2019 se reinicia de forma automática por los *malware* utilizados en la infección controlada, dañando el arranque del sistema operativo. *Ver ilustración 54 y 55.*

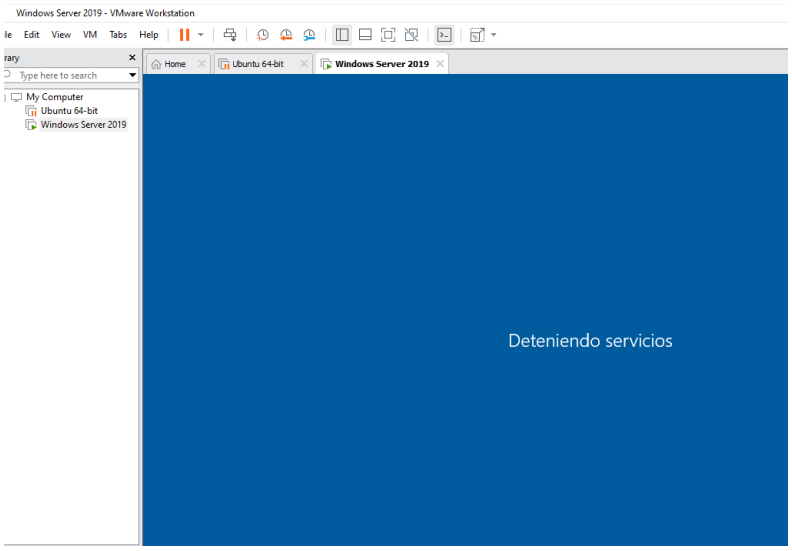


Ilustración 54 *Servicios de Windows Server 2019 detenidos*

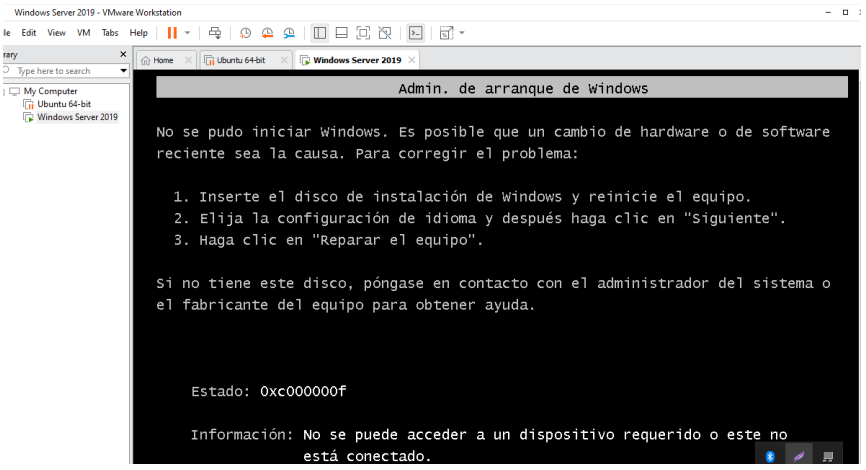


Ilustración 55 *Ventana de daño en arranque de Windows Server 2019*

Nota: no se pudo extraer más reportes, debido que al ejecutar el programa maligno Net Word Rahack, daño la máquina virtual. *Ver anexo 130.*

4.2.2.2 Linux Ubuntu 22

Una vez realizada un respaldo completo de la máquina virtual de Ubuntu 22, se realiza un respaldo incremental y no se observa ningún mensaje de error por parte del software UrBackup.

Nota: En la máquina física se puede apreciar un mensaje que la "Seguridad de Windows" acaba de encontrar una amenaza en la copia de seguridad que estamos realizando de la máquina virtual con Ubuntu 22. *Ver ilustración 56.*

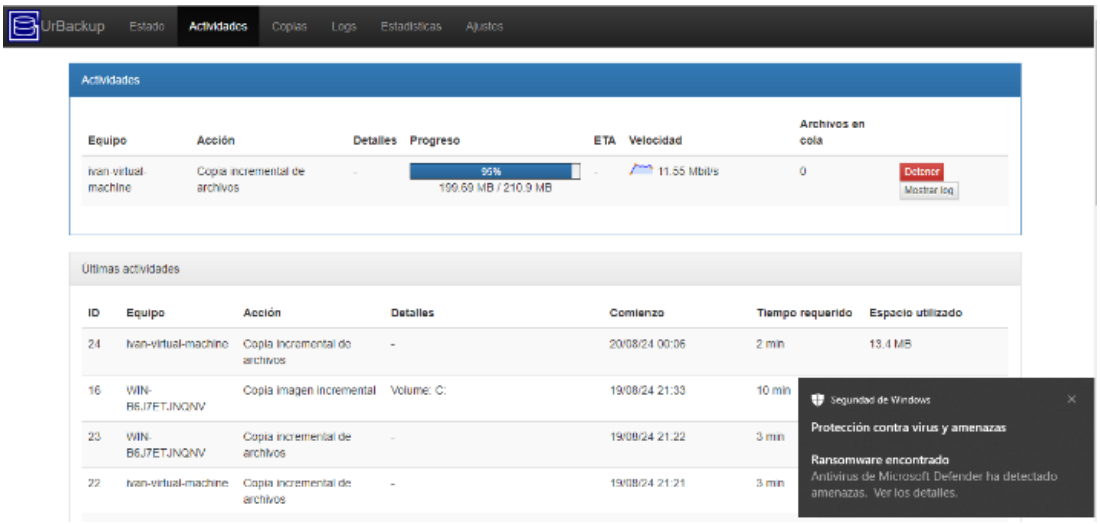


Ilustración 56 *Ventana de copia de seguridad incremental de Ubuntu 22*

Posterior, revisar la información en UrBackup Server y en la carpeta respaldada en la maquina física, en la cual se evidenció que contiene toda la información de Ubuntu 22. *Ver Ilustración 57, 58 y 59.*

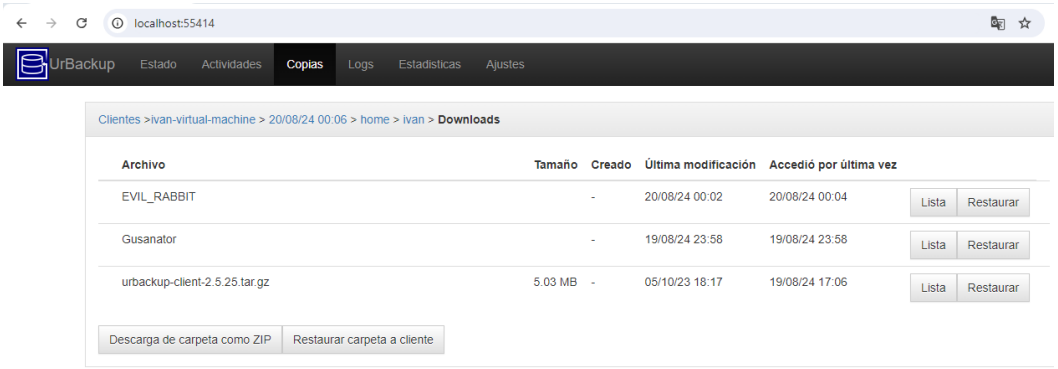


Ilustración 57 *Archivos de la carpeta "Downloads" de Ubuntu 22*

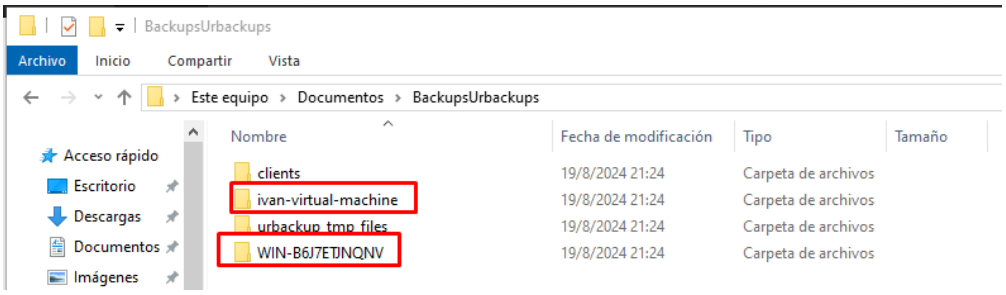


Ilustración 58 *Respaldos de las máquinas virtuales utilizando UrBackup Server*

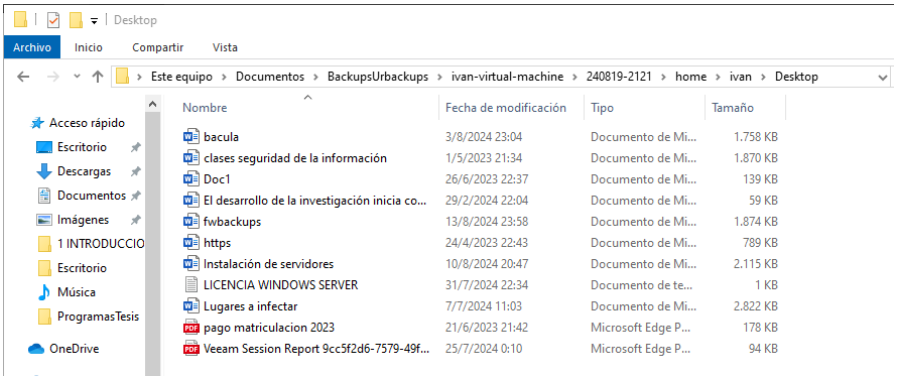


Ilustración 59 *Archivos de la carpeta de descargas de Ubuntu 22*

4.2.2.3 Resumen de resultados

Una vez finalizado el proceso de configuración de Urbackup Server en el servidor, al cliente e infecciones controladas en ambientes de Windows Server 2019 y Ubuntu 22, a continuación, se presenta un cuadro resumen de los resultados obtenidos:

Tabla 2 *Resumen resultados copias de seguridad con Urbackup Server en máquinas*

virtuales (Windows Server 2019 y Ubuntu 22)

N°	Características	Windows Server 2019	Ubuntu 22
1	Instalación de Urbackup Server	Usa instaladores .exe para ejecutar en Windows	Se realiza mediante comandos
2	Rendimiento en máquina virtual	Requiere de más recursos del sistema, CPU y RAM	Es más eficiente, consume menos CPU y memoria que Windows
3	Seguridad y control de infecciones	Mayor exposición de riesgo a programas maliciosos. Urbackup ayuda a mitigar riesgos con copias de seguridad	Menor exposición de riesgo a programas maliciosos. Software más seguro inherente al sistema operativo
4	Soporte de clientes	Buen soporte y fácil integración	Requiere configuración y mantenimiento adicional para usuarios no familiarizados
5	Simplicidad en Administración	Fácil administración para entornos viduales	Mayor complejidad ya que requiere el

			conocimiento de comandos
6	Impacto infecciones controladas	Mayor vulnerabilidad a infecciones si no se toma medidas, el mismo podría afectar al sistema y copias seguridad.	Menor riesgo de impacto, por la robustez frente ataques, igual requiere herramientas seguridad
7	Alertas de *malware*s en máquinas virtuales	No existió errores o Alertas de *malware* no detectadas	No existió errores o Alertas de *malware* no detectadas

NOTA: Es importante destacar que en la copia de seguridad en Ubuntu 22, el sistema operativo de Windows propio de la máquina física detectó la amenaza y lo comunicó al usuario con un mensaje en la parte inferior derecha que dice “Seguridad de Windows” *Ransomware* encontrado. *Ver ilustración 60 y 61.*

Historial de protección nos detecta la seguridad de Windows que encontró una amenaza y es Gonnacry.

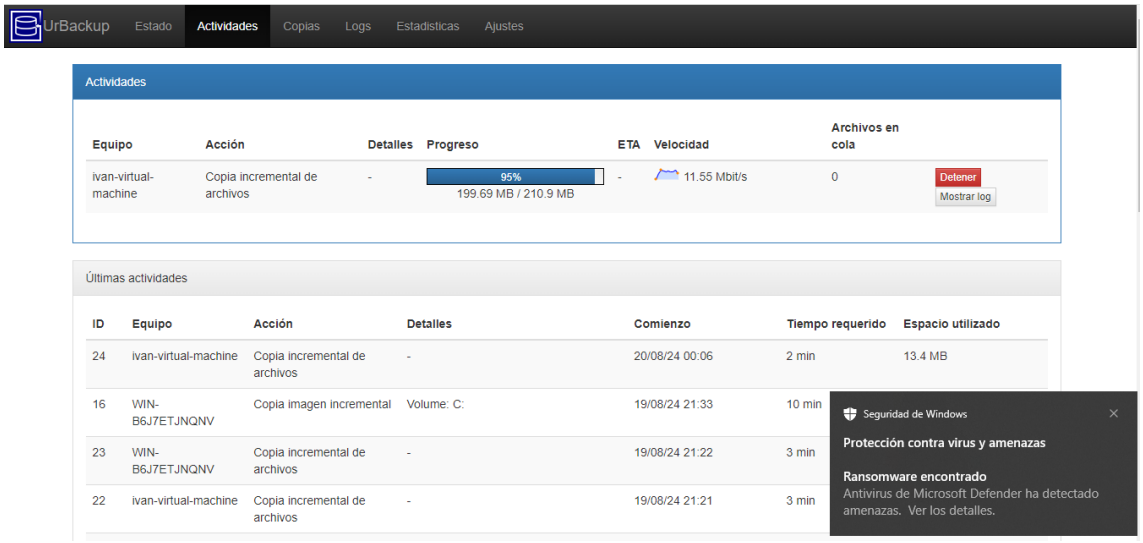


Ilustración 60 *Proceso de copia de seguridad UrBackup*

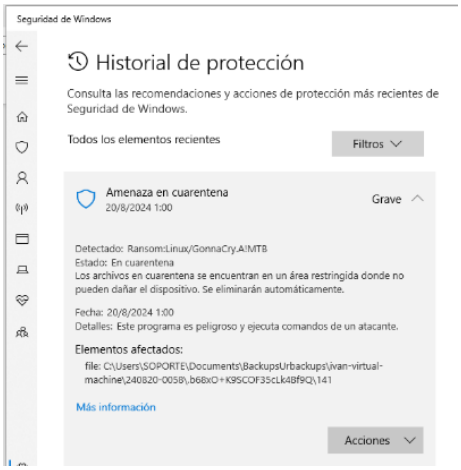


Ilustración 61 *Seguridad de Windows*

4.3 Análisis de entorno simulados

Se desarrolló un entorno simulado utilizando la herramienta comercial Veeam Backup & Replication y la herramienta de código abierto Urbackup con la finalidad de evaluar las características de cada uno de ellos, en la infección controlada con *malware* y copias de seguridad en las máquinas virtuales de Windows Server 2019 y Linux Ubuntu 22.

Al considerar la implementación de soluciones de respaldo, es importante evaluar las características y beneficios de diferentes herramientas. En este contexto, se

justifican el uso de Veeam Backup & Replication por ser uno de los principales en el cuadro de Gartner como una solución comercial, y UrBackup, como una opción de software libre.

Veeam Backup & Replication es reconocido por su robustez y eficiencia en la protección de datos en entornos virtualizados. Su capacidad para realizar copias de seguridad incrementales, replicación de máquinas virtuales y recuperación ante desastres es fundamental para empresas que requieren alta disponibilidad e inmediatez de la información. Además, Veeam Backup & Replication ofrece funcionalidades avanzadas como la verificación automática de backups y la recuperación instantánea, lo que minimiza el tiempo de inactividad. Su interfaz de fácil uso, comprensión y el soporte técnico especializado son ventajas que garantizan un respaldo confiable y una gestión simplificada, lo que resulta atractivo para organizaciones que buscan una solución integral y fácil de implementar.

Por otro lado, se encuentra, UrBackup como una alternativa viable en el ámbito del software libre o también conocido como *open source*. Su modelo permite a las organizaciones personalizar y adaptar la solución a sus necesidades específicas sin incurrir en costos de licencia. UrBackup ofrece características como la realización de copias de seguridad en tiempo real, restauración de archivos individuales y un enfoque eficiente en el uso del ancho de banda. En su plataforma web, existe una comunidad activa que facilita la resolución de problemas o inquietudes por parte del profesional, así mismo, mantiene disponibilidad de documentación. Esto lo convierte en una opción ideal para empresas pequeñas con limitaciones presupuestarias que aún requieren una solución de respaldo efectiva.

En resumen, la elección de Veeam Backup & Replication y UrBackup se fundamenta en la combinación de robustez, flexibilidad y costo-efectividad que

ofrecen. Mientras que Veeam satisface las necesidades de empresas que priorizan la confiabilidad y el soporte técnico, UrBackup se adapta a aquellos que buscan una opción libre y personalizable, garantizando así una estrategia de respaldo integral y eficaz.

Los resultados obtenidos se califican mediante la escala de Likert, una de las metodologías más utilizadas en encuestas de investigación, que mide el nivel de acuerdo sobre un tema (Silva, 2023). Por lo antes indicado, esta calificación se determinó en base a los criterios de expertos del tres profesionales del área de Tecnología de la Información de una empresa farmacéutica.

A continuación, se realiza una comparación entre Veeam Backup & Replication y UrBackup empleando la tabla de valoración de Likert. Para ello, es necesario definir una escala de evaluación estándar entre 1 al 5, en donde 1 es “muy deficiente” y 5 es “excelente” como se muestra en la siguiente tabla:

Tabla 3 *Tabla de valoración*

Tabla de valoración	
Muy Deficiente	1
Deficiente	2
Aceptable	3
Bueno	4
Excelente	5

A continuación, se presenta una tabla comparativa que valora diversas características, basándose en los resultados obtenidos en un entorno simulado de respaldo de máquinas virtuales, tanto comerciales como de código abierto, de acuerdo con esta escala:

Tabla 4 *Comparación de valoración*

N°	Característica	Veeam Backup & Replication	UrBackup
1	Facilidad descarga de software	2	4
2	Facilidad de instalación	4	5
3	Interfaz de usuario	3	4
4	Tipos de *backup* soportados	5	4
5	Análisis de *malware*	0	0
6	Copia de seguridad a nivel de archivos	5	4
7	Copia de seguridad a nivel de máquina virtual	5	2
8	Rendimiento y velocidad	5	4
9	Compresión de datos	5	3
10	Integración con aplicaciones	5	3
11	Soporte y comunidad	5	3
12	Costo	3	4
13	Actualizaciones y mantenimiento	5	4
14	Compatibilidad con sistemas operativos	5	5
	TOTAL	**57**	**49**

En base a la cuantificación de valoración de cada característica para los dos softwares estudiados, se identificó que Veeam Backup & Replication obtuvo una ponderación superior versus al software libre de Urbackup, de acuerdo con el siguiente detalle:

Tabla 5 *Resultados de variables de software comercial y open source en porcentaje y promedio*

	Veeam Backup & Replication	UrBackup
Total valoración	57	49
Porcentaje *	81.43%	70.00%
Promedio **	4.07	3.50

Consideraciones:

* El cálculo para el porcentaje se estableció en función del 100% aspiracional, para este caso la puntuación mayor corresponde a 70 puntos en valoración, la fórmula aplicada es la siguiente.

Porcentaje = (Total valoración / 70) × 100

** El cálculo para determinar el promedio, se estableció en función de la sumatoria total que arrojo cada herramienta y luego se dividió para el número total de variables, la fórmula aplicada es la siguiente.

Promedio = Total valoración / 14

Ilustración 62 *Promedio valoración resultados*

El gráfico de barras presentado se observa que en el eje horizontal representa la valoración de Likert, mientras que el eje vertical muestra el rango de promedio. Se identifica que el software comercial de Veeam Backup & Replication concentran una puntuación promedio total de 4.07 catalogado como "Bueno" en función a la valoración de Likert, mientras que, el software *open source* de Urbackup concentra una puntuación de 3.5 catalogado como "Aceptable" en función a la valoración de Likert. Por tal motivo, de la representación de los estos resultados, se determinó que

el software comercial de Veeam Backup & Replication presenta mejores características para la ejecución de copias de seguridad de máquinas virtuales completas.

Por otra parte, a continuación, se detalla cada uno de los hallazgos por cada característica evaluada:

Facilidad descarga de software: Veeam Backups & Replication se clasifica como una opción comercial con una puntuación de 2, debido a la dificultad que presenta la descarga de su versión de prueba y costo. UrBackup, al ser software libre, obtiene una puntuación de 4, lo que indica su facilidad de descarga y su mayor flexibilidad y accesibilidad para los usuarios.

Facilidad de instalación: UrBackup se destaca por su facilidad de instalación y configuración, mientras que Veeam Backups & Replication presenta una mayor complejidad debido a sus características avanzadas. En este aspecto, UrBackup supera a Veeam con una puntuación de 5 frente a 4, lo que indica que es más sencillo de implementar en diversos entornos.

Interfaz de usuario: Ambas soluciones cuentan con interfaces gráficas amigables que incluyen configuraciones predeterminadas para el uso del servidor y el cliente. Sin embargo, la complejidad de Veeam Backups & Replication, derivada de las herramientas avanzadas que ofrece, lo que influye en la comparación con la simplicidad de UrBackup. Por lo tanto, en términos de usabilidad, UrBackup recibe una puntuación de 4, ligeramente superior a la de Veeam Backups & Replication, que obtiene un 3, lo que sugiere que UrBackup puede facilitar una mejor experiencia para el usuario.

Tipos de backups soportados: Veeam Backups & Replication ofrece una extensa variedad de opciones de respaldo, incluyendo soporte para sistemas operativos como Windows y Linux, así como para entornos de virtualización como VMware y Hyper-V. También es compatible con almacenamiento en red (NAS), lo que la convierte en una solución robusta para organizaciones que manejan infraestructuras complejas. Se asigna una puntuación de 5 a Veeam Backups & Replication por su versatilidad en los tipos de respaldo que puede realizar, en comparación con UrBackup, que obtiene una puntuación de 4., lo que indica que Veeam Backups & Replication es de adaptabilidad a diferentes entornos y requisitos de respaldo, lo que la hace ideal para empresas que requieren una solución integral y flexible.

Análisis de malware: En la evaluación de Veeam Backups & Replication, software comercial, y UrBackup, software de código abierto se constató que ninguno de los respaldos generó alertas de infección en las máquinas virtuales. Ambos programas recibieron una puntuación de 0 en este aspecto, lo que sugiere que carecen de características significativas para la detección y mitigación de *malware*. Es importante considerar que esta falta de alertas en el software comercial podría estar relacionada con la versión de prueba de 30 días para el ejercicio realizado, en lugar de una versión completa de paga, la cual ofrece funcionalidades adicionales en términos de seguridad.

Copia de seguridad a nivel de archivos: Veeam Backups & Replication se asigna una puntuación de 5 debido que demuestra efectividad en la copia de seguridad a nivel de archivos y se destaca por ofrecer una mayor flexibilidad en sus opciones de configuración y recuperación, lo que indica su capacidad para adaptarse a diversas necesidades de los usuarios y facilitar procesos de restauración más personalizados. Por su parte, UrBackup también demuestra efectividad en la copia de seguridad a nivel,

sin embargo, se asigna una calificación de 4, ya que refleja su eficiencia en la restauración de datos, aunque con menos opciones de personalización en comparación con Veeam Backups & Replication. Esta diferencia en flexibilidad puede ser un factor determinante para organizaciones que requieren un enfoque más específico y versátil en sus estrategias de respaldo.

Copia de seguridad a nivel de máquina virtual: Veeam Backup & Replication se destaca en la gestión de copias de seguridad de máquinas virtuales, ofreciendo funcionalidades específicas para entornos virtualizados, como respaldos en tiempo real, recuperación instantánea y replicación, que aseguran la continuidad del negocio. En contraste, UrBackup no soporta copias de seguridad a nivel de máquina virtual, limitándose a respaldos de archivos y del sistema operativo, lo que reduce su eficacia en entornos virtualizados. Esto se refleja en las puntuaciones: Veeam obtiene un 5, mientras que UrBackup se queda en 2, indicando que Veeam Backup & Replication es la opción más adecuada para organizaciones que dependen de la virtualización.

Rendimiento y velocidad: Veeam Backup & Replication proporciona un rendimiento superior gracias a sus características avanzadas, logrando una puntuación de 5 que destaca su capacidad para realizar respaldos de manera rápida y eficiente. En comparación, UrBackup obtiene una puntuación de 4, lo que indica un buen rendimiento, pero inferior al de Veeam en términos de velocidad y eficacia en los procesos de respaldo.

Compresión de datos: En este aspecto, Veeam Backup & Replication también se posiciona como líder con una puntuación de 5, lo que indica su alta eficiencia en la reducción del tamaño de los backups a través de técnicas avanzadas de compresión como la compresión por bloques y en comparación con UrBackup obtiene una

puntuación de 3, lo que sugiere que su método de compresión es menos efectivo, utilizando compresión gzip, que, aunque es funcional pero no alcanza el mismo nivel de eficiencia que el de Veeam. Esto resalta la superioridad de Veeam Backup & Replication en términos de optimización del espacio de almacenamiento y rendimiento general.

Integración con aplicaciones: Veeam Backup & Replication y UrBackup ofrecen integración con aplicaciones empresariales críticas, aunque Veeam se destaca por su amplia compatibilidad con plataformas como Microsoft SQL Server, Microsoft Exchange y entornos de virtualización como VMware y Hyper-V. Esto permite a las organizaciones realizar copias de seguridad y recuperaciones específicas para datos críticos. En contraste, UrBackup tiene un enfoque más limitado, centrándose en respaldos de archivos y sistemas operativos, lo que puede ser una desventaja para empresas que requieren soluciones integrales. Veeam obtiene una puntuación de 5 en este aspecto, mientras que UrBackup se queda en 3, indicando que Veeam ofrece mejores opciones de integración con otros sistemas.

Soporte y comunidad: Veeam Backup & Replication ofrece un soporte comercial robusto, brindando asistencia técnica integral a sus usuarios. En contraste, UrBackup se basa principalmente en la comunidad y ofrece un soporte más básico. Veeam recibe una puntuación de 5 por su sólido soporte técnico, mientras que UrBackup obtiene un 3, lo que indica una comunidad de apoyo menos extensa y recursos limitados para los usuarios que requieren asistencia.

Costo: UrBackup se presenta como una opción gratuita, mientras que Veeam resulta costoso, dependiendo de las licencias y características seleccionadas. Esta comparación proporciona una visión general basada en la valoración de características clave de ambos softwares. La elección entre Veeam Backup & Replication y UrBackup

dependerá de las necesidades específicas del usuario, el presupuesto y el entorno de implementación. UrBackup se beneficia por ser un software libre de código abierto obteniendo una puntuación de 4 en comparación con 3 para Veeam Backup & Replication que corresponde a un software de pago, lo que puede ser un factor determinante para organizaciones con presupuestos limitados.

Actualizaciones y mantenimiento: Veeam Backup & Replication recibe una puntuación de 5, lo que indica su enfoque proactivo en el mantenimiento y la gestión de actualizaciones. La compañía ofrece actualizaciones regulares que incluyen nuevas funcionalidades, mejoras de seguridad y optimizaciones de rendimiento, asegurando que los usuarios se beneficien de las últimas innovaciones y se mantengan protegidos contra vulnerabilidades, así mismo, Veeam Backup & Replication proporciona soporte técnico continuo y recursos de formación para ayudar a los usuarios a implementar eficientemente estas actualizaciones.

En comparación, UrBackup obtiene una puntuación de 4, lo que refleja un enfoque sólido en el mantenimiento, aunque menos intensivo en términos de frecuencia de actualizaciones. UrBackup también ofrece actualizaciones regulares, pero su enfoque puede ser más reactivo, centrado en la corrección de errores y en la implementación de nuevas características basadas en las necesidades de la comunidad. A pesar de esto, UrBackup sigue siendo una opción confiable para usuarios que buscan un mantenimiento efectivo, especialmente en entornos más pequeños donde los recursos son limitados. La diferencia en las puntuaciones de mantenimiento y actualizaciones puede influir en la decisión de las organizaciones, dependiendo de su necesidad de un soporte más robusto y continuo.

Compatibilidad con sistemas operativos: Finalmente, en términos de compatibilidad con los sistemas operativos, Veeam Backup & Replication destaca con

una puntuación de 5, lo que refleja su amplia capacidad para integrarse con diversas plataformas, incluyendo Windows, Linux y entornos de virtualización como VMware y Hyper-V. Esto permite a Veeam Backup & Replication ser una solución versátil para empresas que operan en entornos mixtos, asegurando una protección eficaz de datos en diferentes sistemas.

Así mismo, UrBackup obtiene una puntuación máxima de 5, debido a su buena compatibilidad, con sistemas operativos Windows y Linux, que se centra en la protección de archivos y sistemas operativos en estos entornos.

En base a la metodología aplicada de valoración de Likert, Veeam Backup & Replication se posiciona como una solución más robusta y completa, ideal para entornos empresariales que requieren alta disponibilidad y un sólido soporte técnico, con una puntuación global de 57, mientras que, UrBackup representa una alternativa valiosa para quienes buscan un software libre, flexible y personalizable, especialmente en situaciones donde el presupuesto es una preocupación primordial, con una puntuación global de 49.

Esta diferencia subraya que, aunque UrBackup es más accesible al ser un software libre para una empresa nueva con pocos recursos y que inicia en sus operaciones, mientras que, Veeam Backup & Replication al ser una herramienta comercial de pago proporciona una solución más integral y versátil, especialmente adecuada para infraestructuras empresariales más sólidas.

4.4 Desarrollo de un plan de datos enfocados a la seguridad informática.

En función a lo descrito en los puntos anteriores, a continuación, se detalla un plan de respaldo de datos de máquinas virtuales (VM) en una empresa farmacéutica utilizando la herramienta Veeam Backup & Replication por la puntuación máxima

alcanzada en comparación con la herramienta *open source* Urbackup, además, de ser uno de los principales en el cuadrante superior derecho (líder) del cuadro Gartner y garantizar que cumpla con las necesidades de seguridad de la información.

Introducción

El plan de respaldo tiene como objetivo asegurar la disponibilidad, integridad y confidencialidad de los datos en un entorno de máquinas virtuales (VM) de una empresa farmacéutica mediante el uso del software comercial de Veeam Backup & Replication al ser una solución robusta y escalable que garantizará la protección de la información.

1. Objetivo del Plan:

El objetivo principal del plan es implementar y gestionar un sistema de copias de seguridad utilizando **Veeam Backup & Replication** para garantizar la disponibilidad, seguridad y recuperación de datos críticos en una empresa farmacéutica.

Liderazgo y compromiso

- La alta dirección debe demostrar su compromiso con la seguridad de la información y proporcionar los recursos necesarios para implementar este plan.
- Establecer como prioridad dentro del departamento de Tecnologías de la Información la gestión de seguridad de los datos de la empresa farmacéutica.

2. Alcance del Plan:

- **Descripción del Plan:**
    - Implementar una solución integral de copias de seguridad usando Veeam Backup & Replication, cubriendo desde la instalación, configuración y

monitoreo hasta la automatización de copias de seguridad y recuperación ante desastres.

- **Áreas que se cubrirán:**
    - Backup de servidores físicos y virtuales.
    - Monitoreo y generación de reportes.
    - Recuperación ante desastres.

3. Metodología de Trabajo:

Fase 0: Reunión con el departamento de finanzas para compra de licencias

El objetivo de esta fase es asegurar que se obtengan la licencia para la implementación del plan.

La duración estimada para esta fase será de 1 semana.

- **Tareas específicas:**
    - Realizar una reunión con el departamento financiero para discutir presupuesto y su aprobación.
    - Cotización y negociación con Veeam Backup & Replication o proveedores autorizados.
    - Realizar el proceso de compra y adquisición de la licencia.
    - Planificar con el proveedor la entrega e instalación de las licencias.
- **Responsables:**
    - Líder de Proyecto TI
    - Finanzas

- **Fecha de inicio:** 06/01/2025
- **Fecha de finalización:** 10/01/2025

Fase 1: Análisis y planificación

El objetivo de esta fase es evaluar las necesidades de la copia de seguridad aplicada a la empresa farmacéutica y preparar el plan de implementación de Veeam Backup & Replication.

La duración estimada para esta fase será de 1 semana.

- **Tareas:**
    - Evaluar la infraestructura tecnológica actual.
    - Identificar los datos críticos a proteger.
    - Definir las políticas de respaldo (frecuencia, tipo de copia).
    - Analizar las máquinas virtuales y físicas previo y posterior a la ejecución de las copias de seguridad.
    - Establecer criterios de recuperación ante desastres.
    - Planificar el uso de recursos (almacenamiento en nube y ancho de banda).
- **Responsables:**
    - Líder de Proyecto TI
    - Equipo de TI
    - Equipo de Seguridad Informática
- **Fecha de inicio:** 13/01/2025
- **Fecha de finalización:** 17/01/2025

Fase 2: Instalación y configuración de Veeam Backup & Replication

El objetivo de esta fase es instalar Veeam Backup & Replication y configurarlo de acuerdo con las políticas definidas.

La duración estimada para esta fase es de 2 semanas

- **Tareas:**
    - Instalar el software Veeam Backup & Replication en el servidor designado como Administrador e instalación del cliente en los servidores físicos y virtuales con Windows Server 2019.
    - Configurar las políticas de *backup*: copias completas, incrementales, diferenciales de forma automática.
    - Establecer las tareas de recuperación ante desastres.
    - Configurar almacenamiento y nube para *backups*.
    - Integrar la solución con sistemas de monitoreo existentes.
- **Responsables:**
    - Líder del Proyecto TI
    - Equipo de TI
    - Equipo de Seguridad Informática
- **Fecha de inicio:** 20/01/2025
- **Fecha de finalización:** 31/01/2025

Fase 3: Pruebas y validación

El objetivo es validar que el sistema de copias de seguridad funcione correctamente y que

los datos sean recuperables.

La duración estimada en esta fase es de 1 semana.

- **Tareas:**
    - Realizar pruebas de respaldo (completos e incrementales).
    - Probar la recuperación de datos en diferentes escenarios.
    - Verificar la consistencia de los *backups*.
    - Realizar pruebas de restauración desde almacenamiento físico y desde la nube.
- **Responsables:**
    - Líder proyecto TI
    - Equipo TI
    - Equipo Seguridad Informática
- **Fecha de inicio:** 03/02/2025
- **Fecha de finalización:** 07/02/2025

Fase 4: Entrenamiento y documentación

El objetivo es capacitar al personal de TI y Seguridad Informática en el uso de la herramienta Veeam Backup & Replication, así como crear documentación operativa.

La duración estimada en esta fase es de 1 semana

- **Tareas:**
    - Capacitación del personal para la gestión y restauración de *backups*.

    - Crear manuales de procedimientos para la gestión en Veeam Backup & Replication.
    - Entrenar al equipo de soporte para la gestión de incidentes relacionados con *backups*.
    - Elaboración de planes de contingencia y recuperación ante desastres

- **Responsables:**
    - Líder de Proyecto
    - Equipo de TI
    - Equipo de Seguridad Informática

- **Fecha de inicio:** 10/02/2025
- **Fecha de finalización:** 14/02/2025

Fase 5: Implementación final y monitoreo

El objetivo es implementar el sistema de copias de seguridad de forma definitiva y configurar el monitoreo para la operación continua automática.
La duración estimada en esta fase es de 1 semana.

- **Tareas:**
    - Configuración de alertas y notificaciones de fallos en *backups*.
    - Implementación de informes automáticos de estado de *backups*.
    - Integración con otras herramientas de monitoreo existentes.
    - Aseguramiento de políticas de retención y eliminación de *backups*.

- **Responsables:**

- Líder del Proyecto TI
- Equipo de TI

- **Fecha de inicio:** 17/02/2025
- **Fecha de finalización:** 21/02/2025 (a lo posterior se continuará el monitoreo)

4. Flujograma de las Actividades Iniciales

A continuación, se muestra el flujograma de procesos que representas las actividades principales para el plan de desarrollo de datos enfocados a la seguridad informática y copias de seguridad mediante el uso de la herramienta comercial de Veem Backup & Replication.

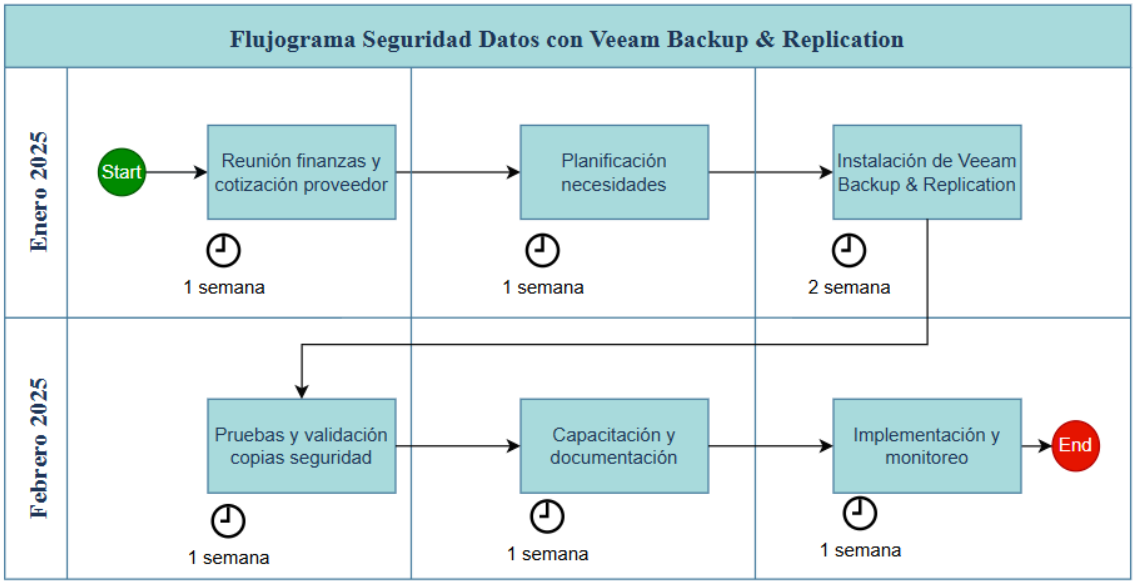


Ilustración 63 *Flujograma Seguridad con Veeam Backup & Replication.*

5. Cuadro de Gantt:

SEGURIDAD DATOS CON VEEAM BACKUP & REPLICATION Diagrama de Gannt:	ENERO 2025 Semana 1	2	3	4	FEBRERO 2025 Semana 1	2	3	4	RESPONSABLES
Reunión finanzas y cotización proveedor									• Líder proyecto TI • Finanzas
Planificación necesidades									• Líder proyecto TI • Equipo TI • Equipo Seguridad Informática
Instalación de Veeam Backup & Replication									• Líder proyecto TI • Equipo TI • Equipo Seguridad Informática
Pruebas y validación copias seguridad									• Líder proyecto TI • Equipo TI • Equipo Seguridad Informática
Capacitación y documentación									• Líder proyecto TI • Equipo TI • Equipo Seguridad Informática
Implementación y monitoreo									• Líder proyecto TI • Equipo TI

Ilustración 64 *Cuadro de Gantt*

6. Temarios para el entrenamiento / capacitación.

1. **Introducción a Veeam Backup & Replication:**
    - ¿Qué es Veeam?
    - Ventajas de usar Veeam en la infraestructura.
    - Componentes y arquitectura de Veeam.
2. **Configuración de Políticas de Backup:**
    - Tipos de backup (Completo, Incremental, Diferencial).
    - Estrategias de retención de datos.
3. **Recuperación ante Desastres:**
    - Cómo restaurar sistemas completos.
    - Recuperación granular de archivos.
4. **Monitoreo y Mantenimiento de backups:**
    - Configuración de alertas y notificaciones.

- Informe de estado de *backups*.
- Solución de problemas comunes.

5. **Documentación y Buenas Prácticas:**
   - Gestión de incidencias y copias de seguridad.
   - Planes de recuperación ante desastres.

7. Recursos Necesarios:

- **Hardware:**
  - Un servidor de almacenamiento físico y uno en la nube.
- **Software:**
  - Veeam Backup & Replication.
  - Windows Server 2019 en adelante.
- **Recurso Humano:**
  - Ingenieros de sistemas.
  - Ingenieros en seguridad informática.
  - Equipo de finanzas.
  - Proveedor.

8. Plan de Monitoreo Post-Implementación:

Después de la implementación, se recomienda realizar un monitoreo continuo de las copias de seguridad. Esto puede incluir:

- Revisiones semanales de logs de copias de seguridad.

- Evaluación mensual de la integridad de los backups.
- Actualización periódica de las políticas de respaldo en función de cambios en la infraestructura.
- Análisis de las copias de seguridad con antivirus a fin de identificar posibles infecciones.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Tras realizar un estudio de las herramientas comerciales y *open source* para la realización de respaldos de máquinas virtuales, se concluye que ambas opciones tienen sus ventajas y desventajas, existen muchas herramientas para grandes, medianas y pequeñas empresas, especialmente cuando se consideran aspectos de seguridad. Las herramientas comerciales ofrecen mecanismos de cifrado más avanzados y una integración más estrecha con sistemas de detección de *malware*, lo cual proporciona una mayor seguridad en entornos corporativos donde la protección de datos sensibles es crítica. Las herramientas *open source*, aunque más flexibles y económicas, pueden requerir personalización adicional para alcanzar el mismo nivel de seguridad, lo que podría implicar mayores inversiones en tiempo y recursos de configuración y mantenimiento.

- Al realizar un análisis en un entorno simulado con ambas categorías de herramientas, se ha demostrado que las soluciones comerciales tienen a ser más fáciles de implementar, con una mayor disponibilidad de soporte técnico y manuales disponibles para la instalación y configuración. Las herramientas *open source*, si bien ofrecen un alto grado de personalización y flexibilidad, pueden ser más complicadas de configurar y administrar, por falta de manuales que complica la utilización de código abierto. En cuanto a las copias de seguridad en las máquinas virtuales de Windows Server 2019 y Linux Ubuntu 22, en ambos casos, ninguna de las dos herramientas de prueba utilizadas detectó con mensajes de alerta o error relacionados a las infecciones controladas.

- En base al desarrollo de un plan de respaldo utilizando Veeam Backup & Replication en una empresa farmacéutica se garantiza la implementación de un plan de respaldo con Veeam Backup & Replication no solo garantiza la protección de las máquinas virtuales, sino que también respalda la continuidad operativa en situaciones de desastre. Con políticas claras de frecuencia de respaldo, replicación de datos, cifrado de la información y pruebas regulares, la organización puede cumplir con los requisitos de seguridad de la información, promoviendo una cultura de resiliencia organizacional, que es un principio clave en ISO 27001.

5.2 Recomendaciones

- Se recomienda adoptar Veeam Backup & Replication con licencia de pago, especialmente para entornos empresariales donde la seguridad de la información y el cumplimiento de normativas como ISO 27001 son prioritarios. Esta herramienta ofrece técnicas avanzadas de cifrado, que protegen la confidencialidad de los datos frente a ciber amenazas, además de garantizar la integridad de la información a través de una arquitectura robusta de respaldo y recuperación ante desastres. Esto no solo asegura la continuidad del negocio, sino también el cumplimiento con las mejores prácticas de seguridad informática, como la protección contra *malware* y la gestión de riesgos.

- Es fundamental Optar por herramientas de respaldo con licencia no solo proporciona acceso a todas las funcionalidades y actualizaciones de seguridad más recientes, sino que también asegura la disponibilidad de soporte técnico especializado. Esto facilita la implementación, configuración y resolución de posibles incidentes. Además, el uso de software licenciado está alineado con

las mejores prácticas de seguridad informática, que promueven la protección continua de datos frente a vulnerabilidades emergentes. Desde el punto de vista de ISO 27001, el uso de herramientas licenciadas contribuye al cumplimiento de la normativa en términos de gestión de activos de TI y mantenimiento de una infraestructura de seguridad confiable.

- Para garantizar una mayor protección de los datos, es recomendable realizar un análisis exhaustivo con antivirus actualizado en los archivos comprimidos antes y después de realizar los respaldos con herramientas como Veeam Backup & Replication y UrBackup. Esto ayudará a identificar posibles amenazas y a prevenir que se propaguen en el sistema, cumpliendo con las mejores prácticas en gestión de riesgos y seguridad de la información, como lo establece ISO 27001, que requiere que los procesos de respaldo estén alineados con las políticas de protección contra *malware* y otras amenazas cibernéticas.

- Al incorporar estas recomendaciones, las empresas pueden garantizar no solo la protección adecuada de sus datos, sino también la alineación con las mejores prácticas en seguridad informática y el cumplimiento de normativas internacionales, lo que refuerza su resiliencia ante incidentes de seguridad.

Referencias

Abalmasov, A. (s.f.). *securitystronghold.* securitystronghold: https://www.securitystronghold.com/es/gates/rahack.html#Technical

Acronis. (2023). *Historia de Acronis*. Historia de Acronis: https://history.acronis.com/#history

Alexey Podrezov, D. F. (s.f.). *kaspersky threats* . kaspersky threats : https://threats.kaspersky.com/mx/threat/Trojan.Win32.IconDance/

Amanda. (25 de Agosto de 2023). *amanda*. amanda: https://www.amanda.org/

Amanda Comunity. (2023). *Zmanda*. Zmanda: https://www.zmanda.com/amanda-community/

Ambit. (7 de Noviembre de 2023). *Ambit*. Ambit: https://www.ambit-bst.com/blog/c%C3%B3mo-las-alertas-y-la-seguridad-est%C3%A1n-cambiando-la-industria-farmac%C3%A9utica

Arcys. (03 de Mayo de 2019). *Respaldo de información*. Respaldo de información: https://www.arsys.es/blog/riesgos-no-hacer-backup

Bacula. (2025). *Bacula*. Bacula: https://www.baculasystems.com/es/copia-de-seguridad-de-nutanix-solucion-de-copia-de-seguridad-de-nutanix/

Báez, J. (28 de Septiembre de 2021). *welivesecurity*. welivesecurity.: https://www.welivesecurity.com/la-es/2021/09/28/que-es-ataque-xss-cross-site-scripting/

Balarezo, R. (Junio de 2020). *Consejo nacional para la igualdad de género*. Consejo nacional para la igualdad de género: https://www.igualdadgenero.gob.ec/wp-content/uploads/downloads/2021/05/POLITICA-DE-RESGUARDO-Y-RECUPERACI%C3%93N-DE-LA-INFORMACI%C3%93N.pdf

Buenning, M. (15 de Noviembre de 2024). *Ninjaone*. Ninjaone:

https://www.ninjaone.com/es/blog/como-prevenir-desastres-con-una-copia-de-seguridad-anti-ransomware/

Burdova, C. (22 de Julio de 2022). *Avast*. Avast: https://www.avast.com/es-es/c-rootkit

Caraguay, G. D. (18 de Abil de 2017). *Univerdidad Nacional de Loja*. Univerdidad Nacional de Loja: https://dspace.unl.edu.ec/jspui/handle/123456789/19097

Chango, W. (2015). *PUCE*. PUCE: https://repositorio.puce.edu.ec/server/api/core/bitstreams/5cef53d4-59ee-4241-9336-0d4fd4f292ed/content

Chaudhry, N. (27 de Junio de 2024). *maketecheasier*. maketecheasier: https://www.maketecheasier.com/use-urbackup-for-efficient-backups-linux/

checkpoint. (2022). *Agent Tesla Malware.* Agent Tesla Malware: https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-malware/agent-tesla-malware/#:~:text=El%20Agente%20Tesla%20es%20una,computadoras%20infectadas%20de%20una%20organizaci%C3%B3n.

Damián. (31 de Agosto de 2024). *Ubunlog.* Ubunlog: https://ubunlog.com/urbackup-sistema-de-copia-de-seguridad-cliente-servidor/

digital, N. (18 de Octubre de 2022). *Fundación telefonica*. Fundación telefonica: https://www.fundaciontelefonica.com/noticias/ciberseguridad-4-tipos-de-ataques-informaticos/

ESET. (18 de Septiembre de 2018). *welivesecurity.* welivesecurity: https://www.welivesecurity.com/la-es/2018/09/21/danabot-sigiloso-troyano-bancario-afecta-europa/

ExeDB. (18 de Marzo de 2014). *Una Guía Completa para Archivos ana.exe.* Una Guía Completa para Archivos ana.exe: https://www.exedb.com/sp/ana---477409-

u0s9syftrq8qwwm.asp

Fernández, E. C. (19 de Septiembre de 2022). *TokioSchool*. TokioSchool: https://www.tokioschool.com/noticias/tipos-ataques-informaticos/

Forti, F. G. (20 de Diciembre de 2017). *itsitio*. itsitio: https://www.itsitio.com/soluciones/seis-consejos-respaldo-la-restauracion-maquinas-virtuales/

Gómez, R. M. (2017 de Diciembre de 2017). *itmastersmag*. itmastersmag: https://www.itmastersmag.com/noticias-analisis/consejos-para-el-respaldo-y-la-restauracion-de-maquinas-virtuales/

Group, L. E. (1 de Abril de 2015). *Logo ESG Innova Group*. Logo ESG Innova Group: https://www.pmg-ssi.com/2015/04/isoiec-17799-politica-de-seguridad/

H. P. (2018). *Metodología de la investigación.* Mc Graw Hill educación.

IONOS. (29 de Octubre de 2021). *Digital Guide*. Digital Guide: https://www.ionos.mx/digitalguide/servidores/seguridad/regla-backup-3-2-1/

ISO/IEC17799. (15 de Junio de 2005). *mmujica*. mmujica: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

IT, I. (8 de Septiembre de 2022). *International IT*. International IT: https://www.internationalit.com/post/cu%C3%A1les-son-los-principales-tipos-de-cifrado-para-la-transferencia-segura-de-archivos?lang=es

Jaimovich, D. (25 de Octubre de 2022). *Invgate*. Invgate: https://blog.invgate.com/es/tipos-de-ciberataque

Jaimovich, D. (4 de Septiembre de 2024). *Invgate*. Invgate: https://blog.invgate.com/es/tipos-de-ciberataque

Kaspersky. (2021). *Ataque cero*. Ataque cero: https://latam.kaspersky.com/resource-center/definitions/zero-day-

exploit?srsltid=AfmBOoqudRQl_YA1zzZbNcZc2MHge3ZGiFqwYiSmyoAjv-EpMUA_5JOd

Kaspersky. (2022). *ransomware*. ransomware: https://latam.kaspersky.com/resource-center/threats/ransomware?srsltid=AfmBOorrN4RbXzgjknMGBovB_pYEtLZGsHL9Mf9N0S3cwtRCzAJAdKHr

Leal, R. (12 de 12 de 2022). *Advisera*. Advisera: https://advisera.com/27001academy/es/que-es-iso-27001/

Luz, S. d. (20 de junio de 2019). *Redeszone*. Redeszone: https://www.redeszone.net/2019/06/20/nakivo-backup-replication/

Meskauskas, T. (1 de Mayo de 2019). *Virus AZORult.* Virus AZORult: https://www.pcrisk.es/guias-de-desinfeccion/8840-azorult-virus

Meskauskas, T. (11 de Enero de 2024). *pcrisk.* pcrisk: https://www.pcrisk.es/guias-de-desinfeccion/12410-win32-floxif-malware

Microsoft. (08 de Noviembre de 2023). *Copia de seguridad de máquinas virtuales de Hyper-V*. Copia de seguridad de máquinas virtuales de Hyper-V: https://learn.microsoft.com/es-es/system-center/dpm/back-up-hyper-v-virtual-machines?view=sc-dpm-2022

Miguel, R. d. (17 de Enero de 2023). *Revistabyte*. Revistabyte: https://revistabyte.es/comparativa/herramientas-de-contingencia/

Morrison, R. (16 de Noviembre de 2024). *Bacula Systems*. Bacula Systems: https://www.baculasystems.com/es/el-blog/copia-de-seguridad-backup-vmware/

Nakivo. (2022). *Nakivo*. Nakivo: https://www.nakivo.com/res/files/nakivo-backup-replication-solution-brief_ES.pdf

NilsUllmann. (16 de Julio de 2021). *Seguridad TI en la Industria Farmacéutica*. Seguridad TI en la Industria Farmacéutica: https://www.zscaler.es/blogs/product-

insights/it-security-pharmaceutical-industry

Pagnotta, S. (29 de Mayo de 2017). *welivesecurity*. welivesecurity: https://www.welivesecurity.com/la-es/2017/05/29/diferencias-wannacryptor-eternalrocks/

Pilco, E. H. (2012). *Repositorio de la UTN*. Repositorio de la UTN: http://repositorio.utn.edu.ec/bitstream/123456789/1722/3/04%20ISC%20244%20ART%C3%8DCULO%20CIENT%C3%8DFICO.pdf

POINT, C. (2023). *ciberataque*. ciberataque: https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-cyber-attack/

Públicos, D. N. (9 de Noviembre de 2021). *Registros Públicos*. Registros Públicos: https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/#:~:text=En%20Ecuador%20el%20art%C3%ADculo%2066,as%C3%AD%20como%20su%20correspondiente%20protecci%C3%B3n.

Rodríguez, G. (16 de 06 de 2020). *Noticias de la industria farmacéutica*. Noticias de la industria farmacéutica: https://www.farmaindustrial.com/articulos-online/la-importancia-de-la-ciberseguridad-en-el-sector-farmaceutico-GBS2h

SEMPLADES. (Septiembre de 2021). *Planificación*. Planificación: https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf

Silva, D. d. (18 de Septiembre de 2023). *zendesk*. zendesk: https://www.zendesk.com.mx/blog/que-es-escala-de-likert/

solution, V. y. (01 de 03 de 2019). *vsquarebackup*. vsquarebackup: https://www.vsquarebackup.com/blog/timeline?tag=update

Solutions, G. (22 de Septiembre de 2023). *GlobalSuite Solutions*. GlobalSuite Solutions:

https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/?gad_source=1&gclid=EAIaIQobChMIp6fXpru9iAMVxYFaBR0T4BfWEAAYASAAEgISm_D_BwE

SPIDER, S. (31 de 05 de 2018). *Malpedia*. Malpedia: https://malpedia.caad.fkie.fraunhofer.de/details/win.danabot

Tecnozero. (2023). *Tecnozero*. Tecnozero: https://www.tecnozero.com/blog/cuadrante-magico-de-gartner-en-soluciones-de-software-de-backup-y-recuperacion-empresarial-2023/

Thakur, A. (2020). *GitHub.* GitHub: https://github.com/compilepeace/EVIL_RABBIT

Urbackup. (24 de Marzo de 2024). *Urbackup*. Urbackup: https://www.urbackup.org/

UTN. (2023). *Vicerrectorado de investigación*. Vicerrectorado de investigación: https://www.utn.edu.ec/direccion/#1678470247794-cf300289-335c

Veeam. (1 de Septiembre de 2023). *La importancia*. La importancia: https://www.veeam.com/blog/es/verify-backup-recoverability.html

veeam. (s.f.). *veeam*. veeam: https://www.veeam.com/data-protection-virtual-machine.html?st=adwordspaidsearch&utm_source=google&utm_medium=cpc&utm_campaign=01P-SPT_LATAM_ES_NOLA_Paid-Search_Trial_Branded-Virtual&utm_content=cid|20903355002_ntw|g_adgr|162943156768_creative|686184525751

Vinay Pamnani, K. N. (26 de Marzo de 2024). *Configuración del espacio aislado de Windows.* Configuración del espacio aislado de Windows: https://learn.microsoft.com/es-es/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-configure-using-wsb-file

Vinchin. (02 de 12 de 2024). *vinchin backup & recovery*. vinchin backup & recovery:

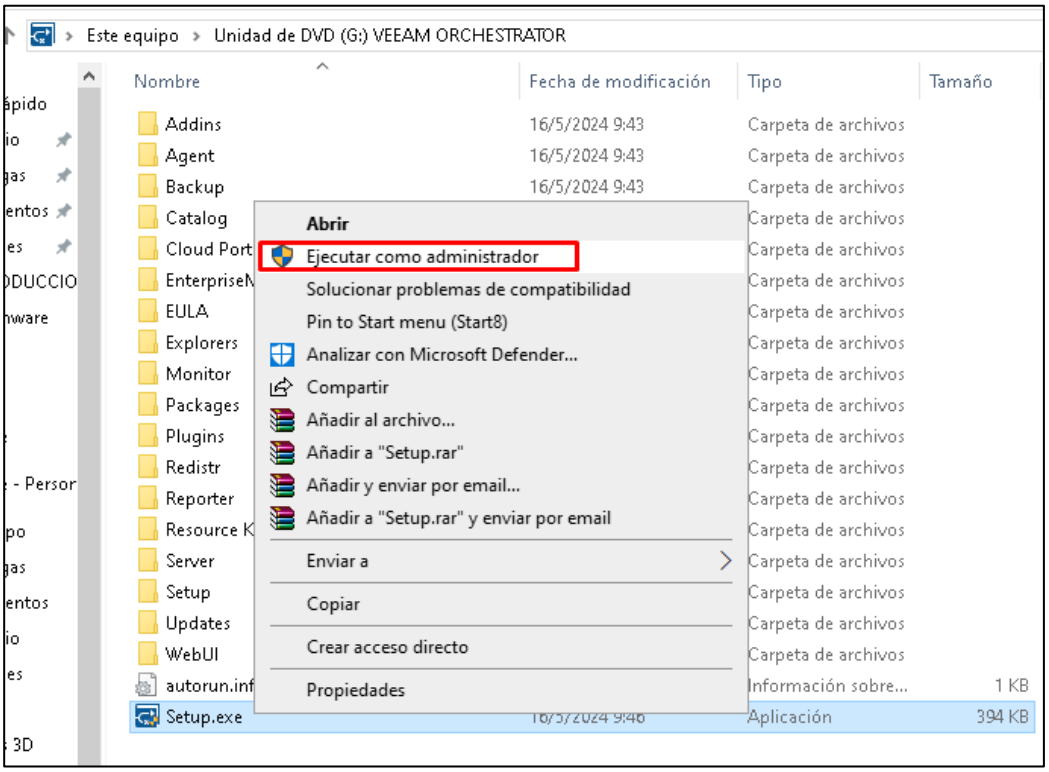
https://www.vinchin.com/vinchin-software-documentation-downloads.html

Vinchin. (s.f.). *Vinchin*. Vinchin: https://www.vinchin.com/es/?utm_source=google&utm_medium=cpc&utm_campaign=20709736464&utm_term=&utm_content=&utm_keyword=&utm_position=&gad_source=1&gclid=CjwKCAiA0bWvBhBjEiwAtEsoW1O_aTW0GU4CkX5NM7EoqwUJnWqpbl9d6SOnu6uLcuE2_EvyFgFovBoC31wQAvD_BwE

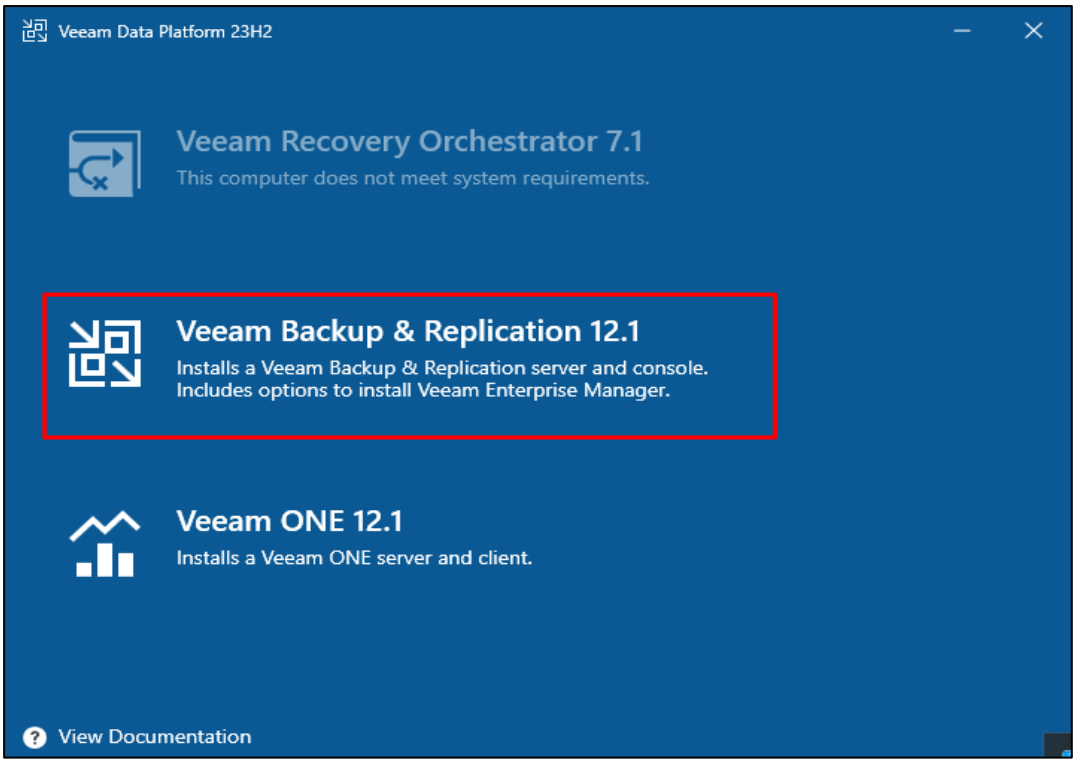
VMware. (22 de Marzo de 2023). *vSphere Replication*. vSphere Replication: https://docs.vmware.com/es/vSphere-Replication/8.7/com.vmware.vsphere.replication-admin.doc/GUID-C987AD18-7C2D-4FA6-B6E4-6B0DDA915A7A.html

Yunga, J. S. (Marzo de 2019). *Universidad Israel*. Universidad Israel: https://repositorio.uisrael.edu.ec/handle/47000/2057

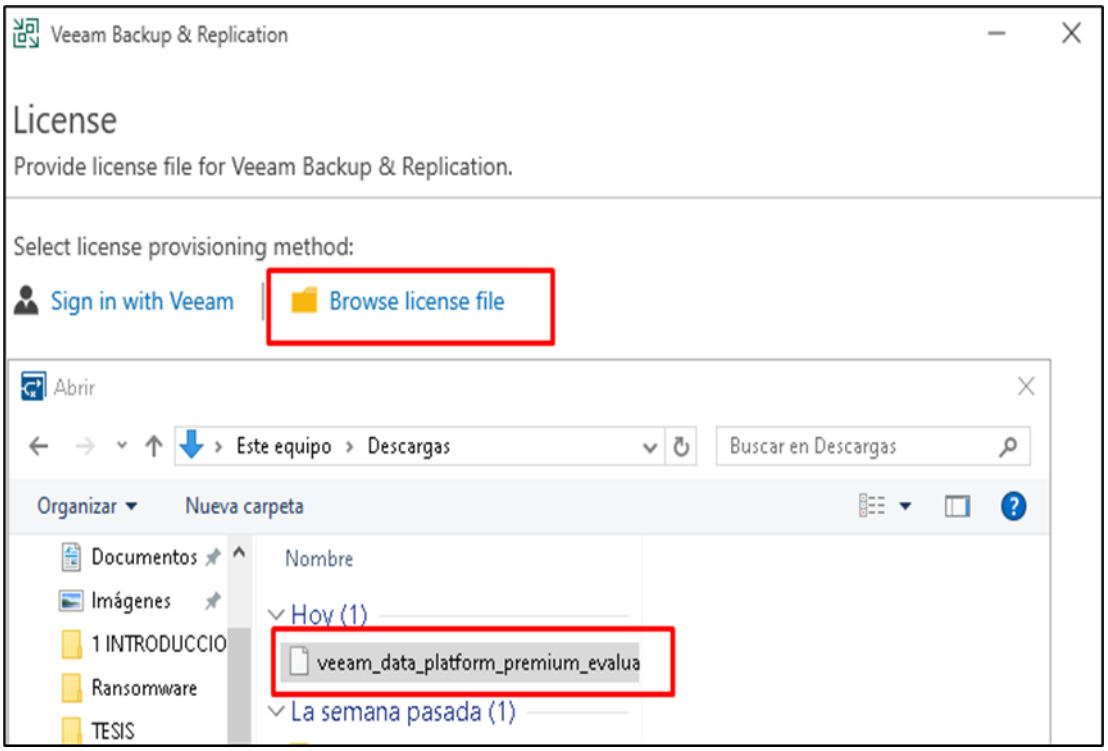
ANEXOS



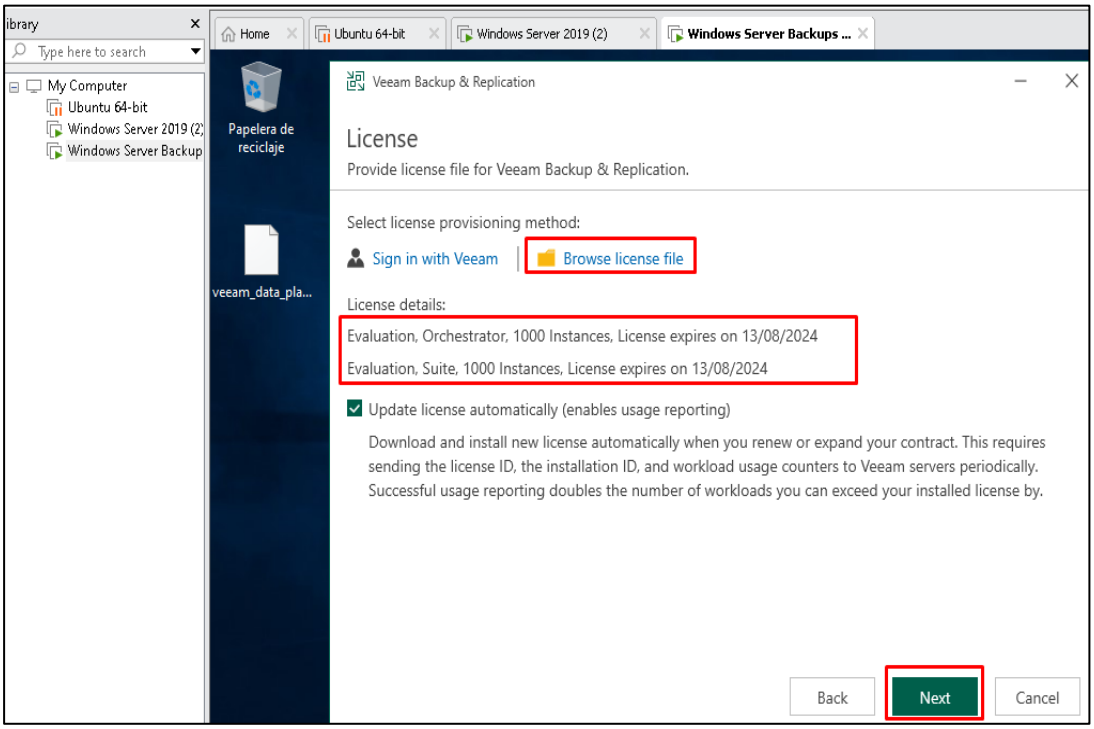
Anexo 1 Ejecución como administrador Veeam Backups Replication



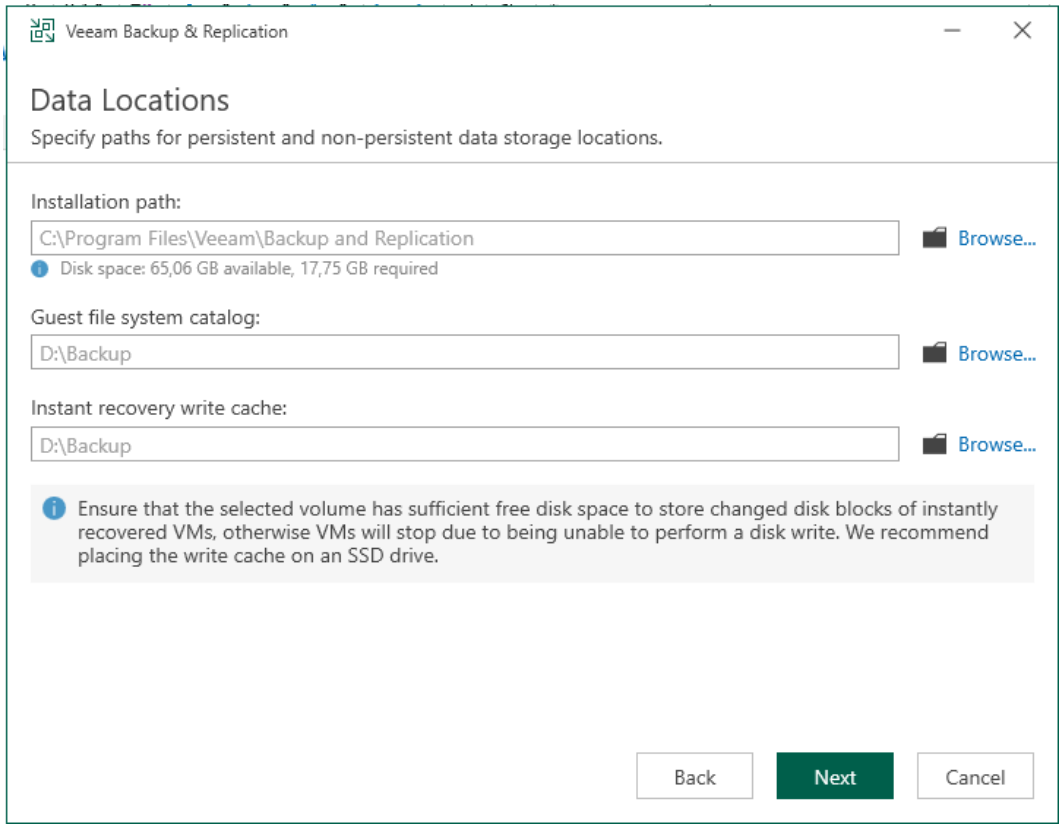
Anexo 2 Veeam Backup & Replication 12.1



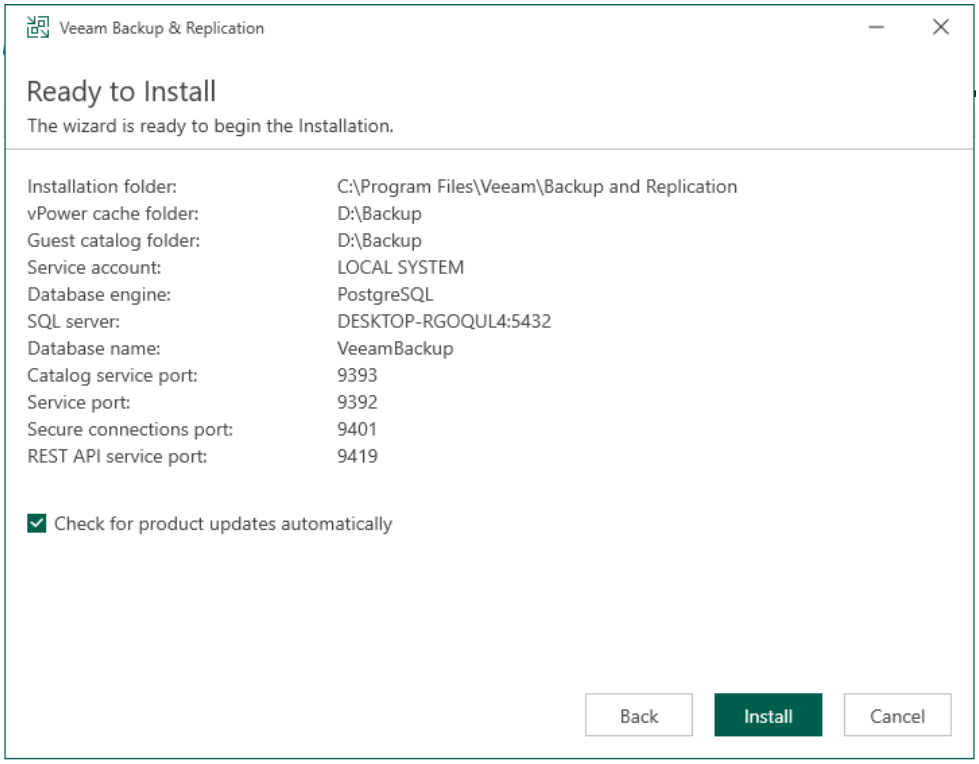
Anexo 3 Licencia de Prueba Veeam Backup & Replication



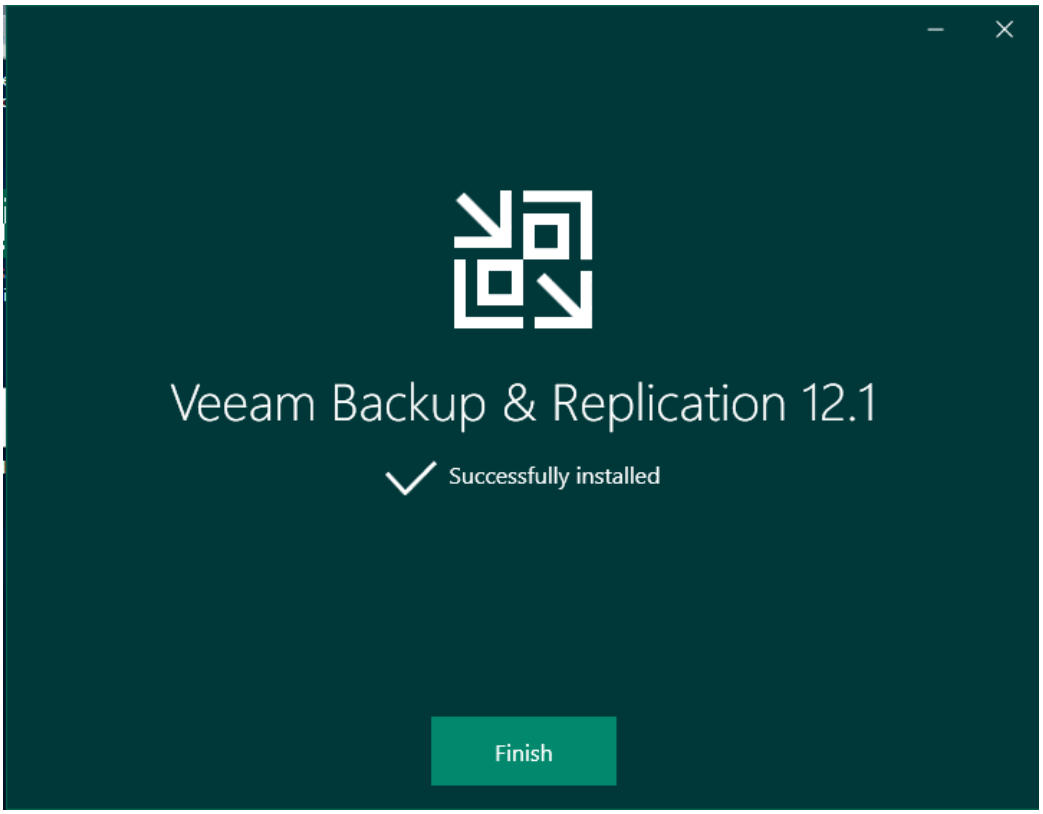
Anexo 4 Fecha de caducidad de la licencia de prueba



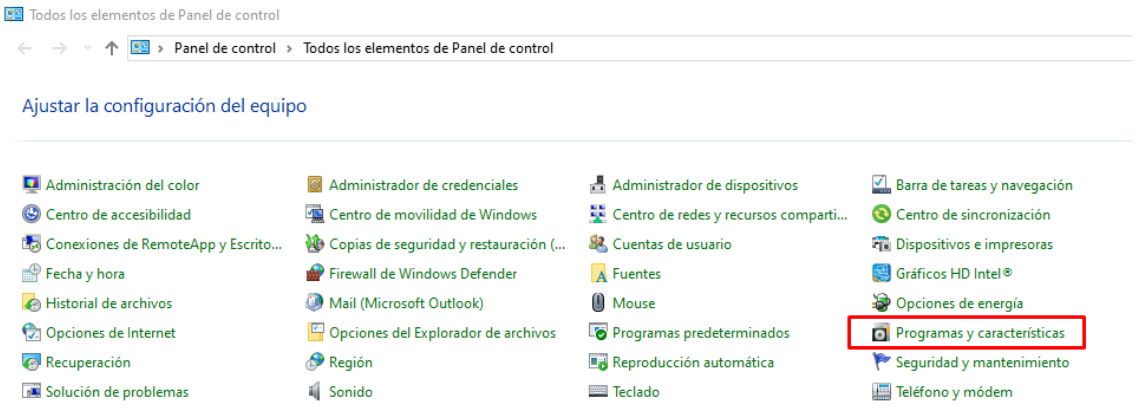
Anexo 5 Creación de carpeta para respaldos de máquinas virtuales



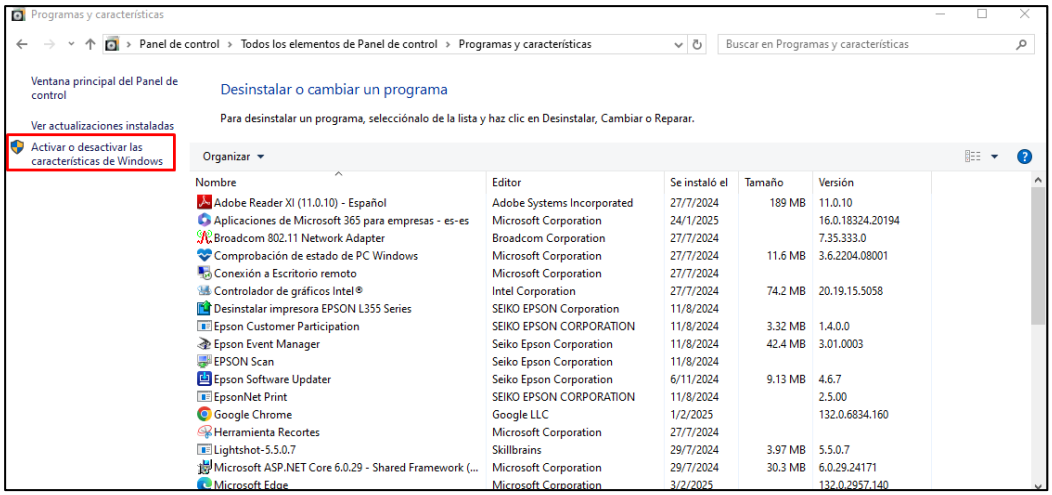
Anexo 6 Instalación del Veeam Backup & Replication



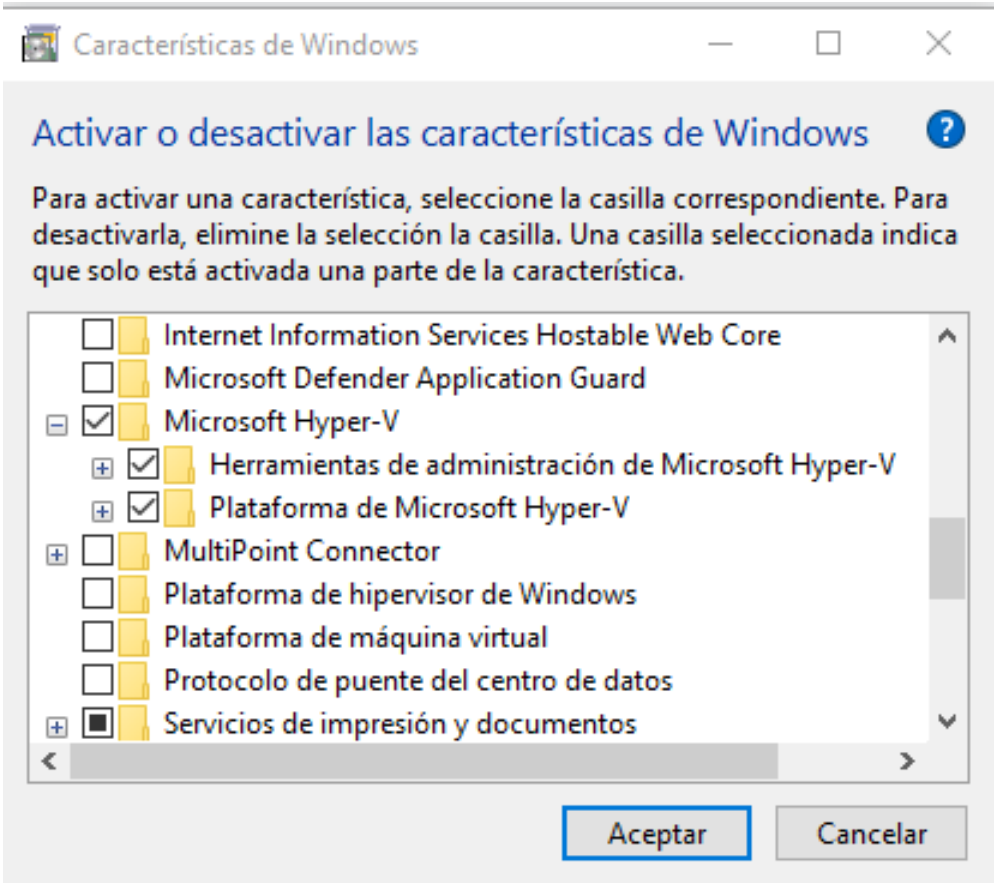
Anexo 7 Finalización de Veeam Backup Replication



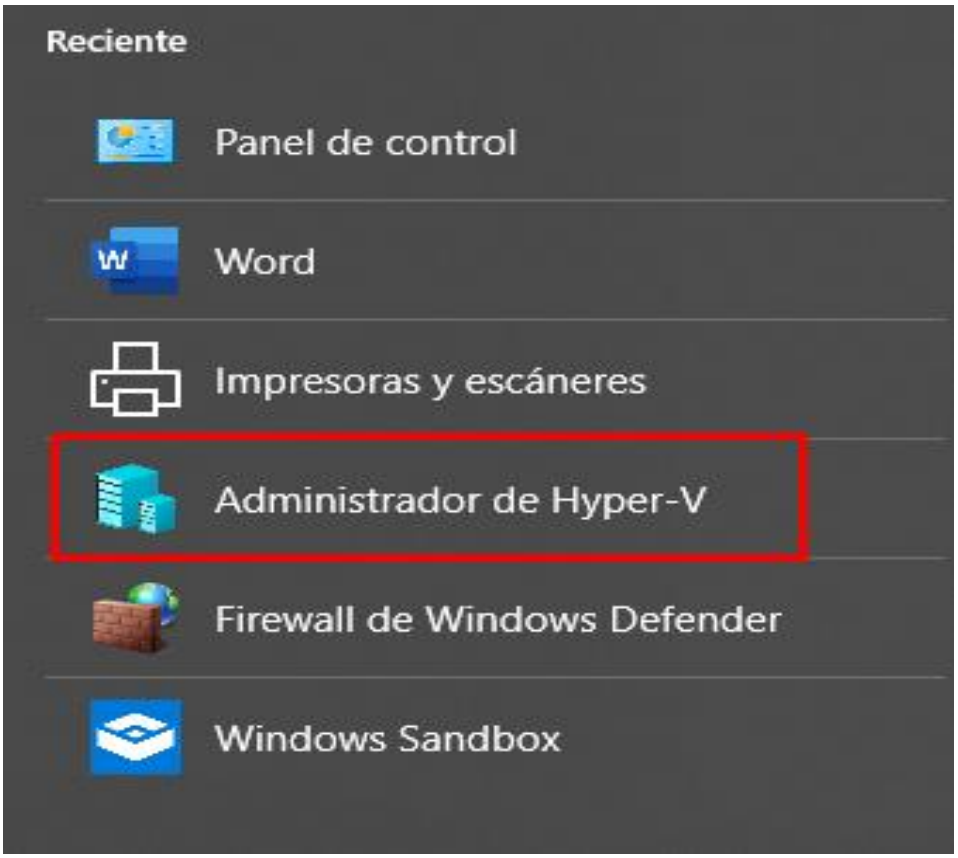
Anexo 8 Panel de control



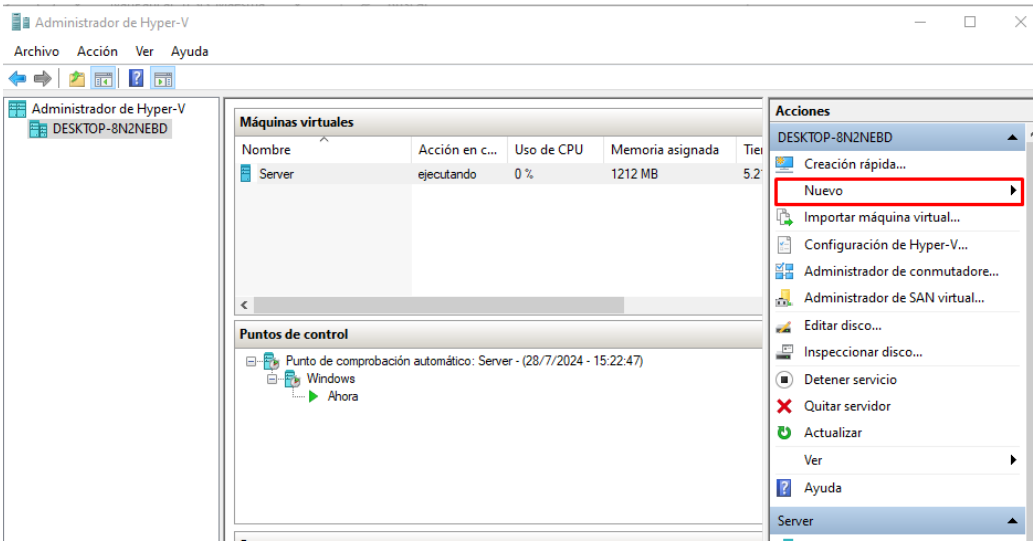
Anexo 9 Activar o desactivar las características de Windows



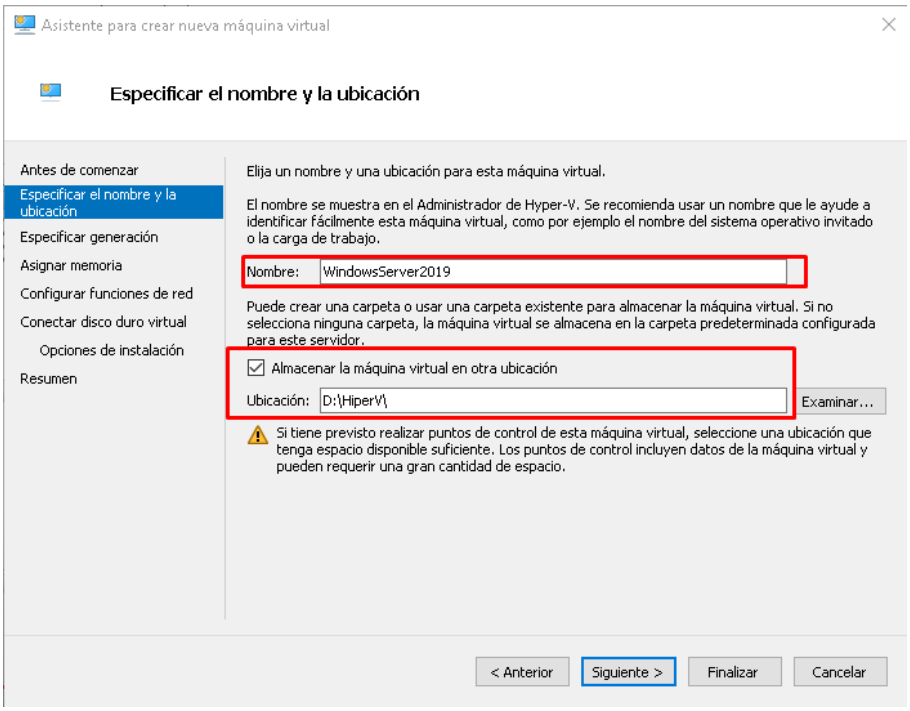
Anexo 10 Ventana de Características de Windows



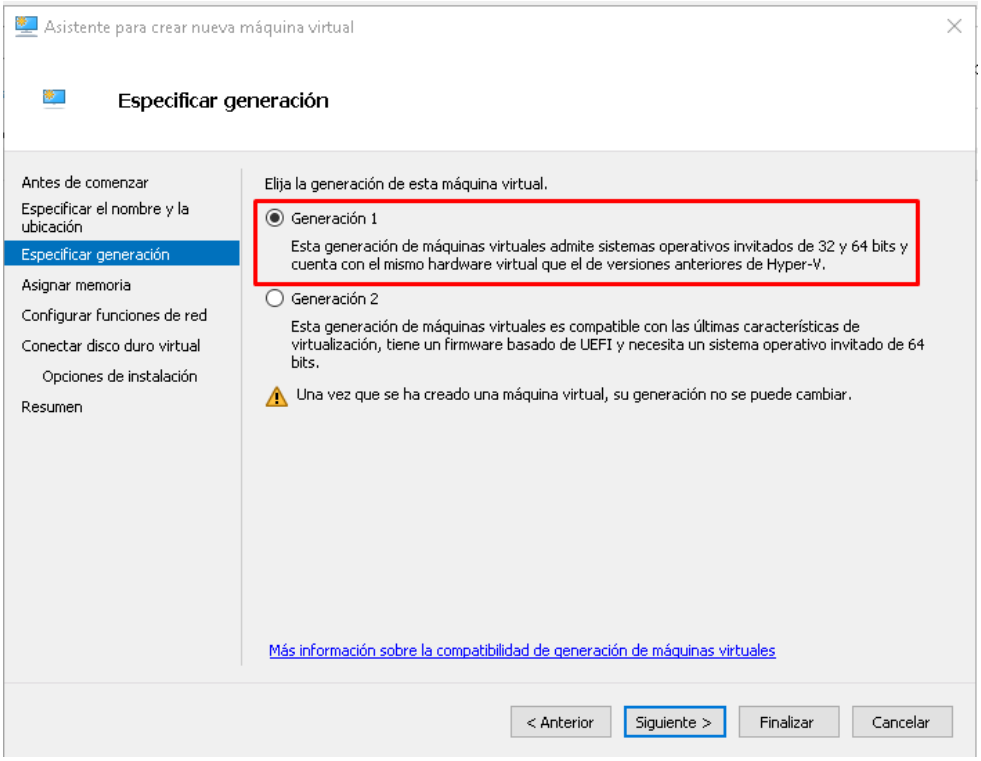
Anexo 11 Administrador de Hyper-V



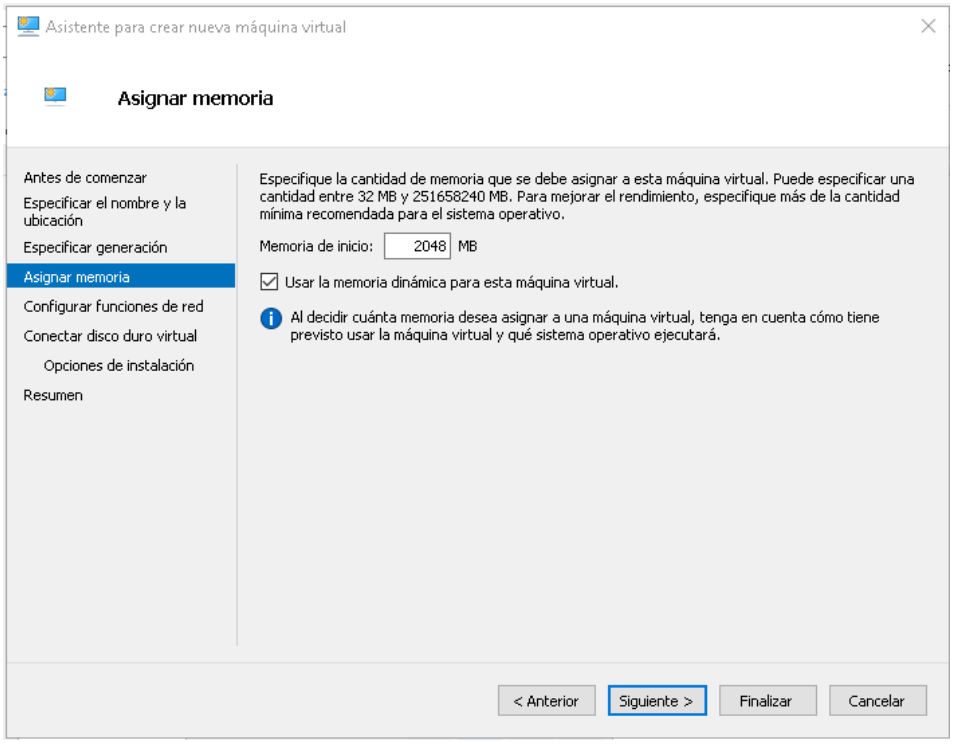
Anexo 12 Administrador de Hyper-V



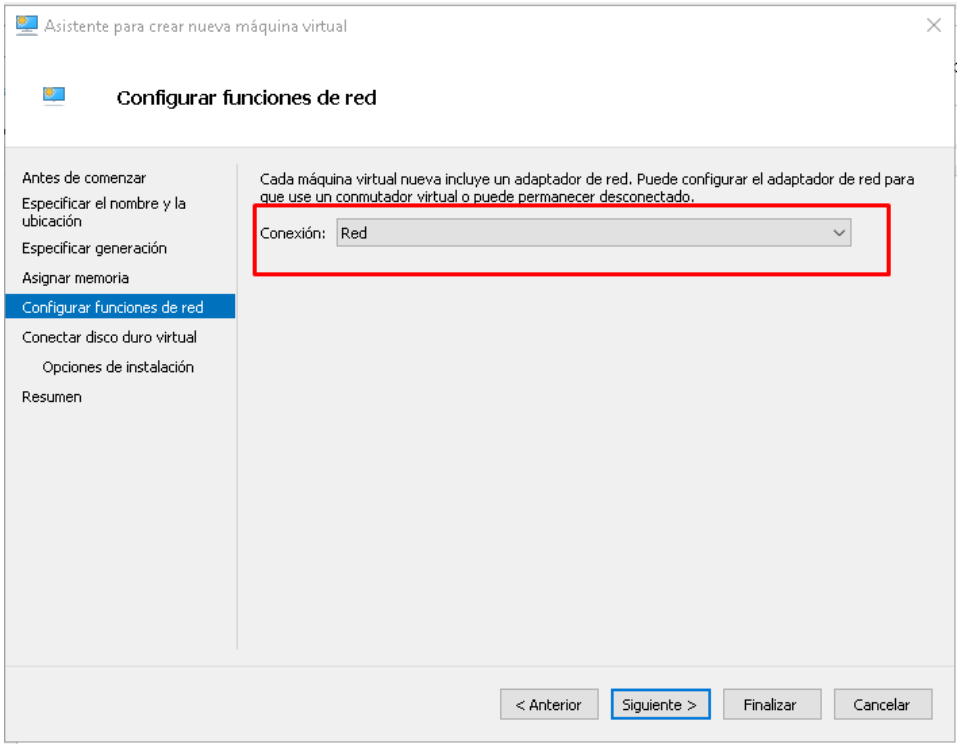
Anexo 13 Especificación de nombre y ubicación de máquinas virtuales



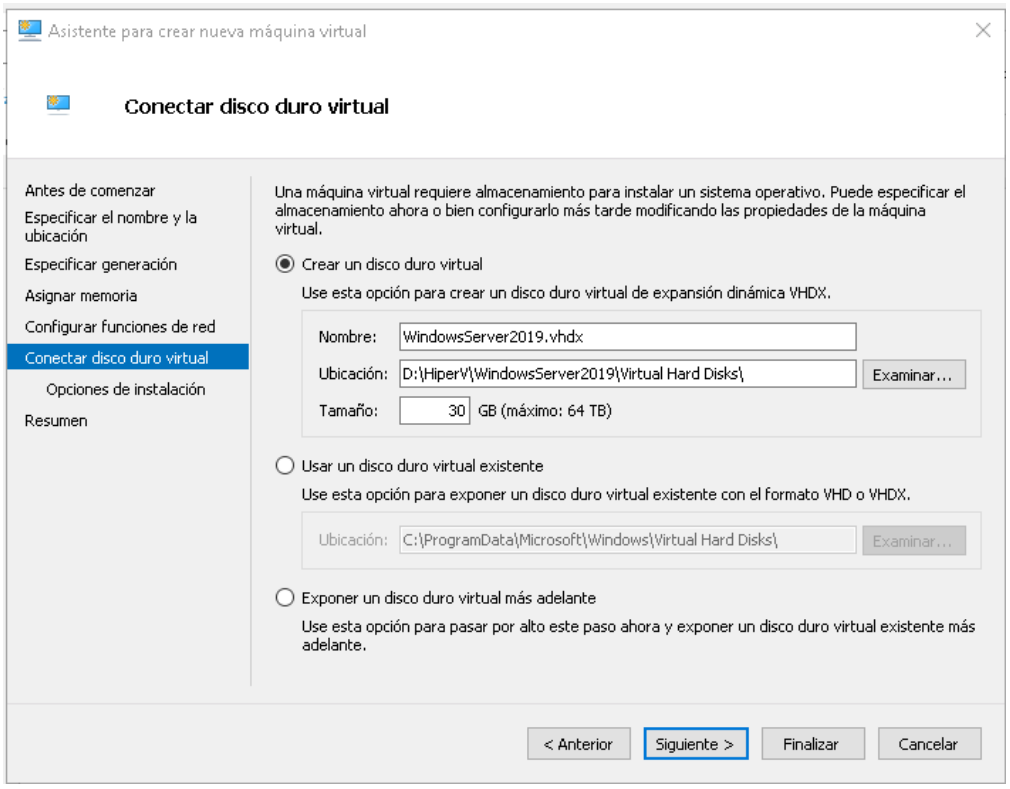
Anexo 14 Especificación de generación 1



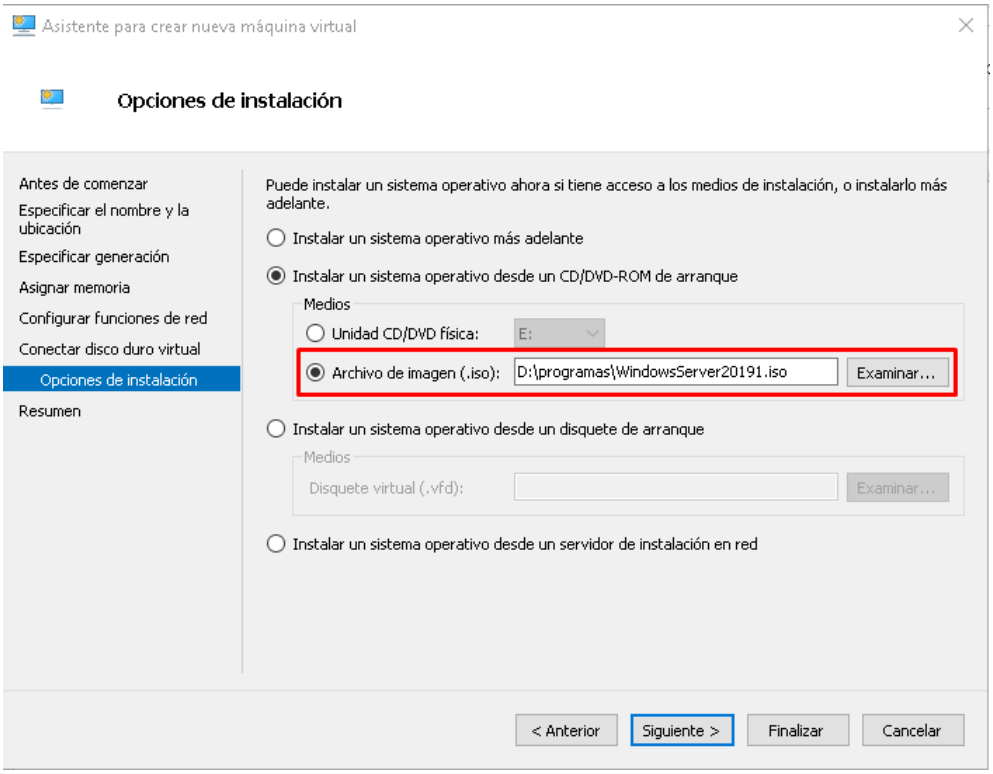
Anexo 15 Asignar memoria a la máquina virtual



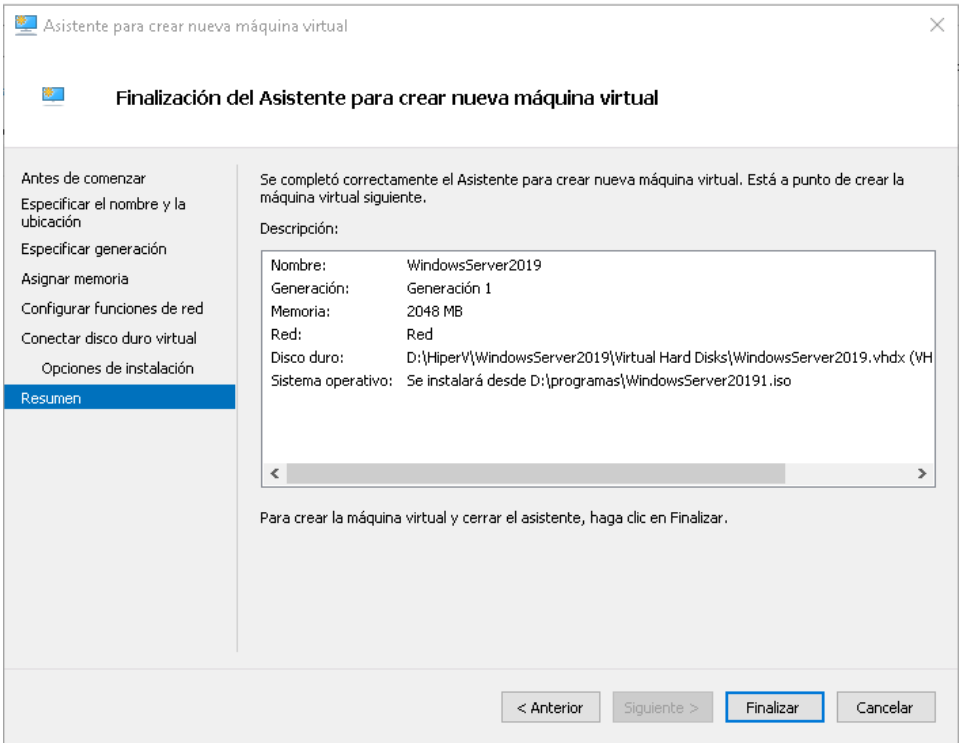
Anexo 16 *Configurar funciones de red*



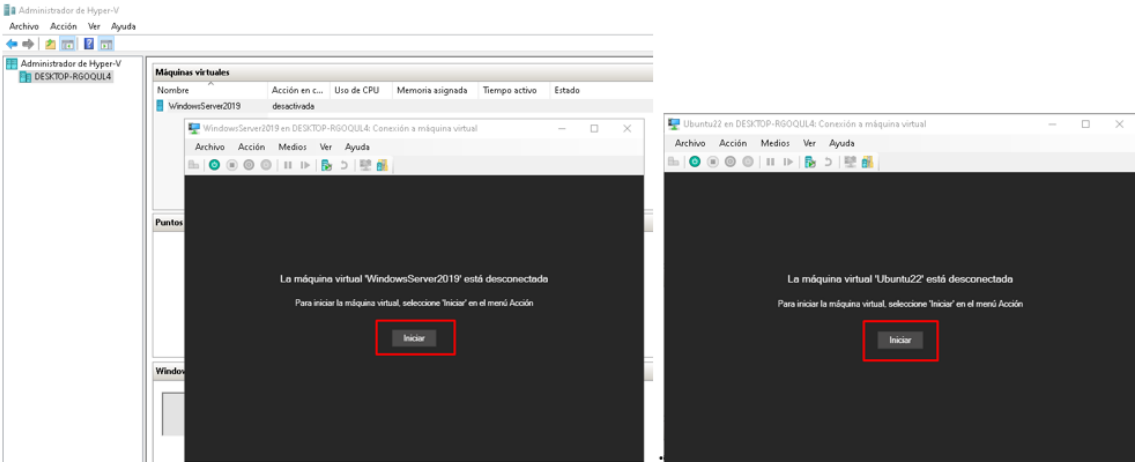
Anexo 17 *Conectar disco duro virtual*



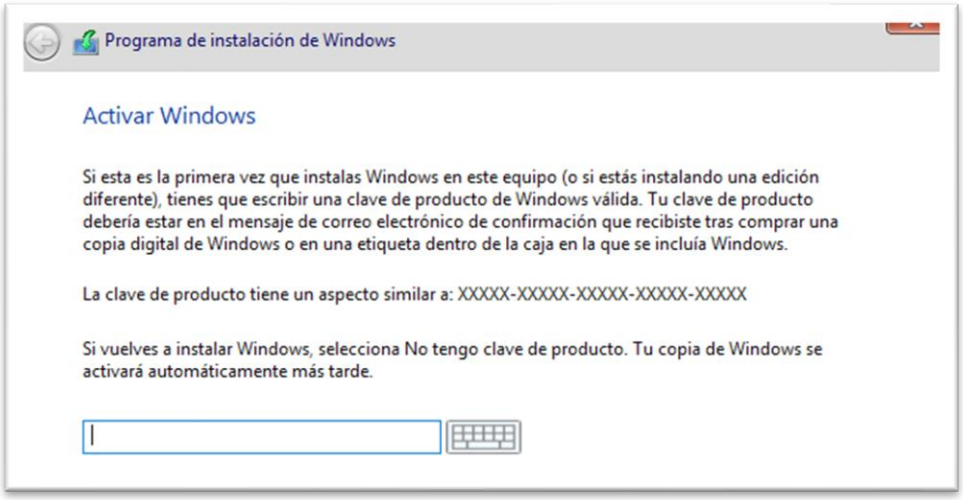
Anexo 18 *Opciones de instalación*



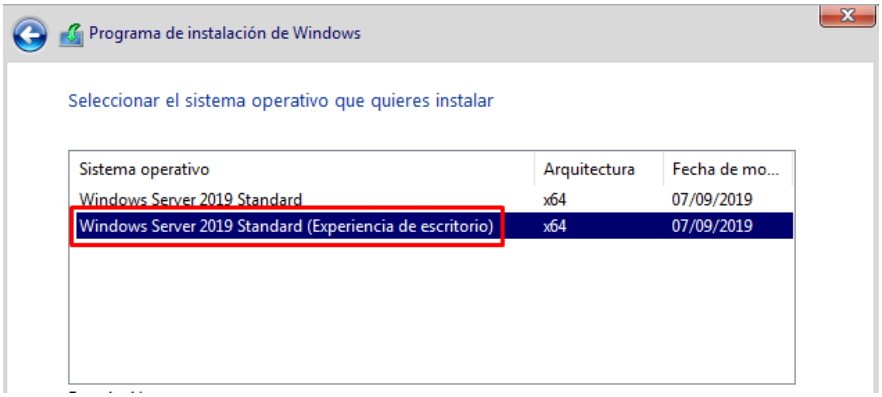
Anexo 19 *Finalización del asistente para crear nueva máquina virtual*



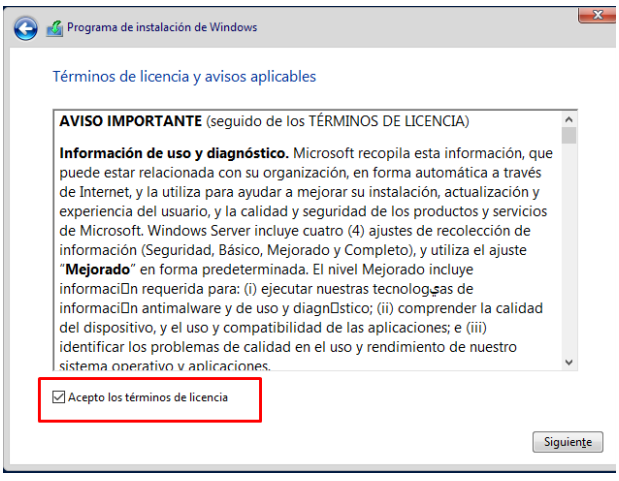
Anexo 20 *Iniciar instalación de Windows Server 2019*



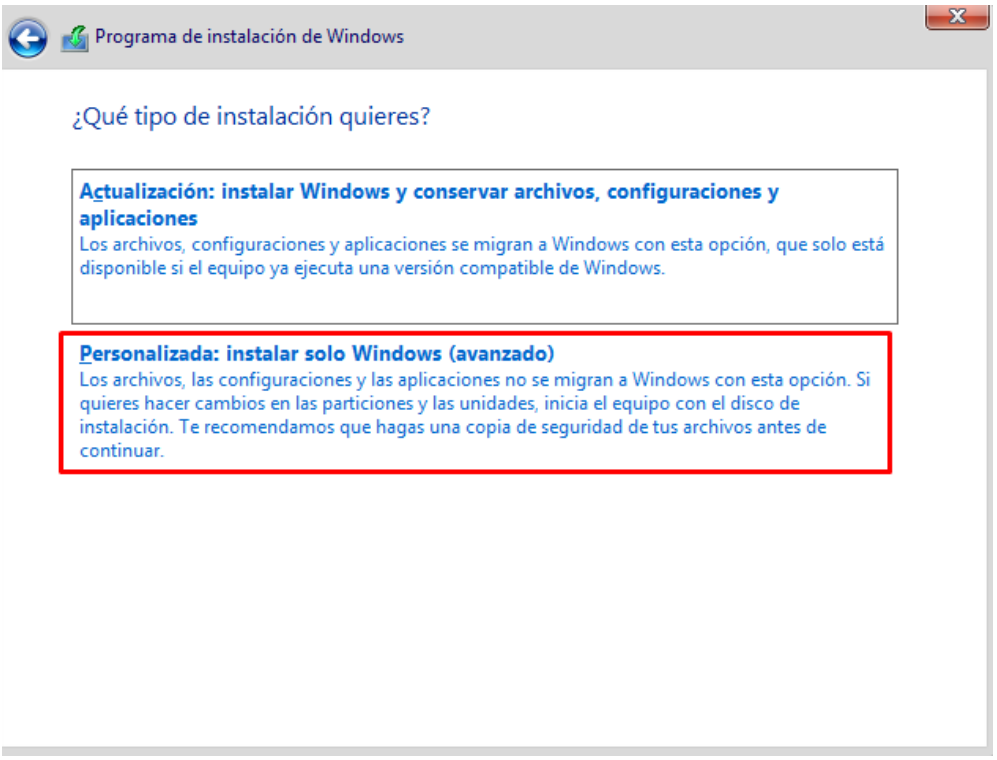
Anexo 21 *Activar Windows*



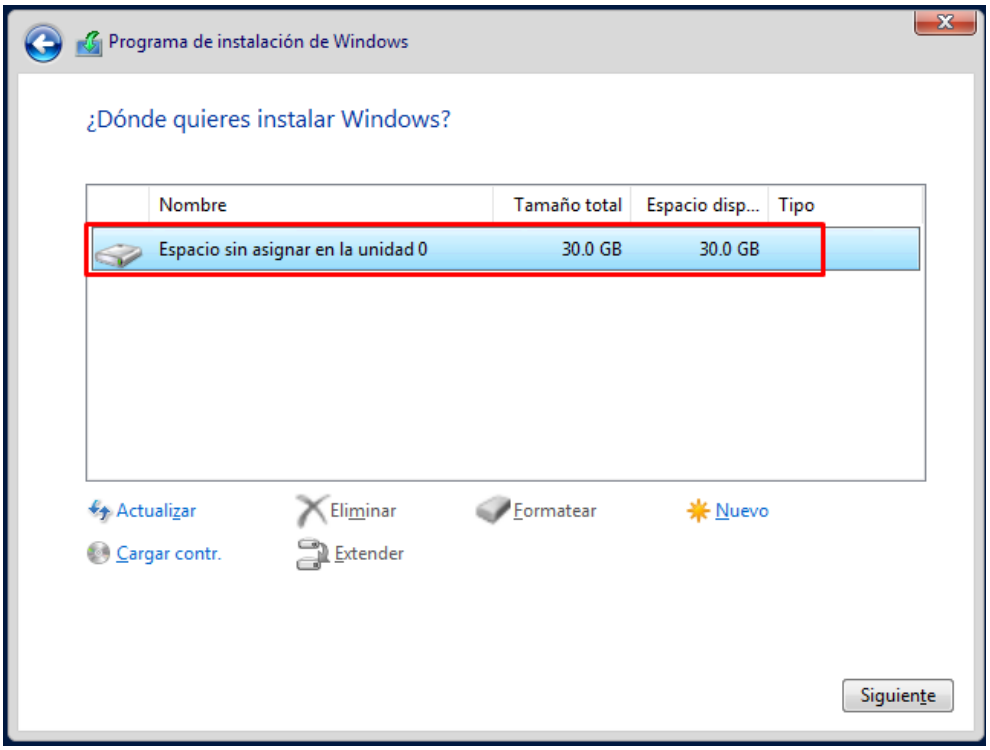
Anexo 22 *Selección del sistema operativo*



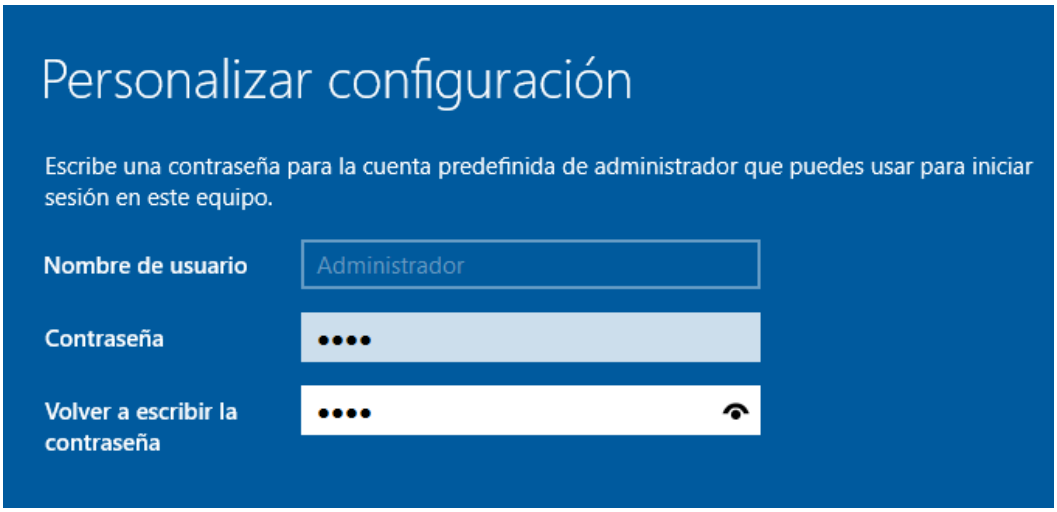
Anexo 23 *Aceptar los términos de licencia*



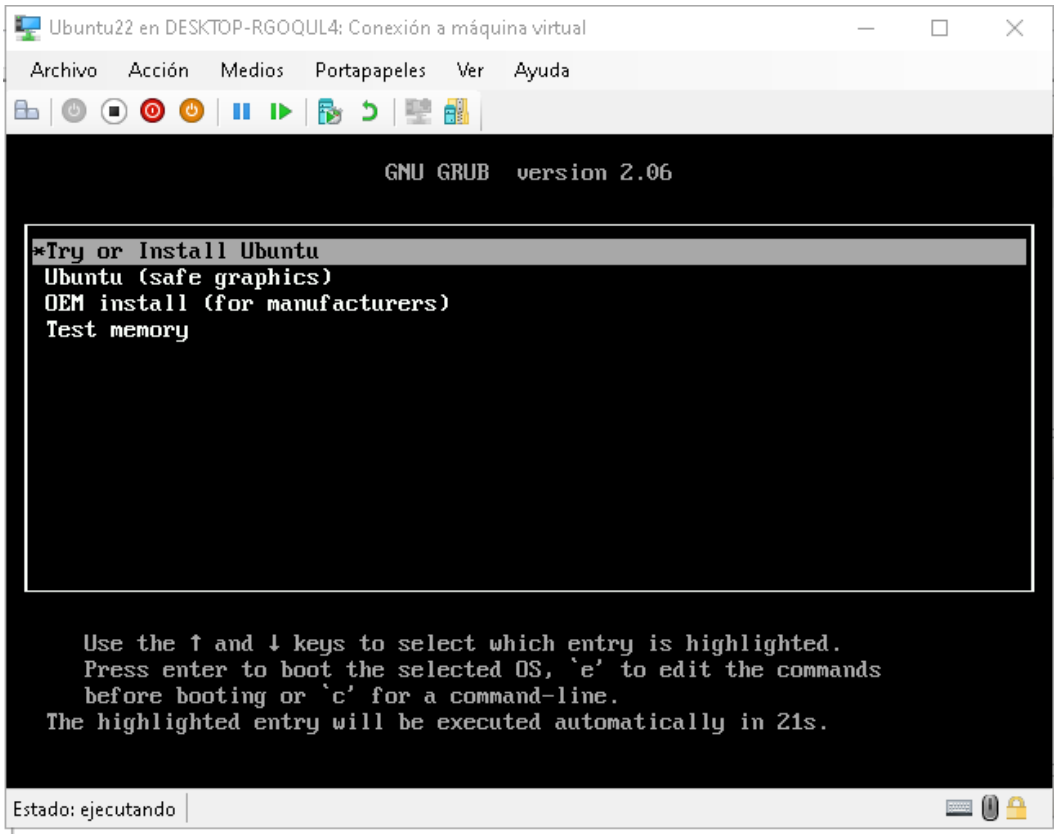
Anexo 24 *Tipo de instalación*



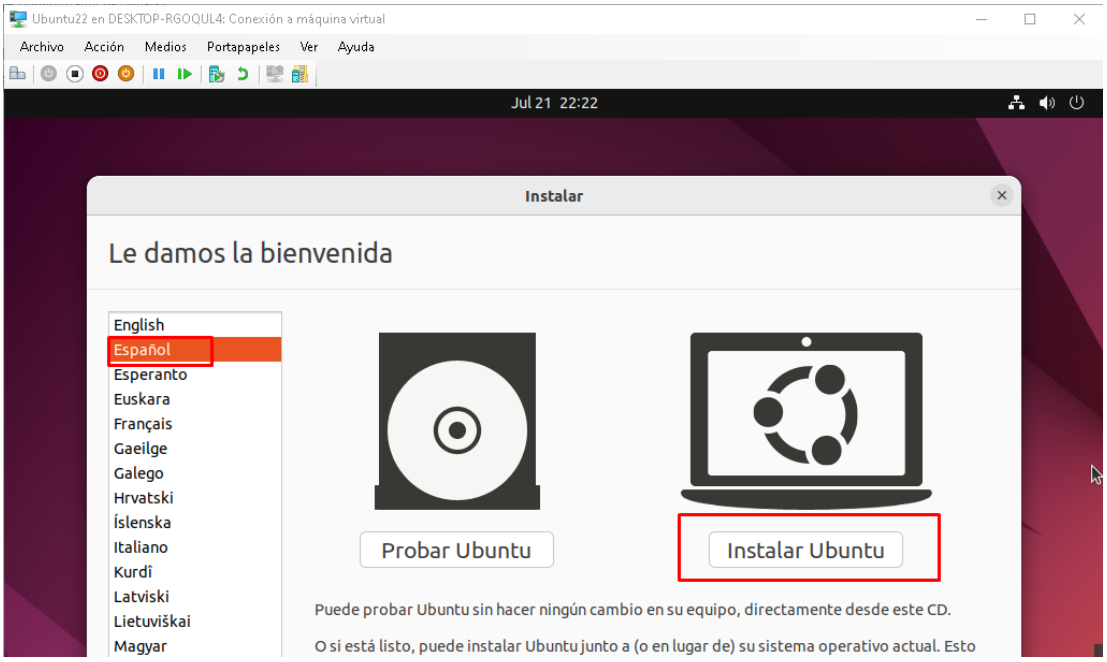
Anexo 25 *Selección de unidad virtual donde se va a instalar*



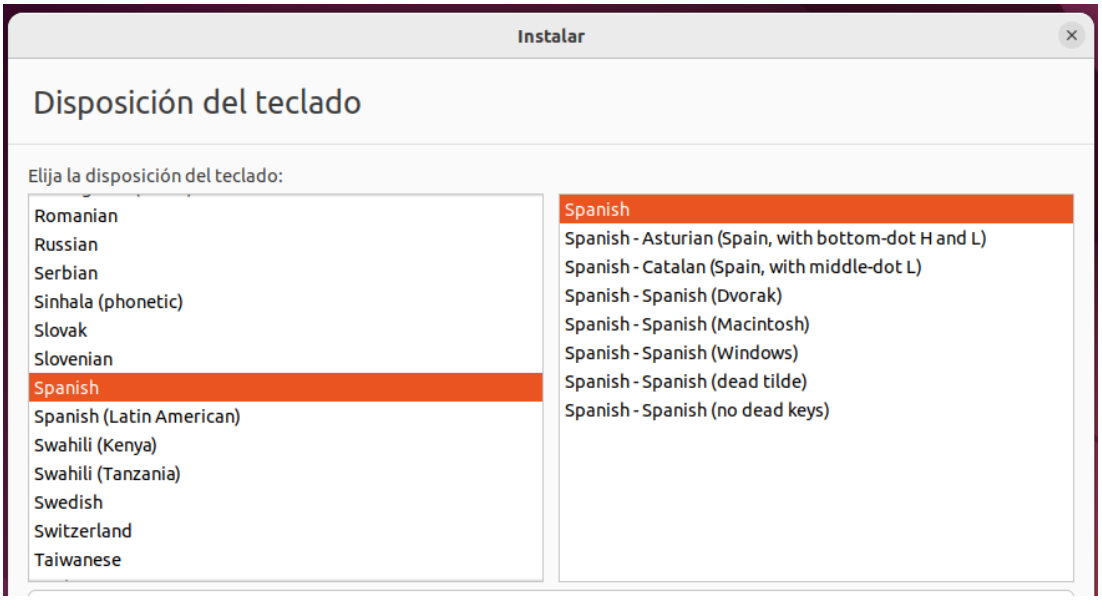
Anexo 26 *Configuración de administrador de Windows Server*



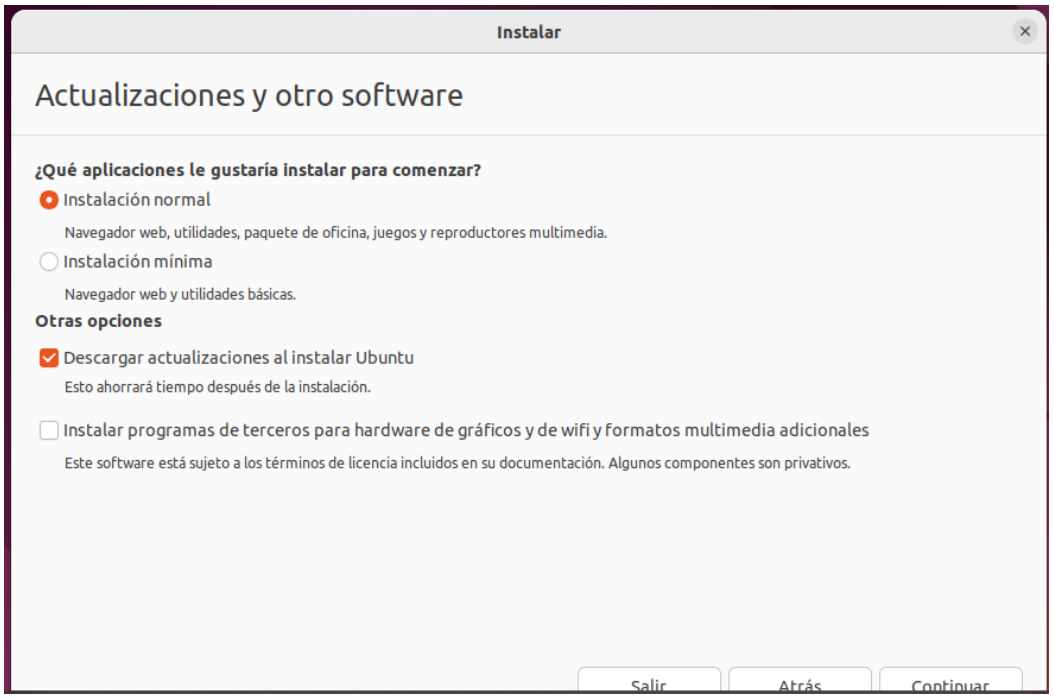
Anexo 27 *Selección Try or Install Ubuntu*



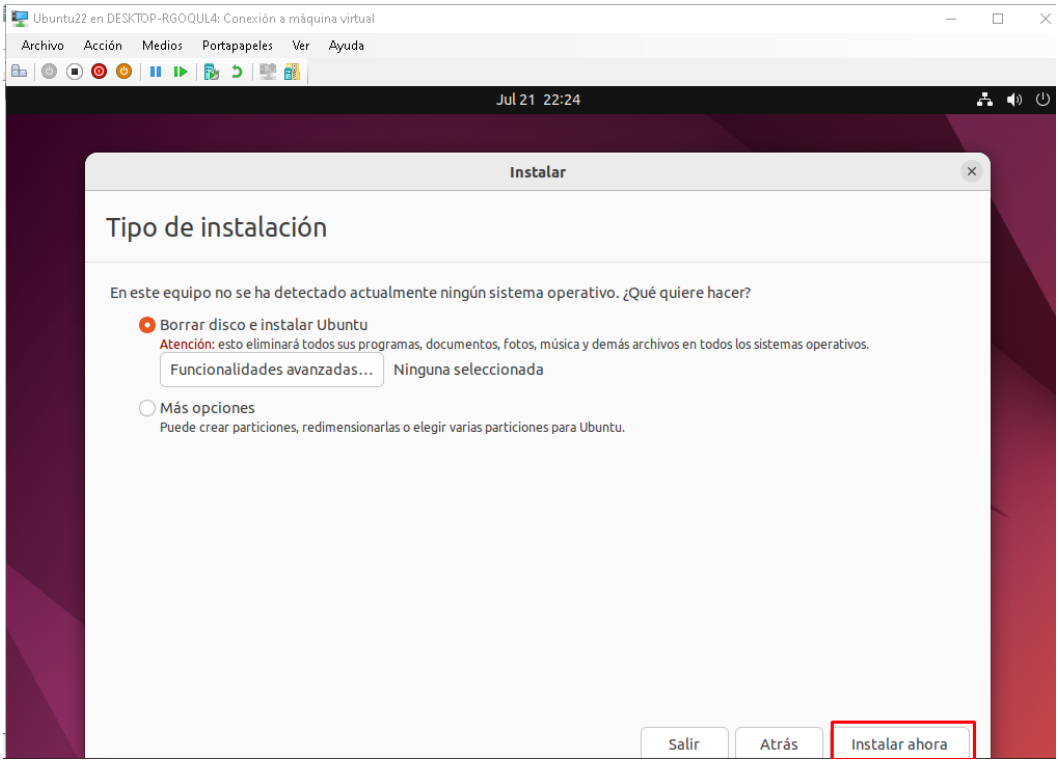
Anexo 28 *Instalación Ubuntu*



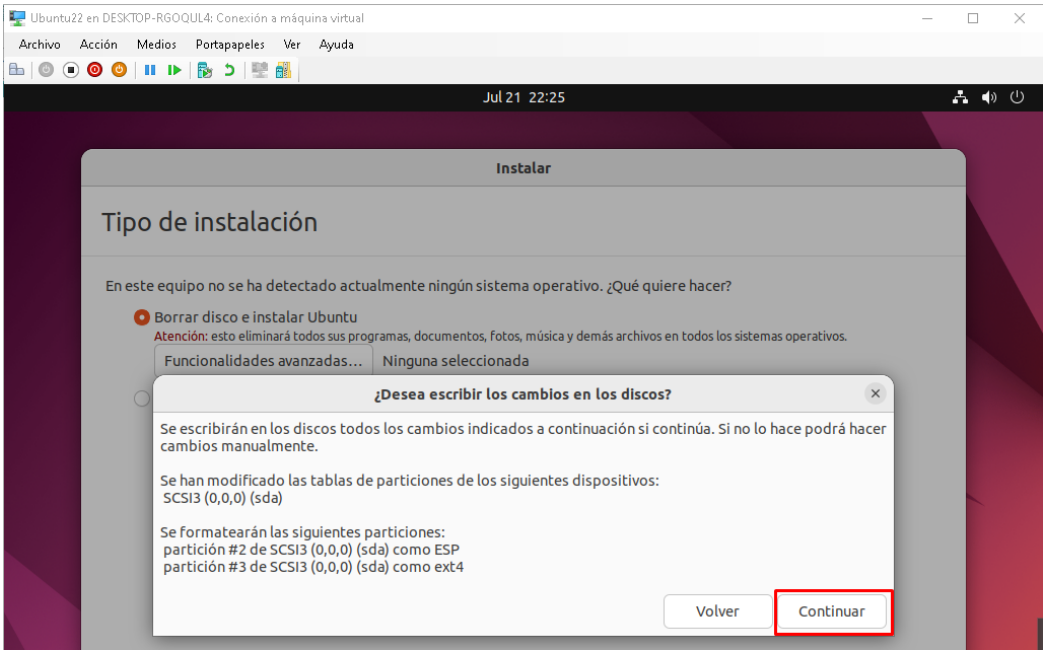
Anexo 29 *Configuración del idioma en teclado*



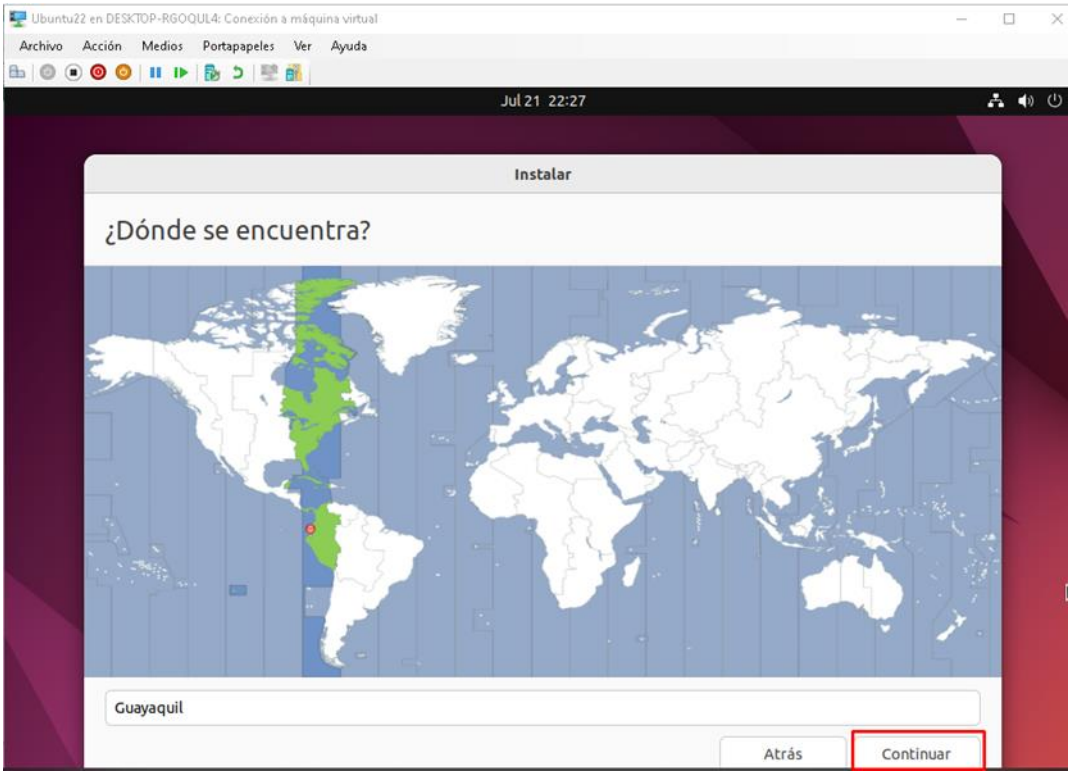
Anexo 30 *Configuración apartado "Actualización y otro software"*



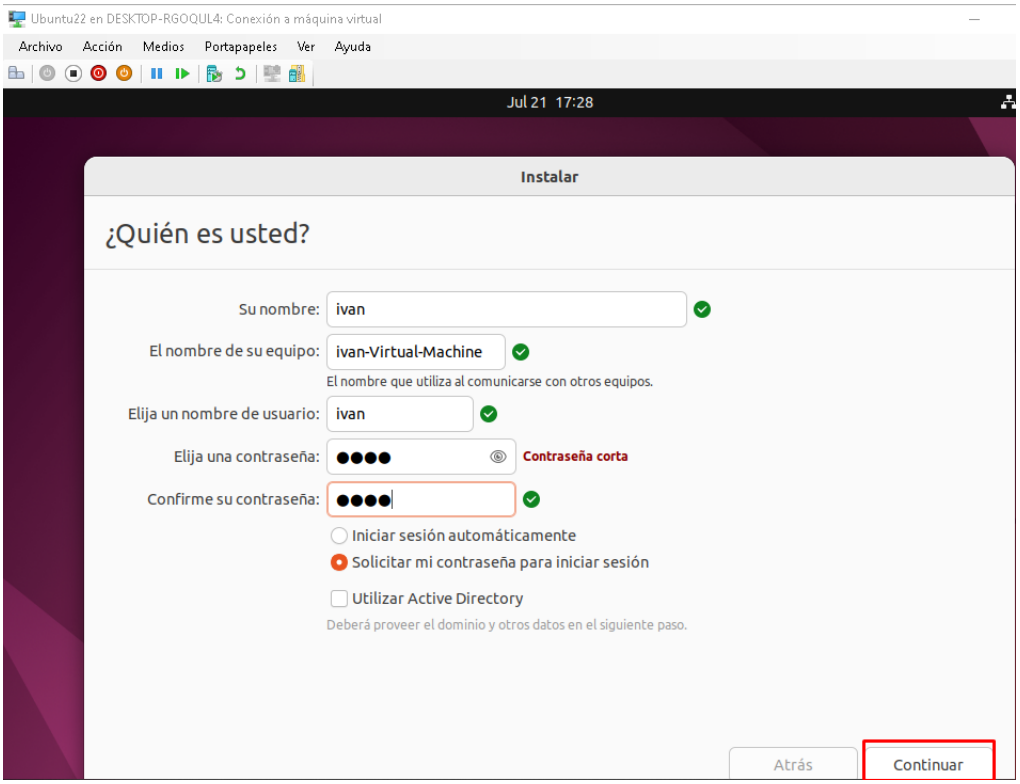
Anexo 31 *Configuración tipo de instalación*



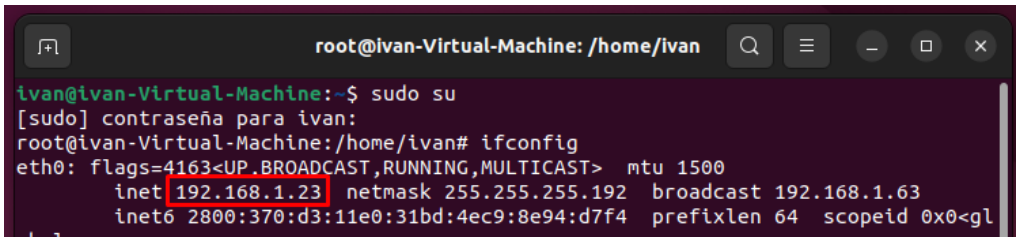
Anexo 32 *Pantalla ¿Desea escribir los cambios en los discos?*



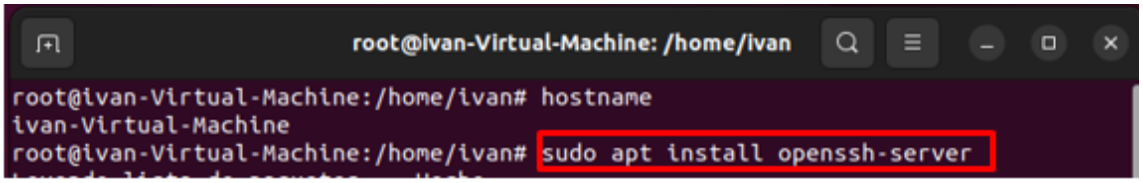
Anexo 33 *Selección de la zona geográfica*



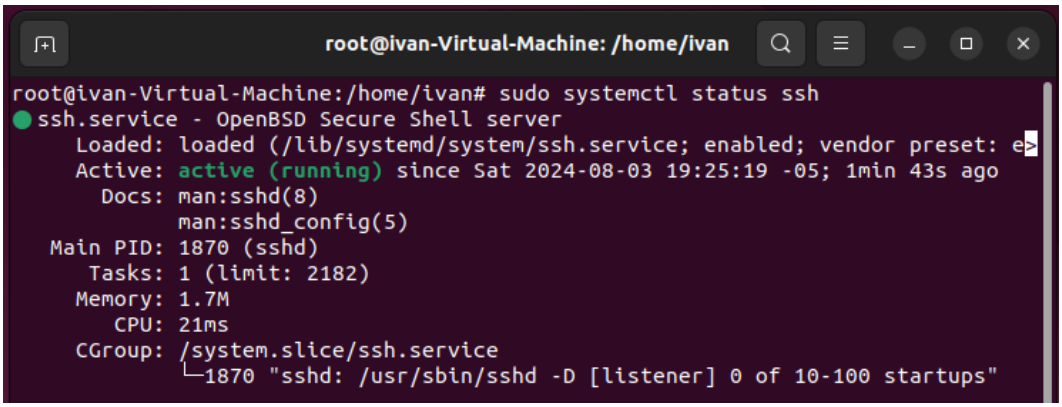
Anexo 34 *Configuración de datos de máquina virtual*



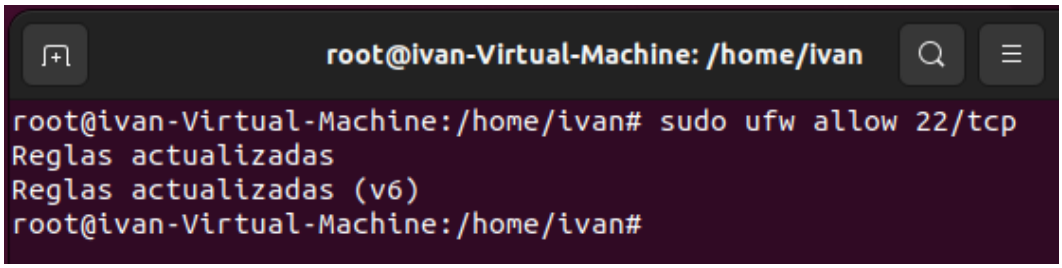
Anexo 35 *Ingreso en la terminal como administrador*



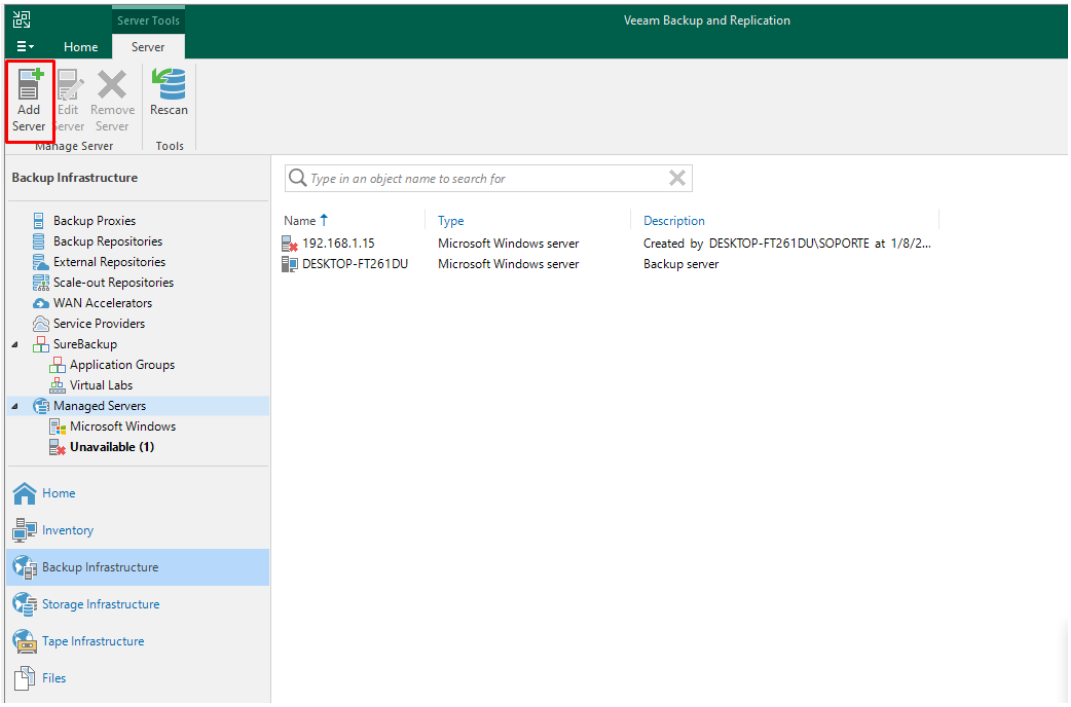
Anexo 36 *Ejecución de comando SSH*



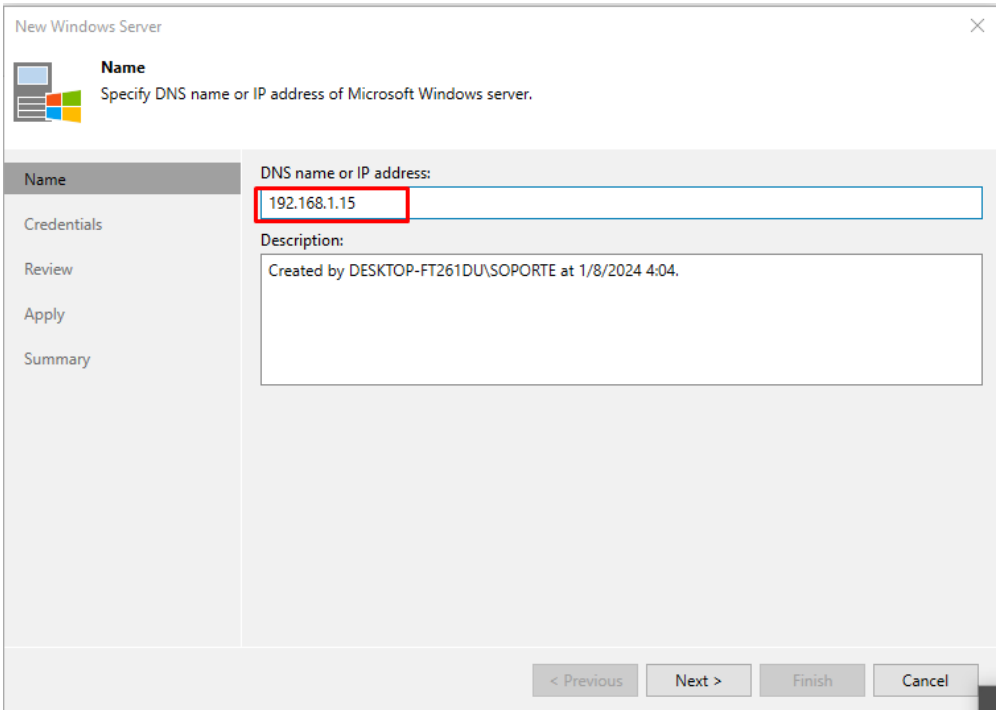
Anexo 37 *Revisión del status de SSH*



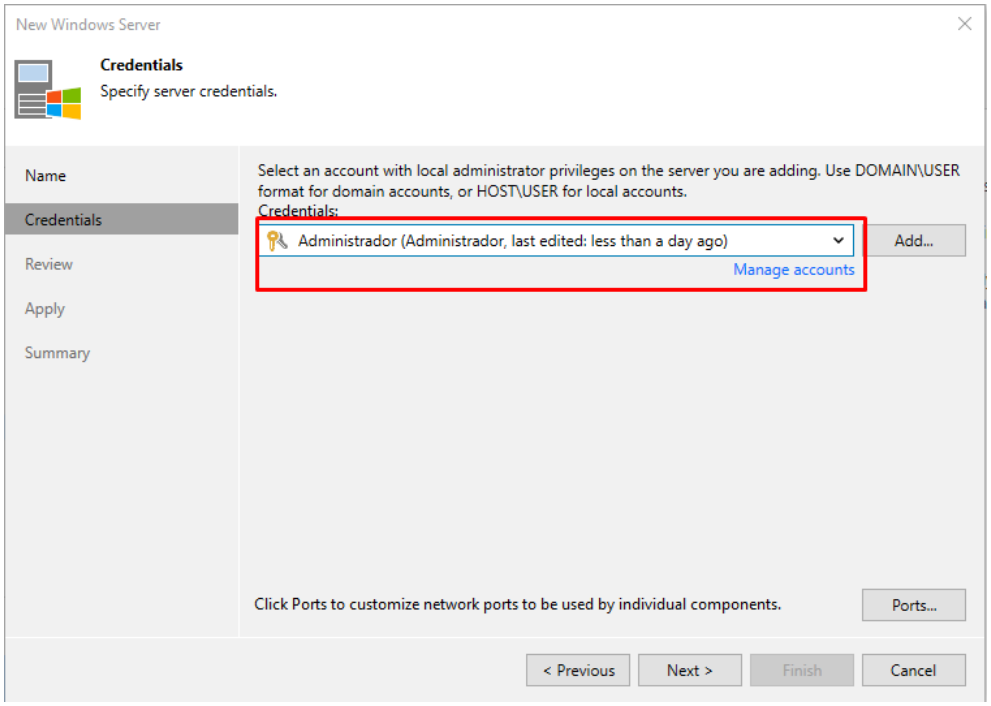
Anexo 38 *Habilitación del puerto 22 en Ubuntu 22*



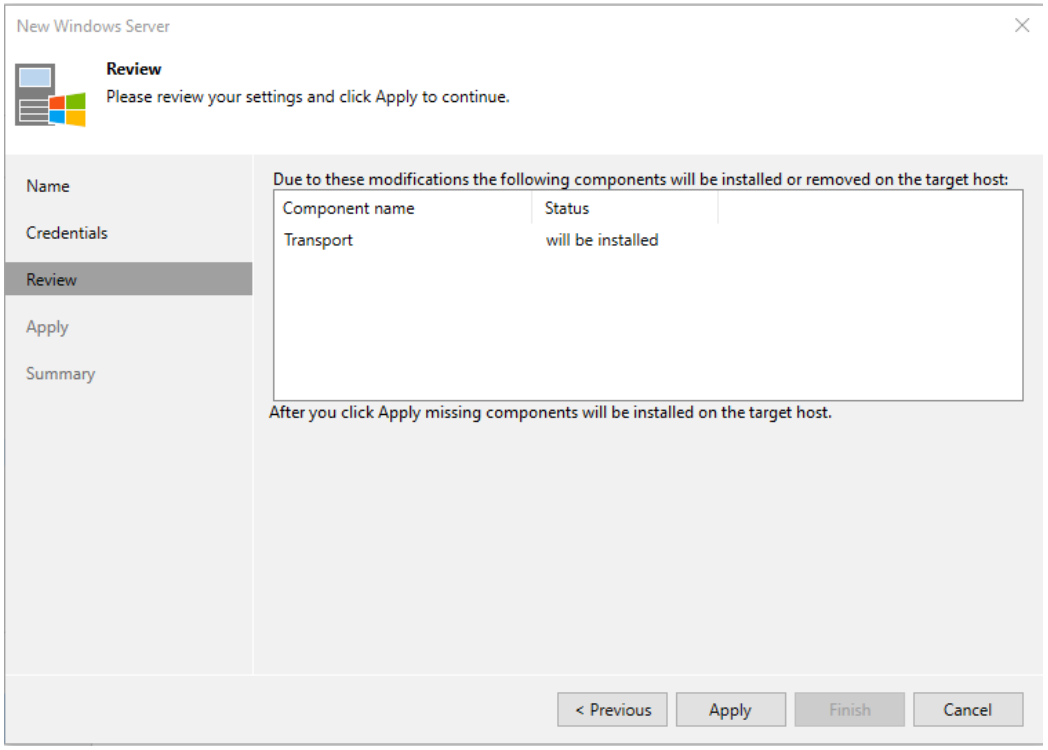
Anexo 39 *Add Server*



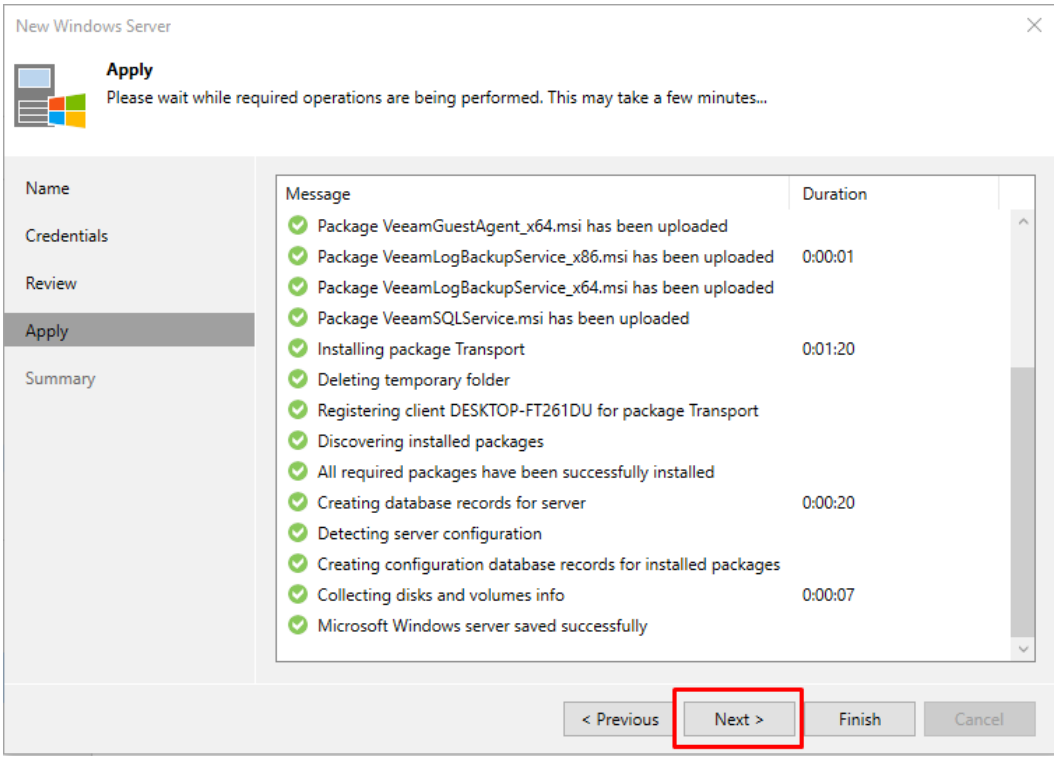
Anexo 40 *Nombre DNS o IP del servidor cliente*



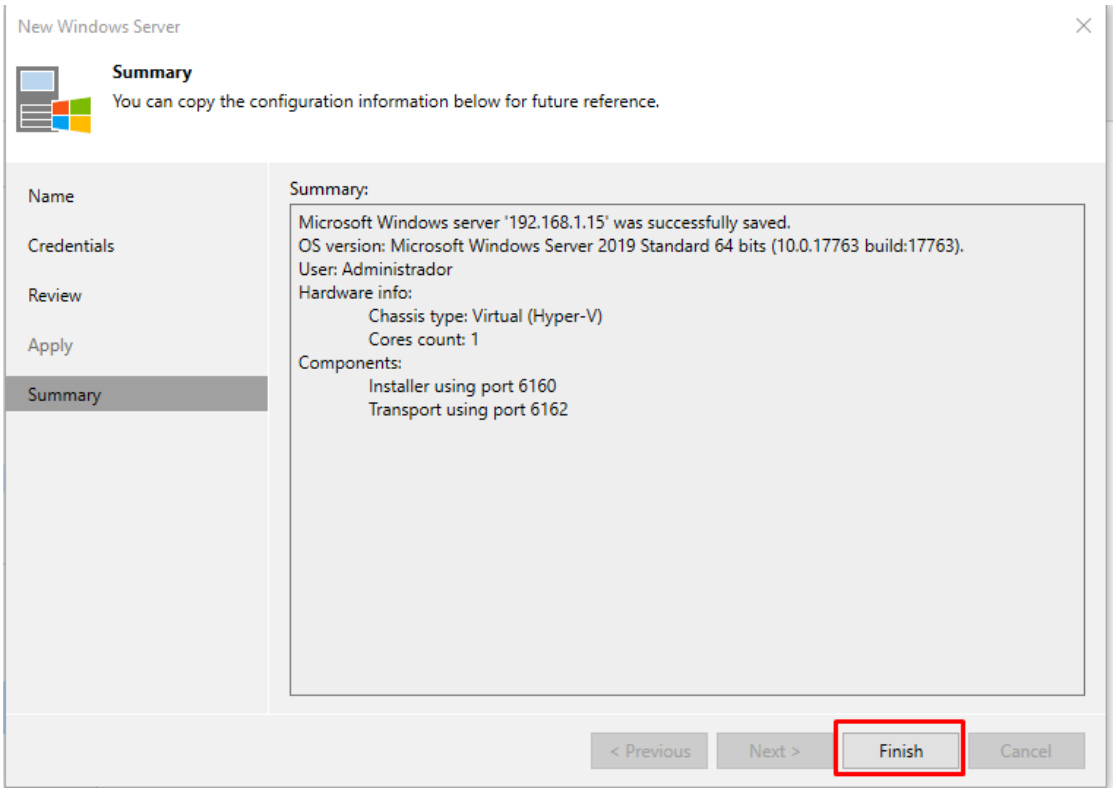
Anexo 41 *Credenciales de administrador Windows Server 2019*



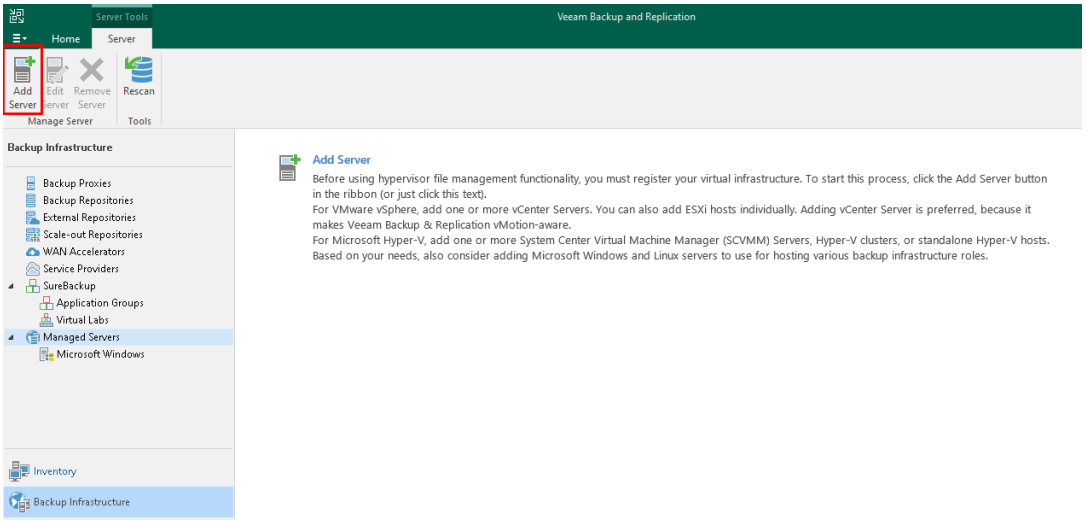
Anexo 42 *Estatus de instalación del cliente*



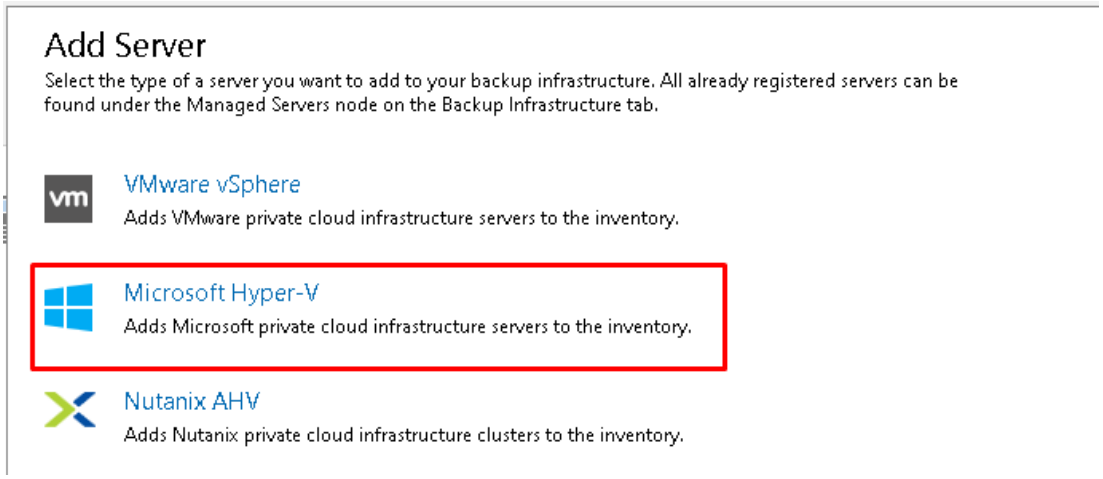
Anexo 43 *Instalación de los complementos en equipo del cliente*



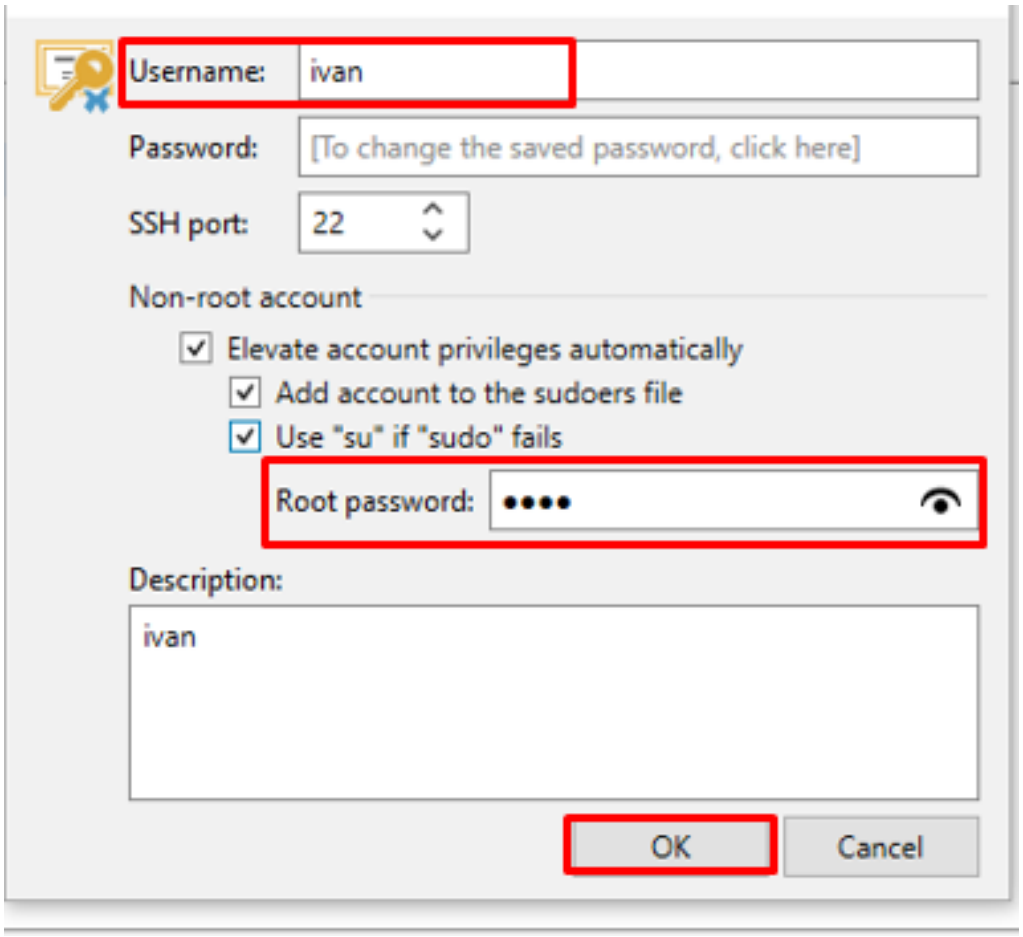
Anexo 44 *Finalización de la instalación del cliente en Windows Server 2019*



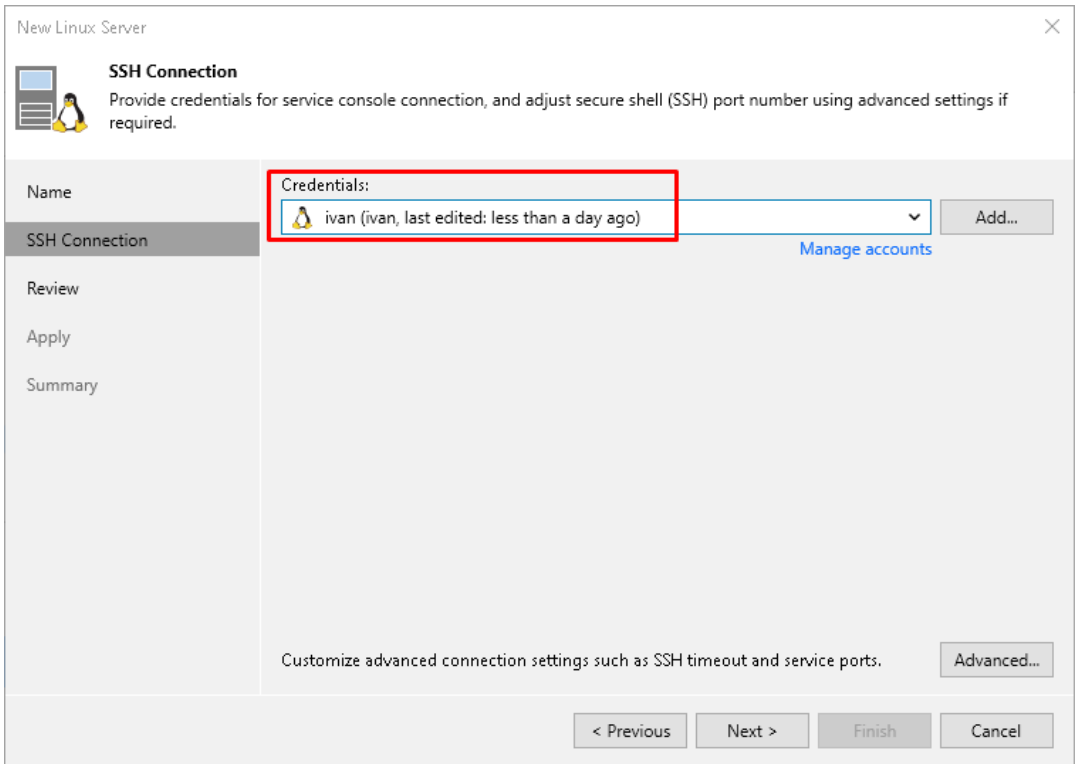
Anexo 45 *Agregar en Veeam Backup & Replicación Linux Ubuntu 22*



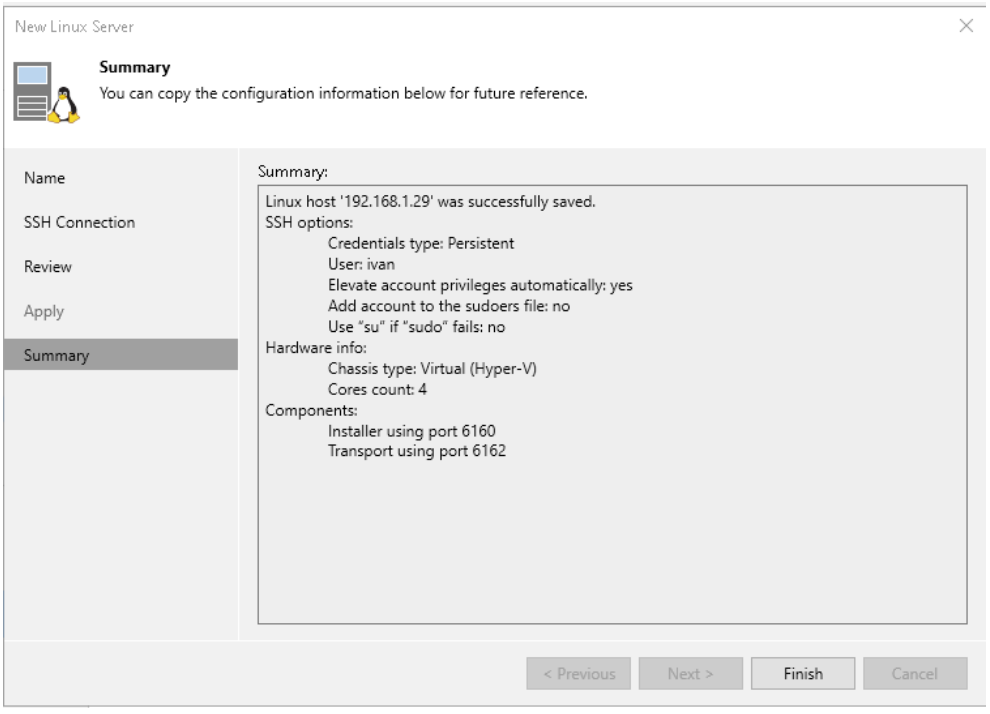
Anexo 46 *Añadir servidor Microsoft Hyper -V*



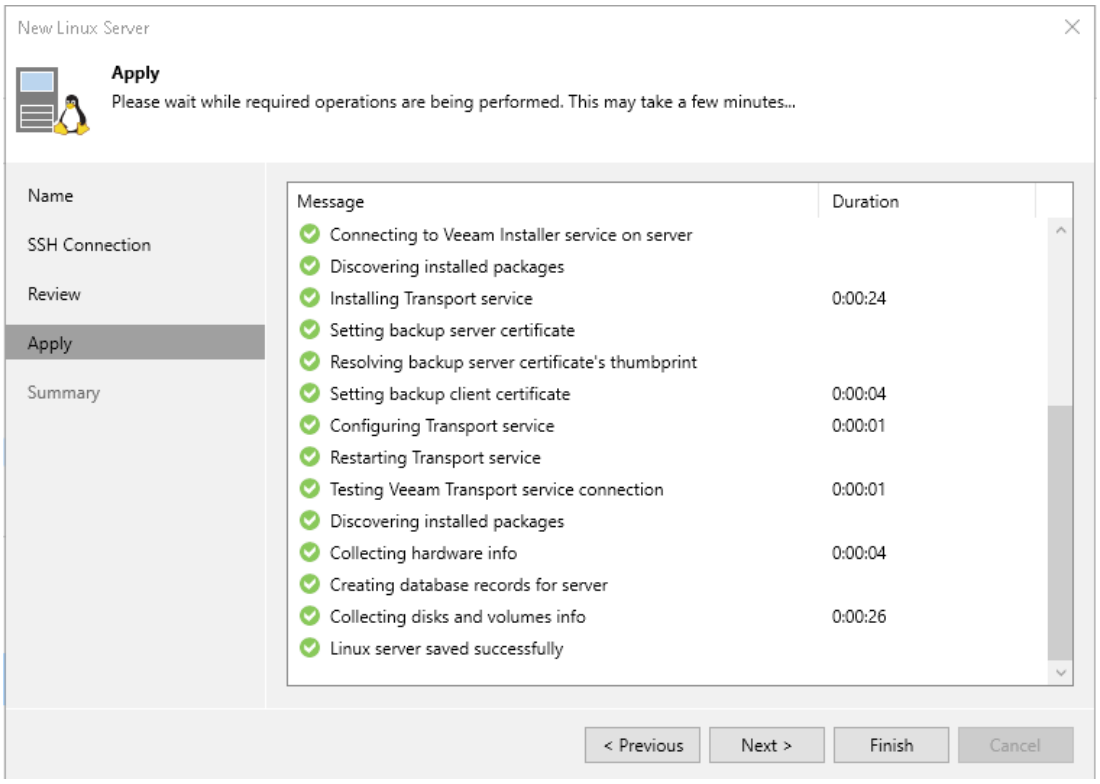
Anexo 47 *Credenciales de admin para conexión con Ubuntu 22 del cliente*



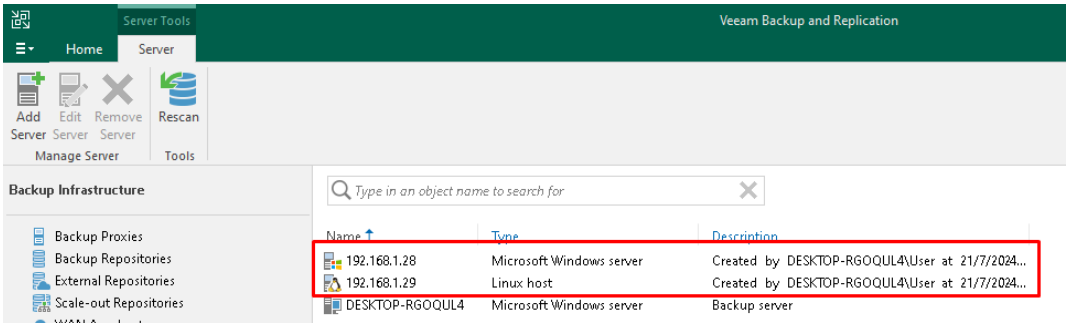
Anexo 48 *SSH Connection para conectar con el root de Ubuntu 22 del cliente*



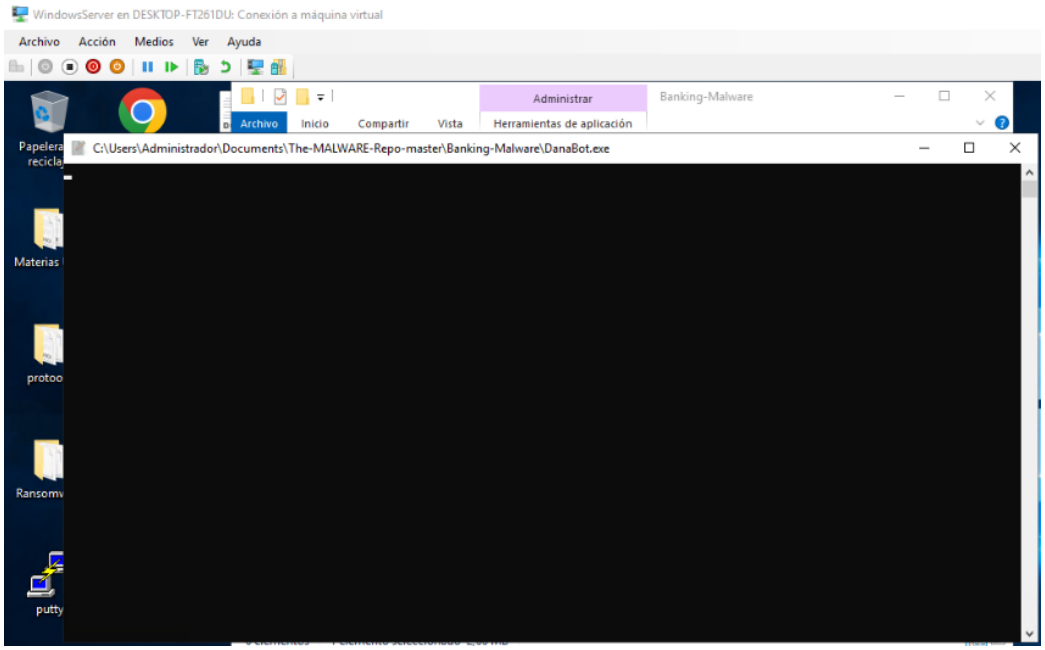
Anexo 49 *Ventana de resumen del cliente Ubuntu 22*



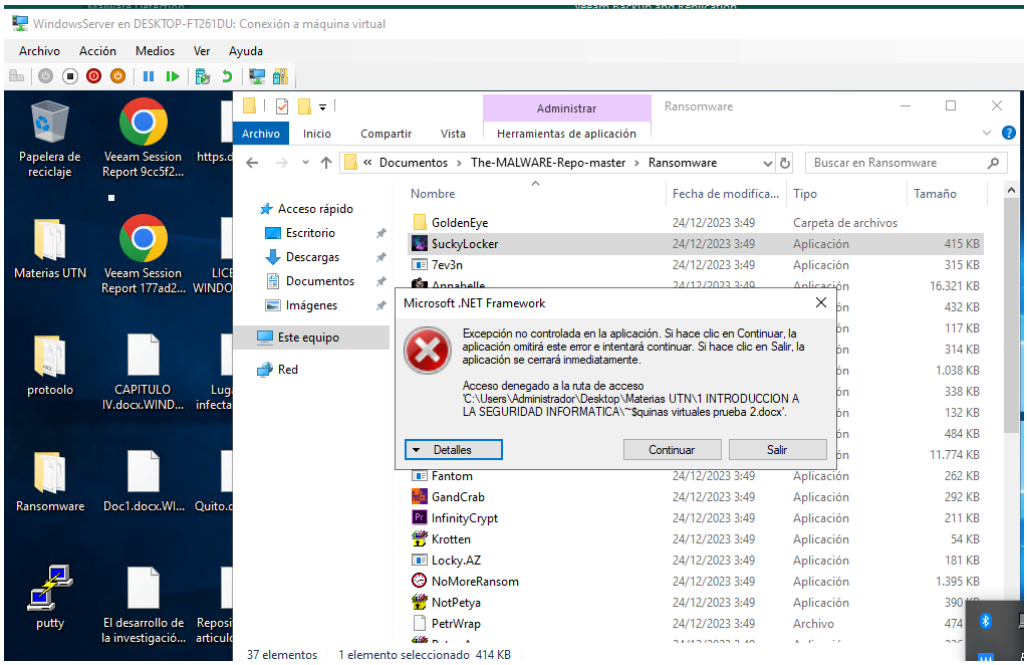
Anexo 50 *Componentes aplicados en cliente Ubuntu 22*



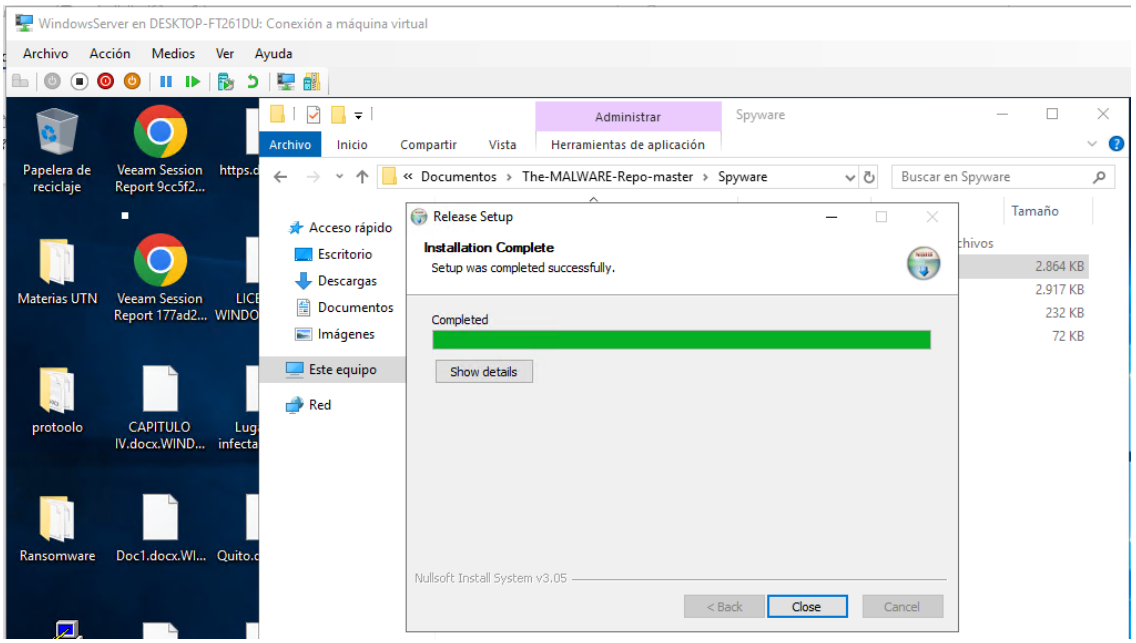
Anexo 51 *Cliente de Ubuntu 22 conectado en Veeam Backups & Replication*



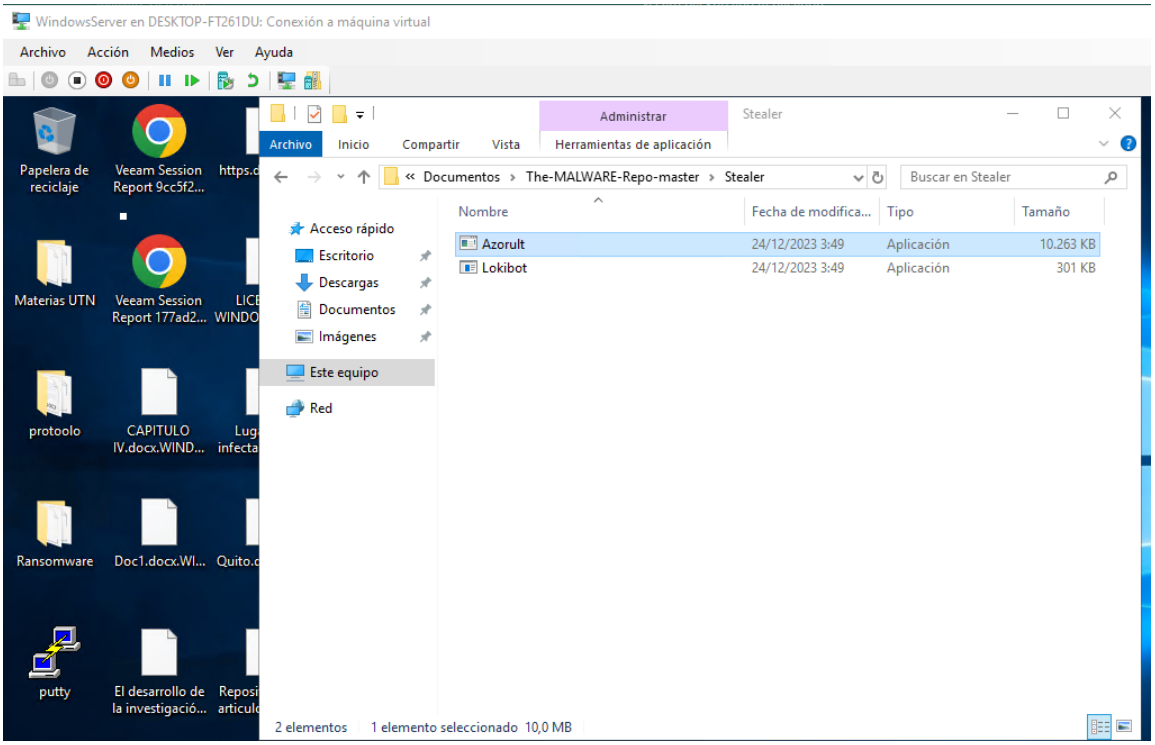
Anexo 52 *Infección a máquinas virtuales con Danabot*



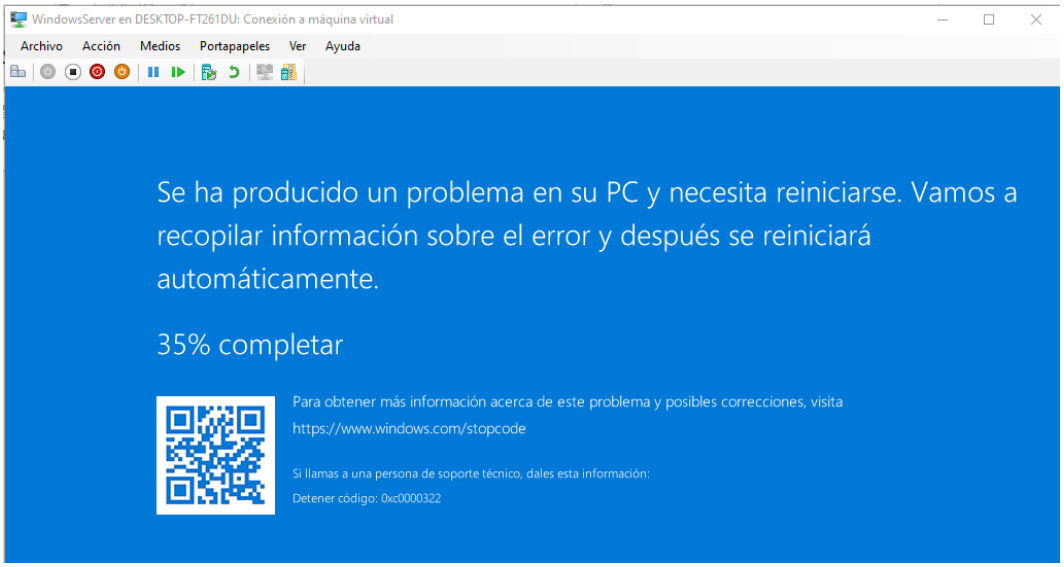
Anexo 53 *Infección de máquinas virtuales con $uckyLocker*



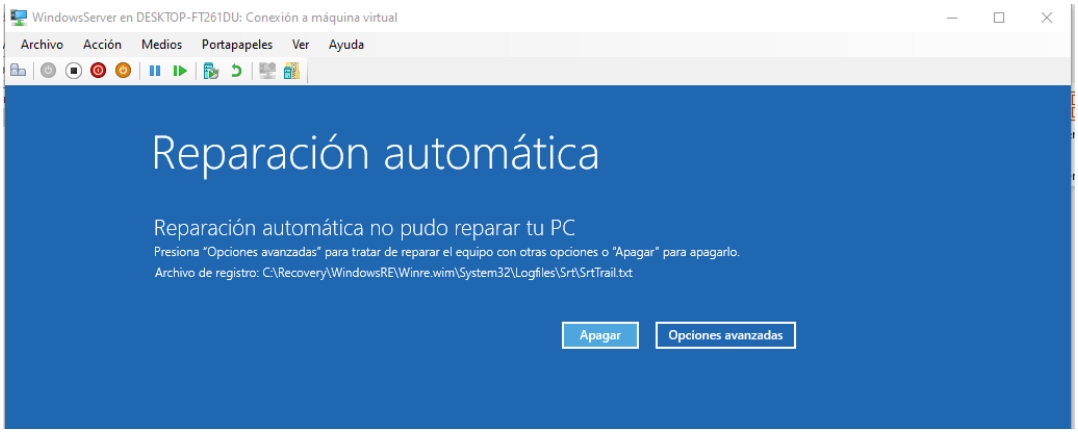
Anexo 54 *Infección de máquinas virtuales con AgentTesla*



Anexo 55 *Infección de máquinas virtuales con Azorult*



Anexo 56 *Infección de máquinas virtuales con Trojan Ana*



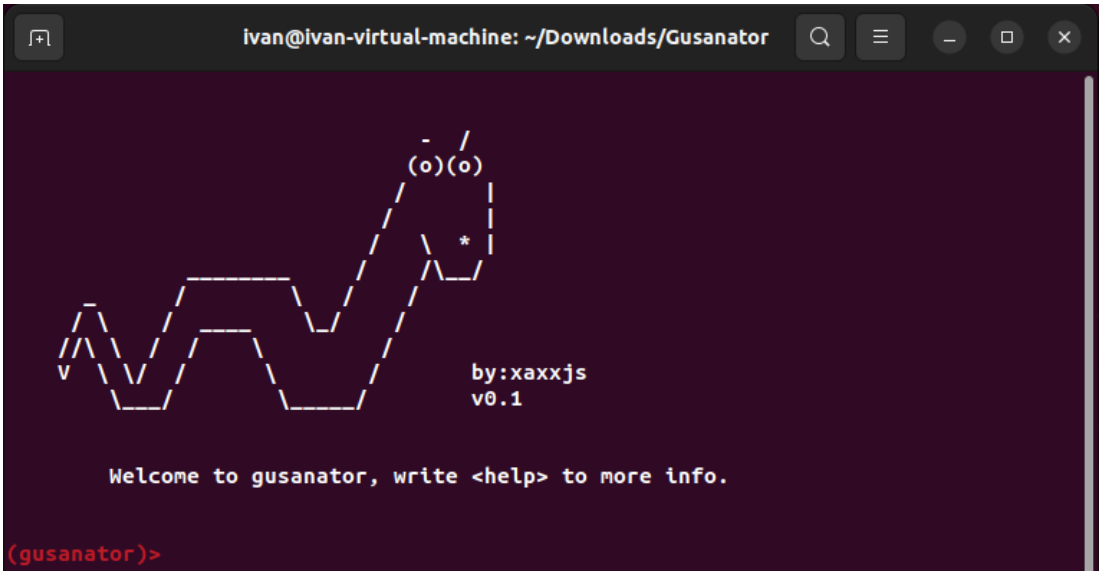
Anexo 57 *Reparación automatica de Windows Server 2019*

```
ivan@ivan-virtual-machine:~$ cd Downloads/
ivan@ivan-virtual-machine:~/Downloads$ ls
ivan@ivan-virtual-machine:~/Downloads$ git clone https://github.com/sergioab7/Gusan
ator.git
Cloning into 'Gusanator'...
remote: Enumerating objects: 64, done.
remote: Counting objects: 100% (64/64), done.
remote: Compressing objects: 100% (56/56), done.
remote: Total 64 (delta 10), reused 47 (delta 4), pack-reused 0
Receiving objects: 100% (64/64), 2.10 MiB | 2.81 MiB/s, done.
Resolving deltas: 100% (10/10), done.
ivan@ivan-virtual-machine:~/Downloads$
```

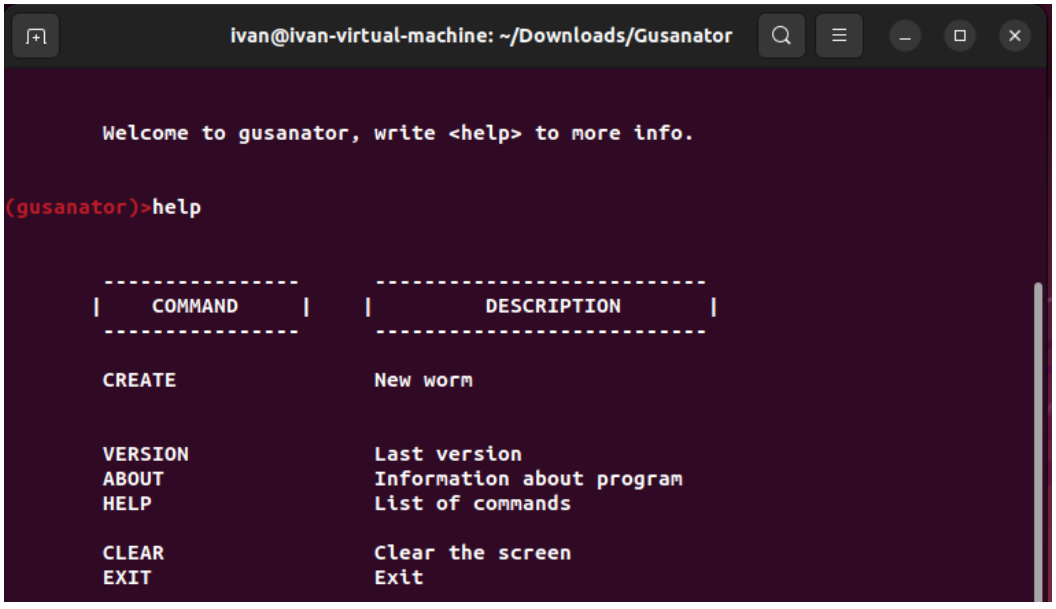
Anexo 58 *Infección de máquina virtual Ubuntu 22 con Gusanator*

```
ivan@ivan-virtual-machine:~/Downloads$ cd Gusanator/
ivan@ivan-virtual-machine:~/Downloads/Gusanator$ ls
gusanator.py  images  README.md
ivan@ivan-virtual-machine:~/Downloads/Gusanator$ python3 gusanator.py
```

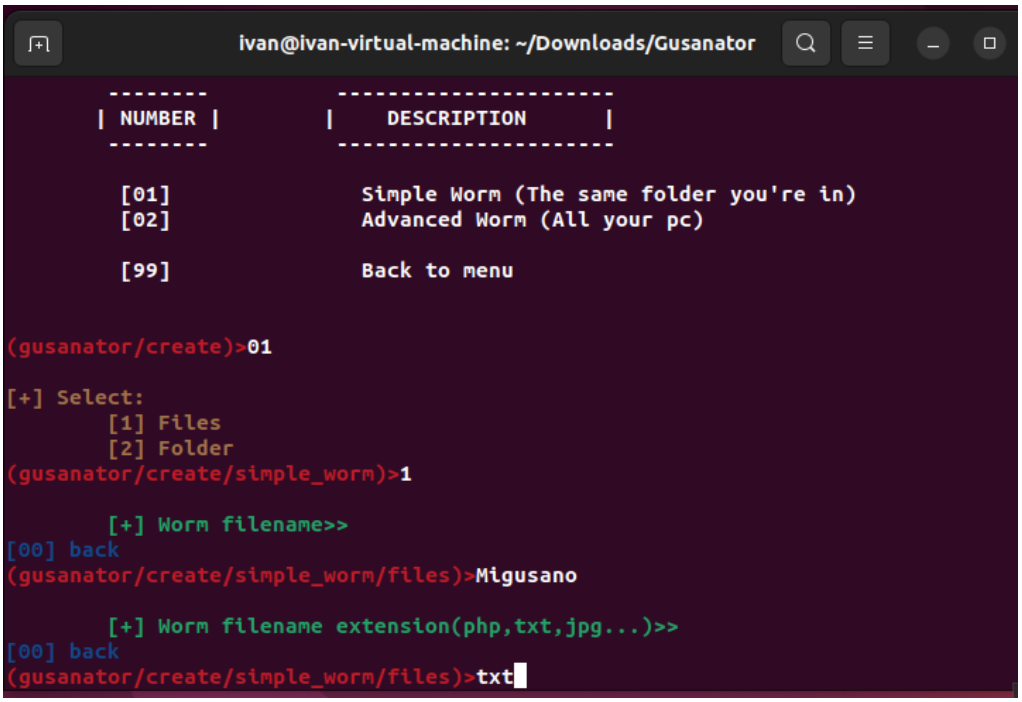
Anexo 59 *Ejecutar con python3 gusanator.py*



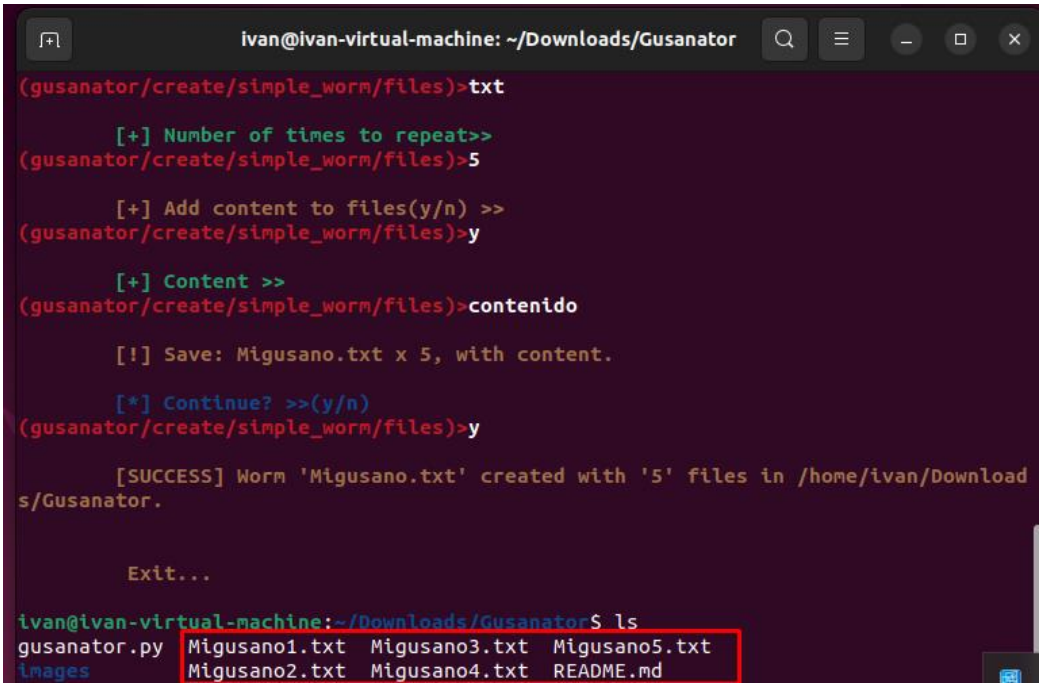
Anexo 60 *Ventana de inicio de Gusanator*



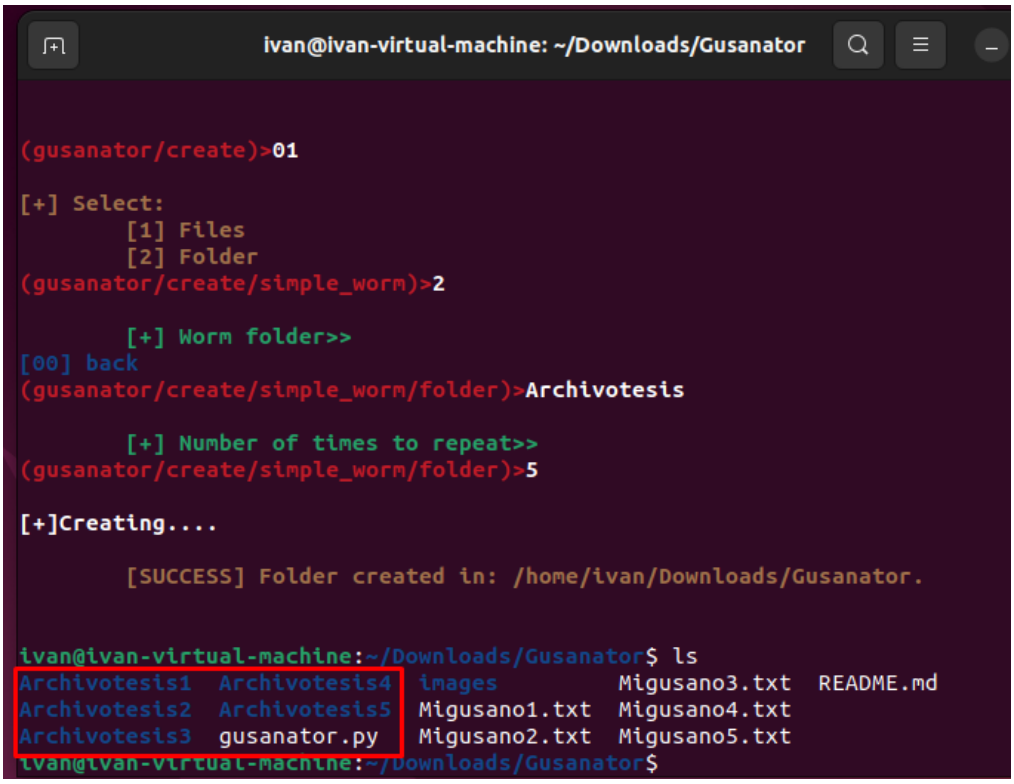
Anexo 61 *Menu de comandos Gusanator*



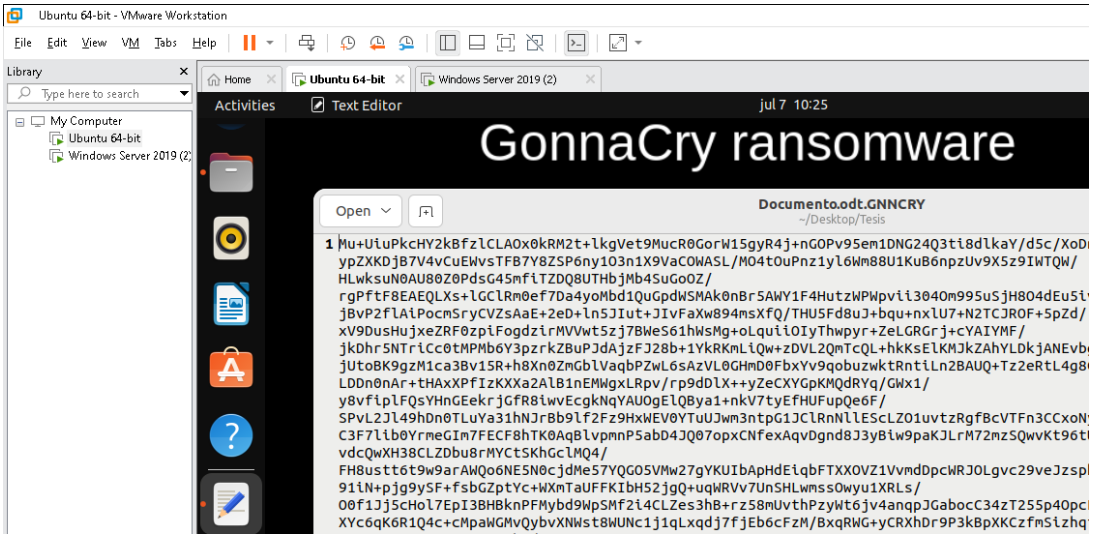
Anexo 62 *Comandos para crear archivos .txt*



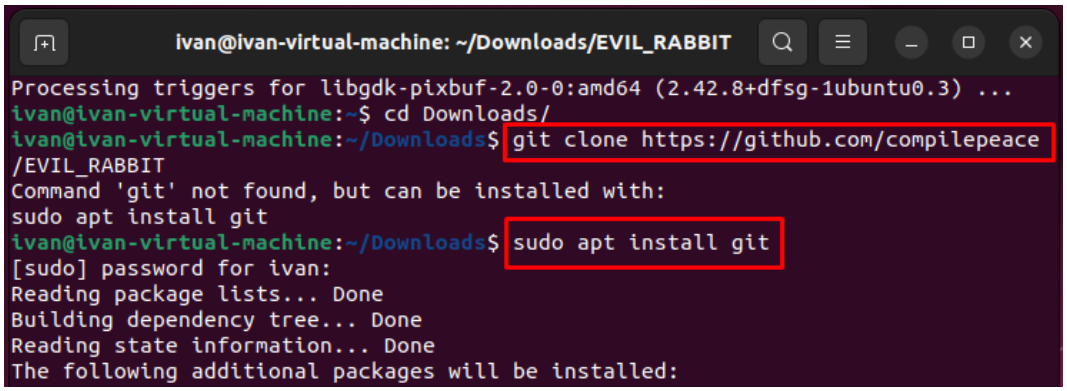
Anexo 63 *Archivos creados con Gusanator*



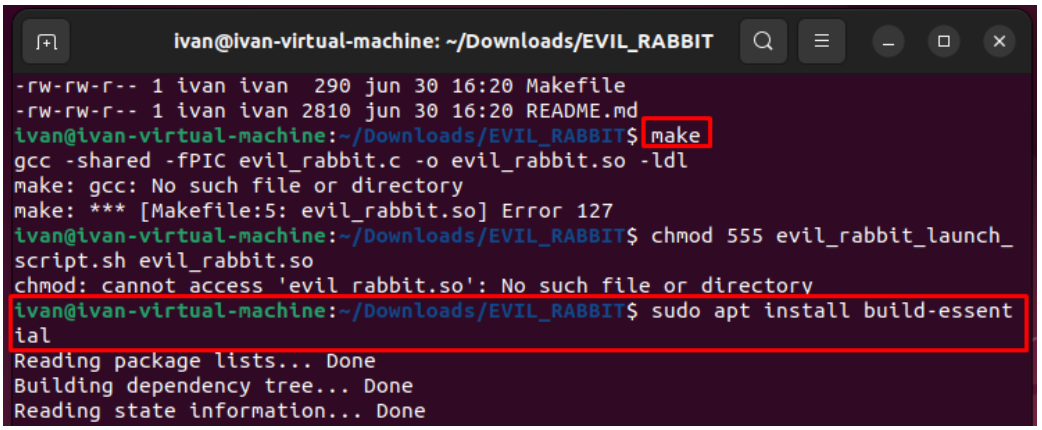
Anexo 64 *Directorios creados con Gusanator*



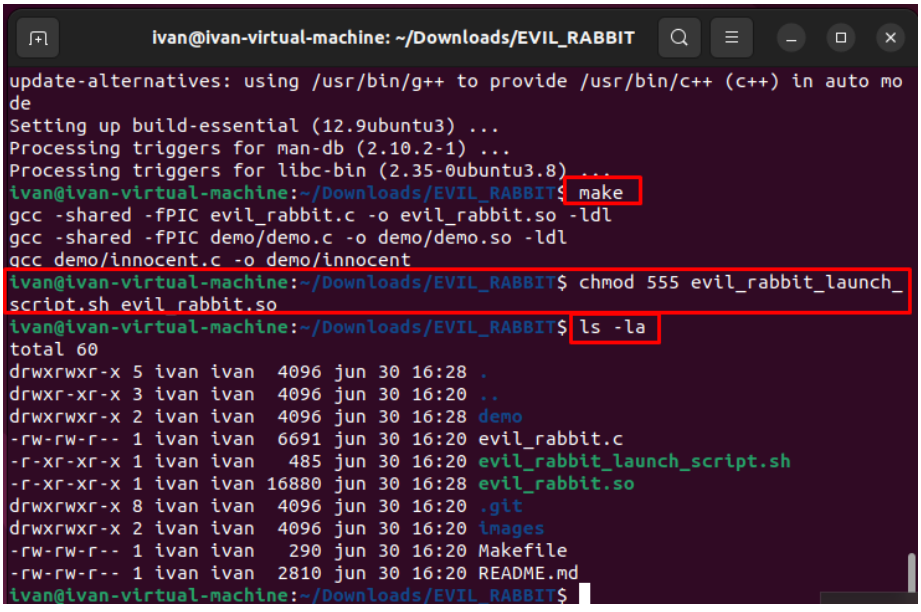
Anexo 65 *Infección con GonnaCry*



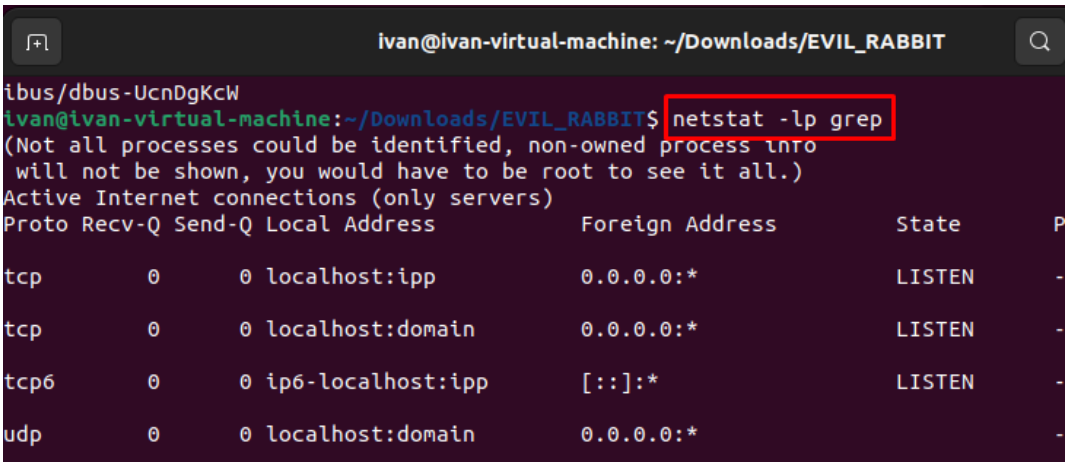
Anexo 66 *Comandos para descargar EvilRabit*



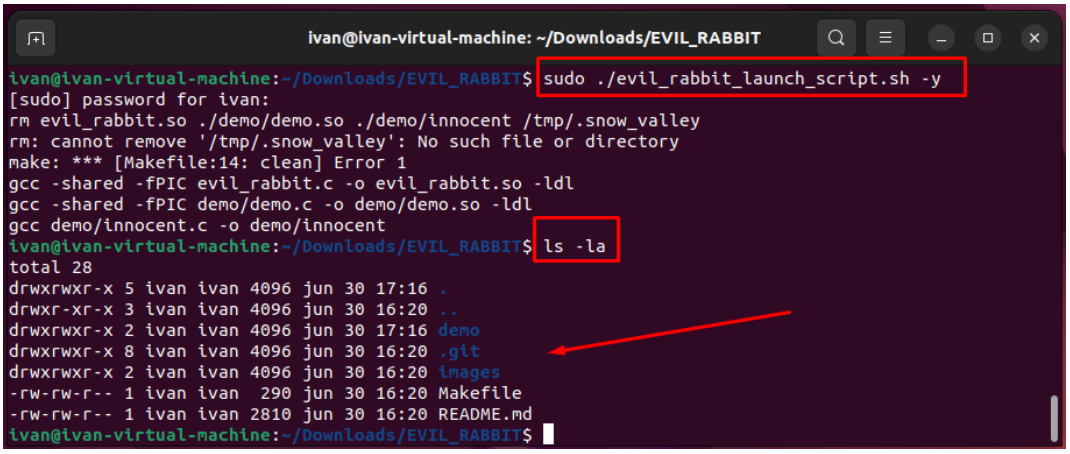
Anexo 67 *Complementos que necesita el comando make*



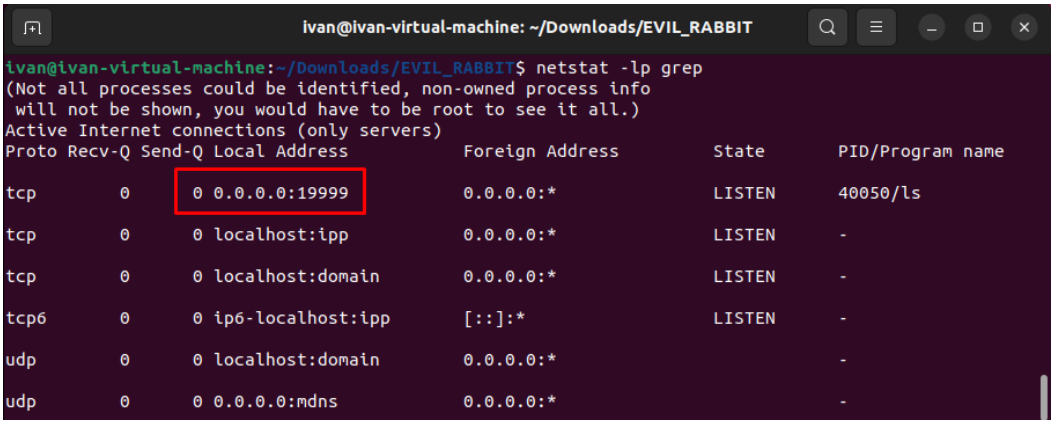
Anexo 68 *Instalación y permisos para make*



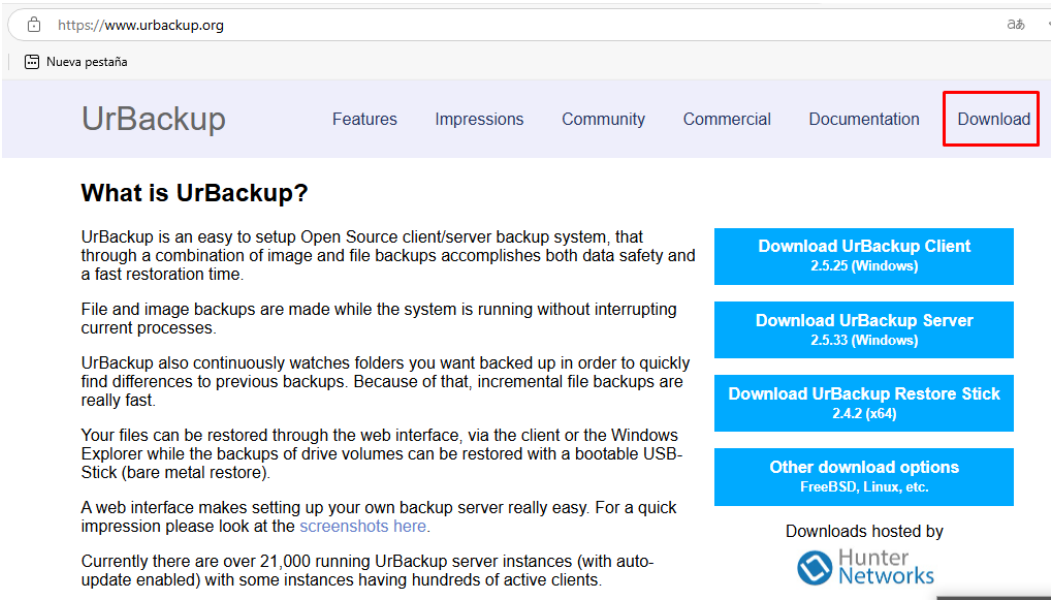
Anexo 69 *Local Host actual en Ubuntu 22*



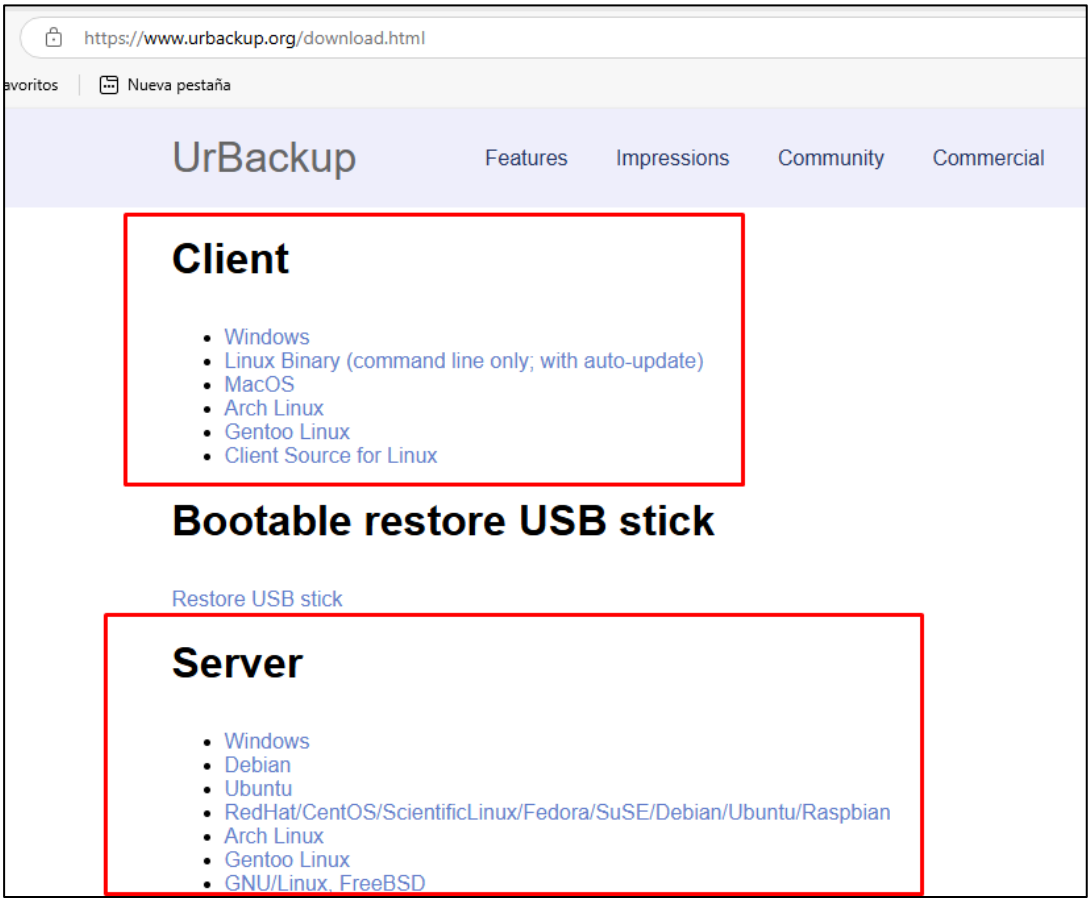
Anexo 70 *Ejecución de Evil_Rabbit*



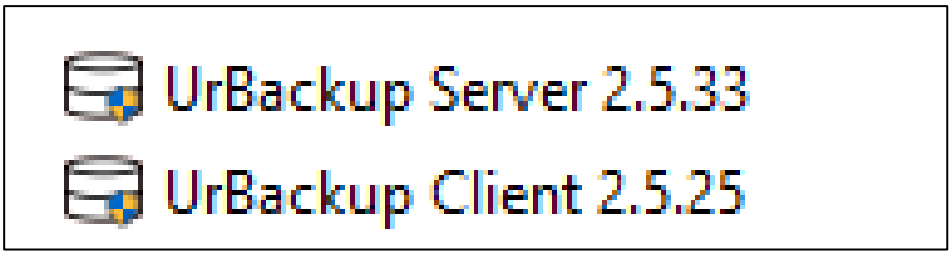
Anexo 71 *Puerto habilitado del atacante usando Evil Rabbit*



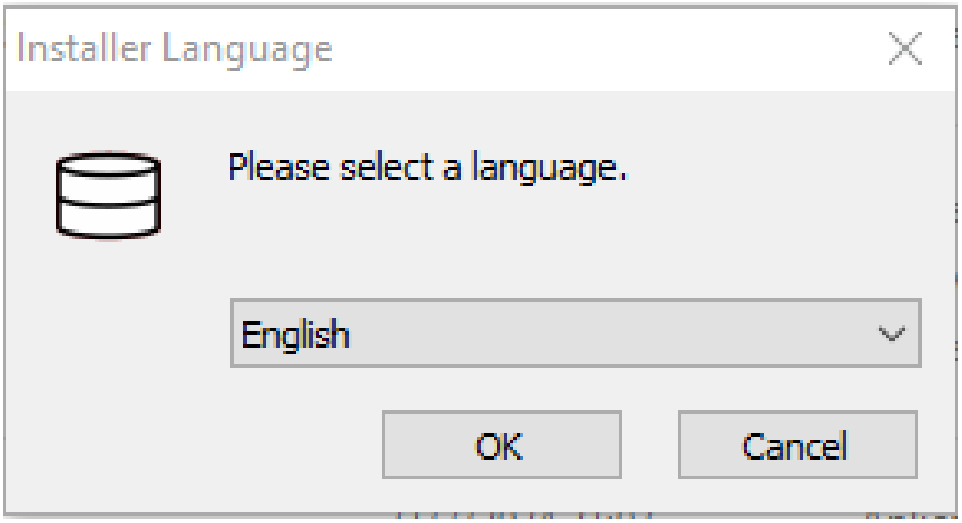
Anexo 72 *Página Oficial UrBackup*



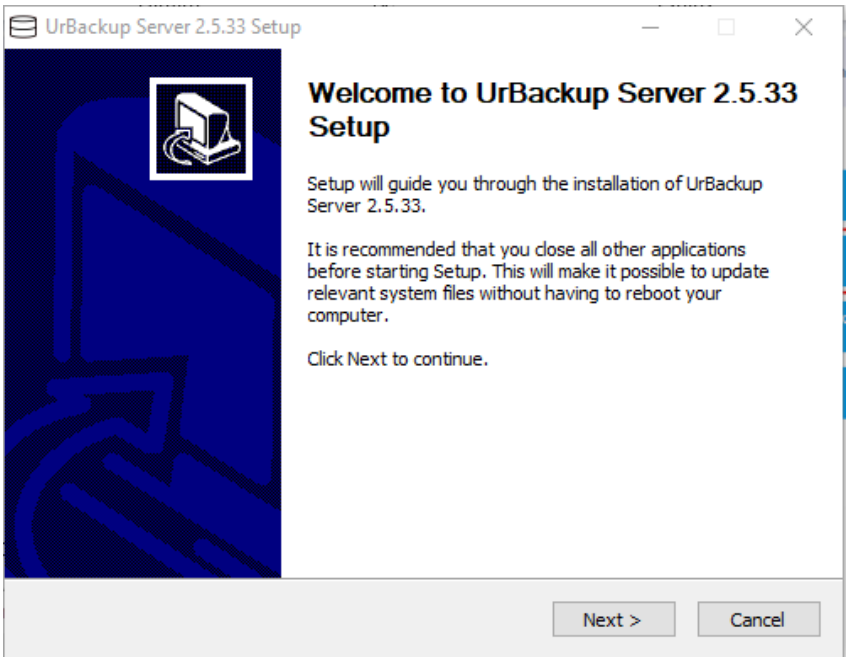
Anexo 73 *Descarga de Servidor y Cliente de UrBackup*



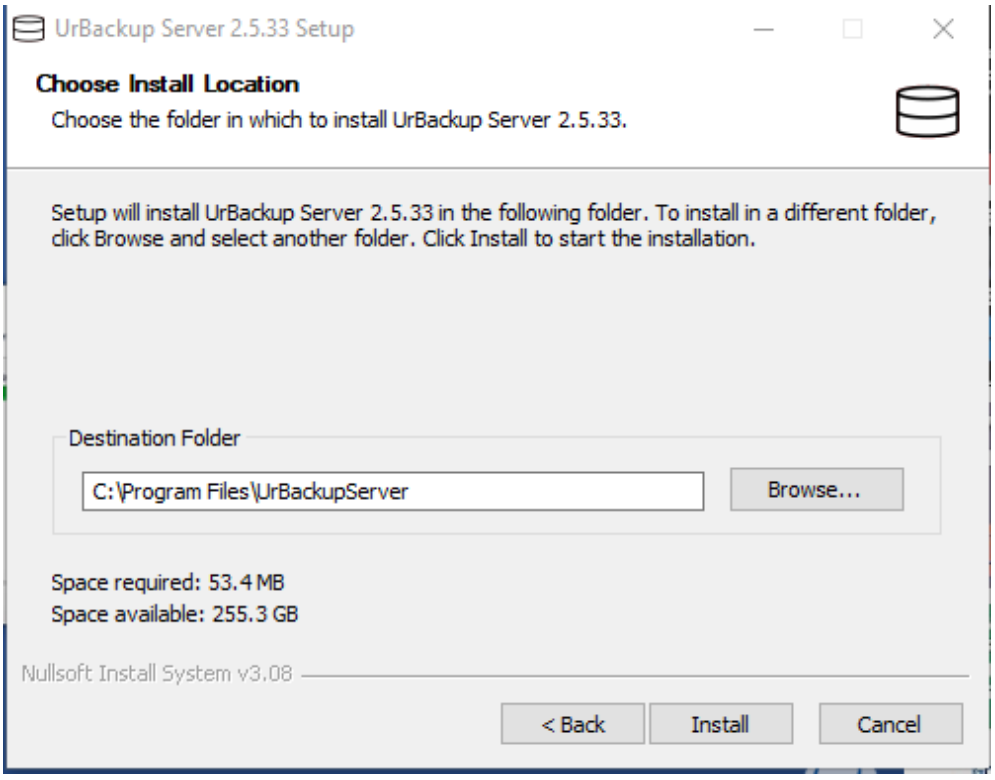
Anexo 74 Instalador Servidor y Cliente UrBackup



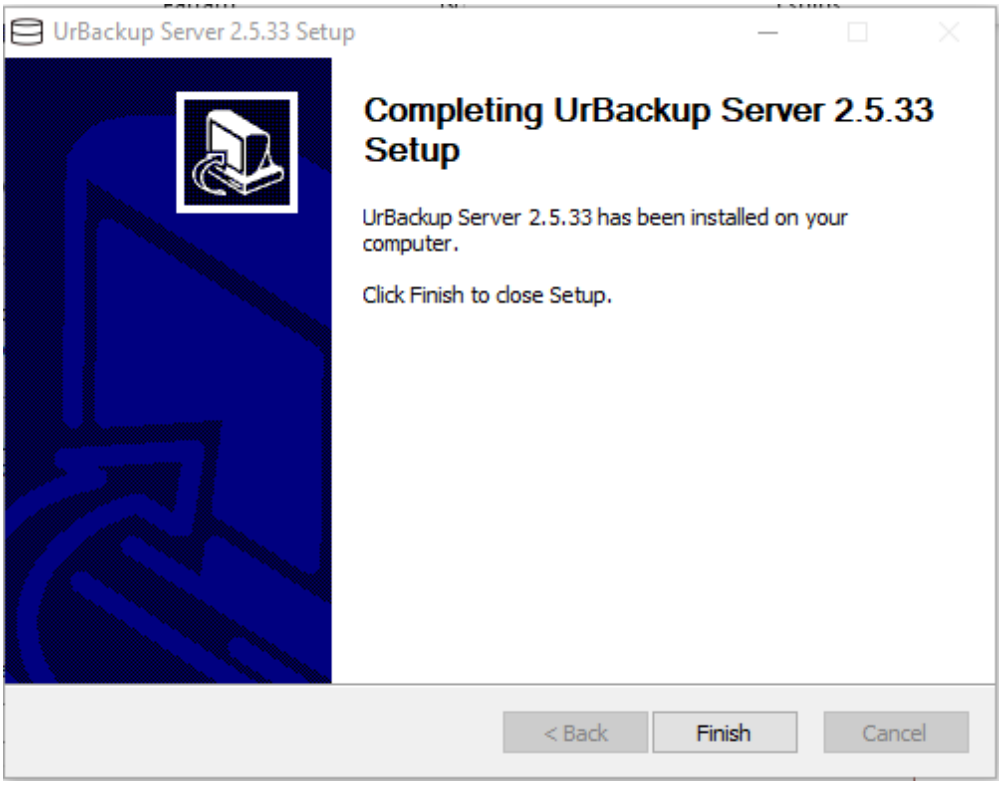
Anexo 75 *Instalación del idioma*



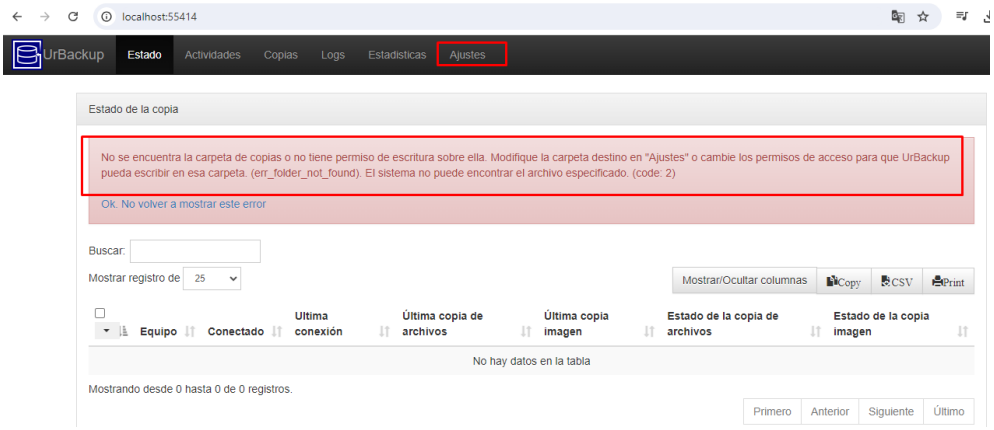
Anexo 76 *Ventana de bienvenido al servidor de UrBackup Server*



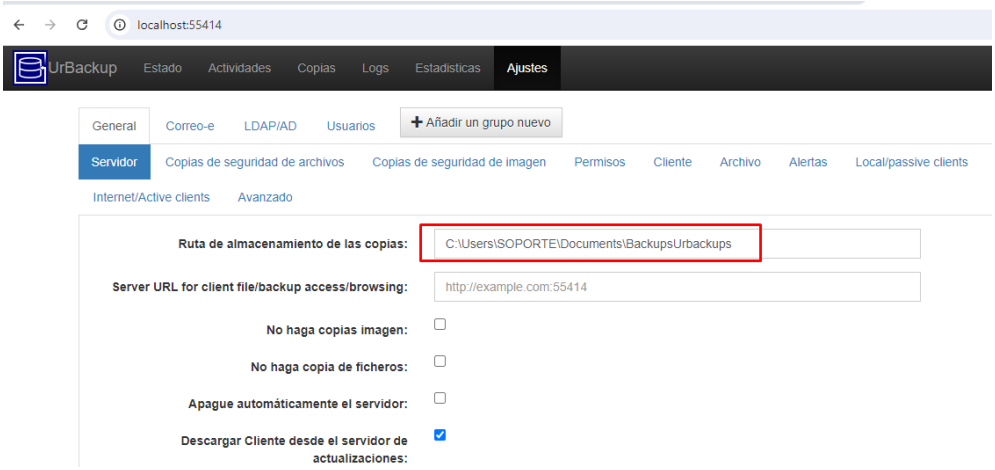
Anexo 77 *Selección de carpeta donde se instalará UrBackup Server*



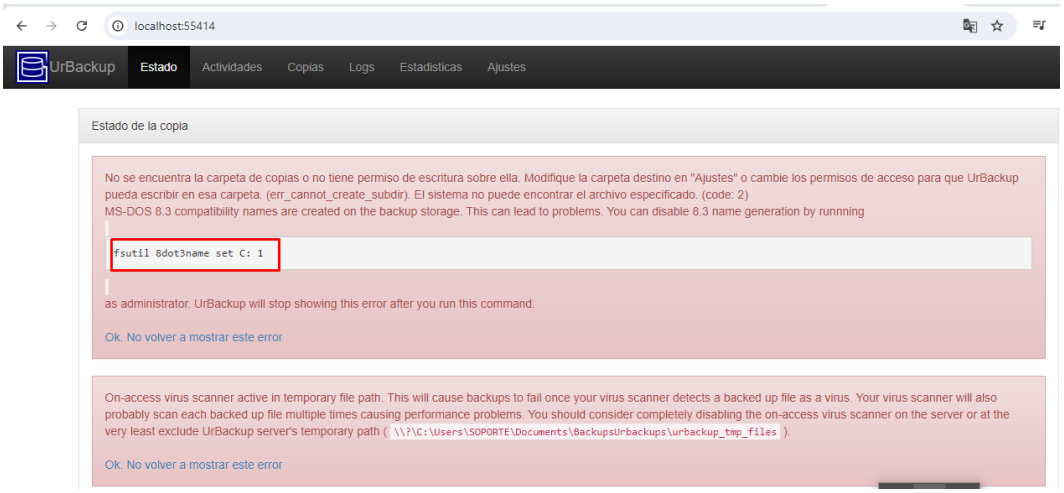
Anexo 78 *Instalación completa de Urbackup Server*



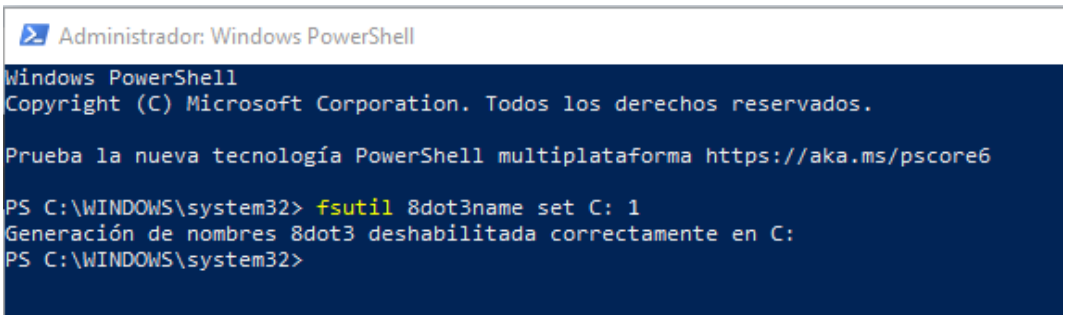
Anexo 79 *Configuración de UrBackup Server clic en ajustes*



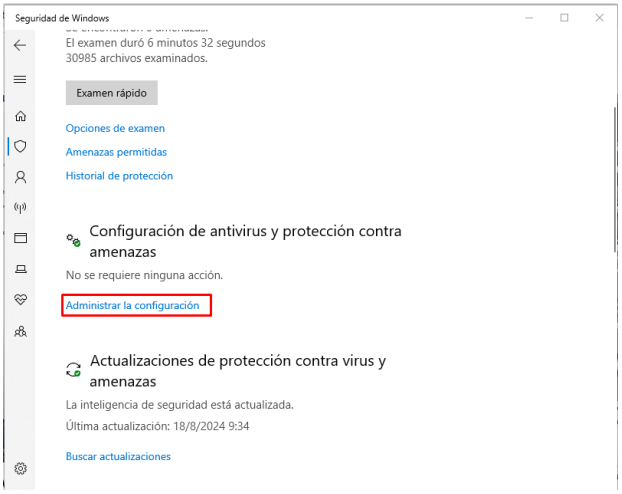
Anexo 80 *Agregar ruta de almacenamiento de las copias de seguridad*



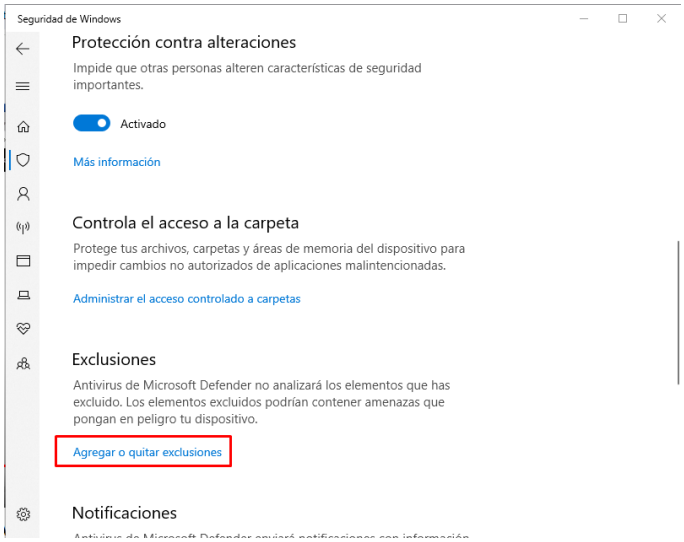
Anexo 81 *Errores a corregir de UrBackup Server*



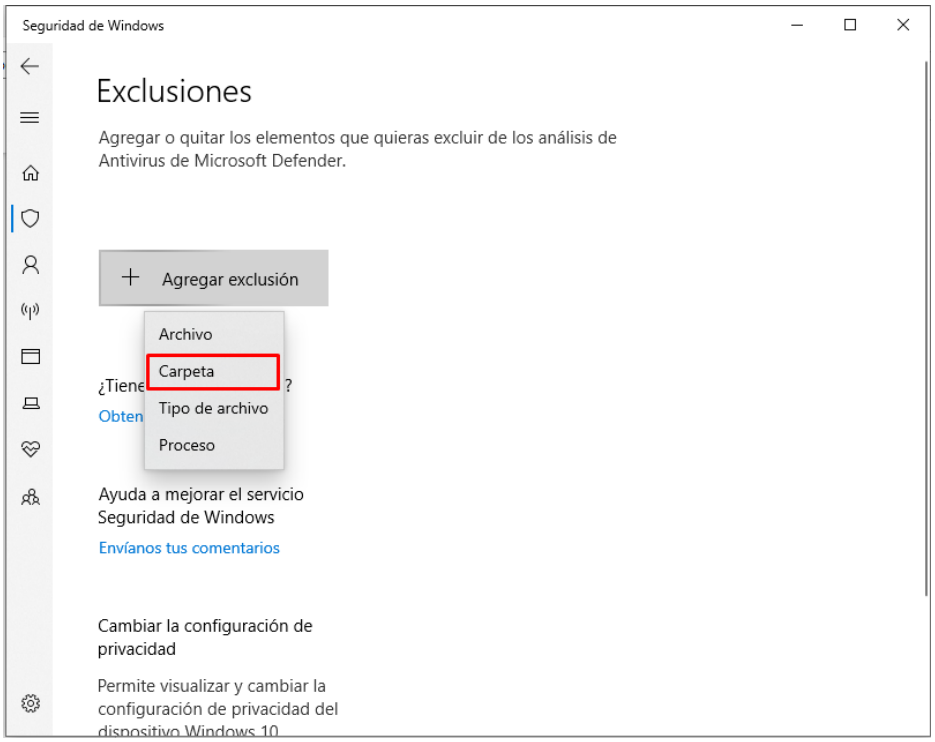
Anexo 82 *Permisos en la carpeta donde se guarda los respaldos PowerShell*



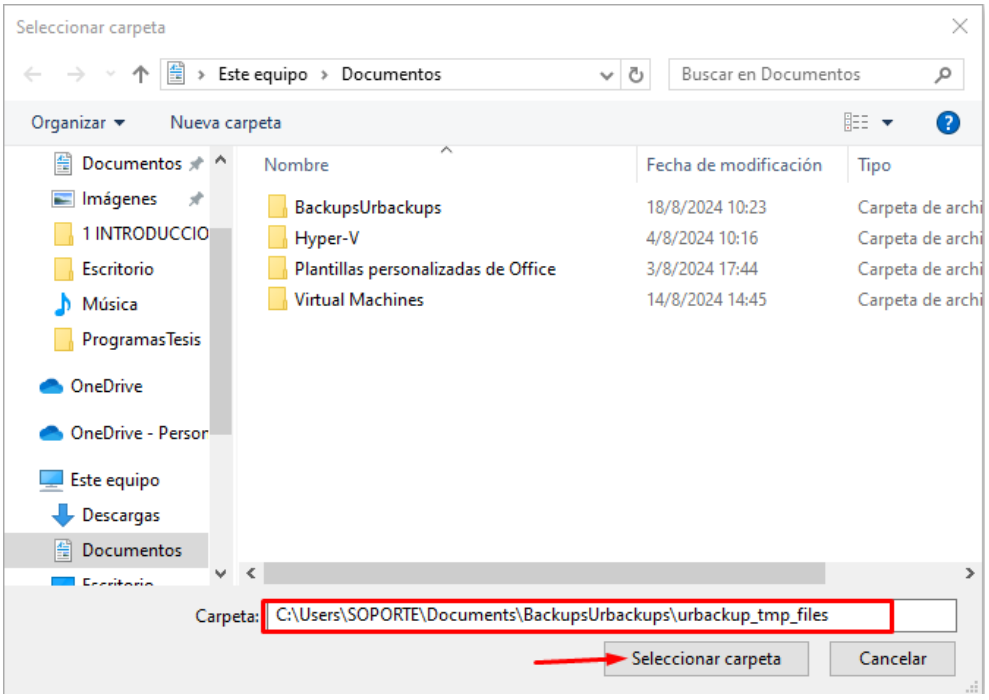
Anexo 83 *Ventana Seguridad de Windows, Administrar la configuración*



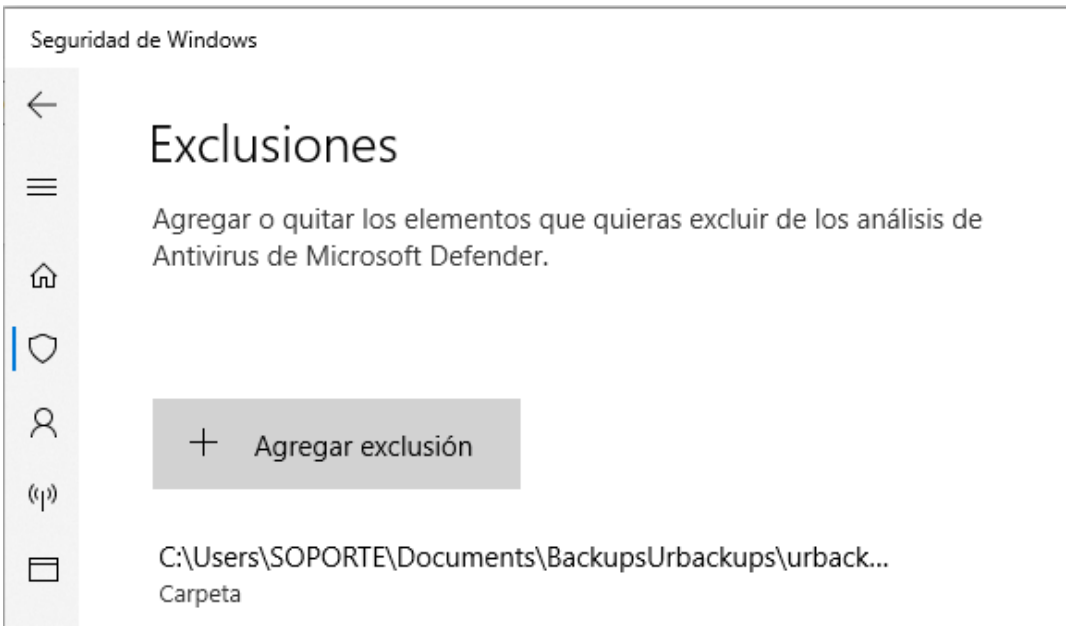
Anexo 84 *Agregar o quitar exclusiones*



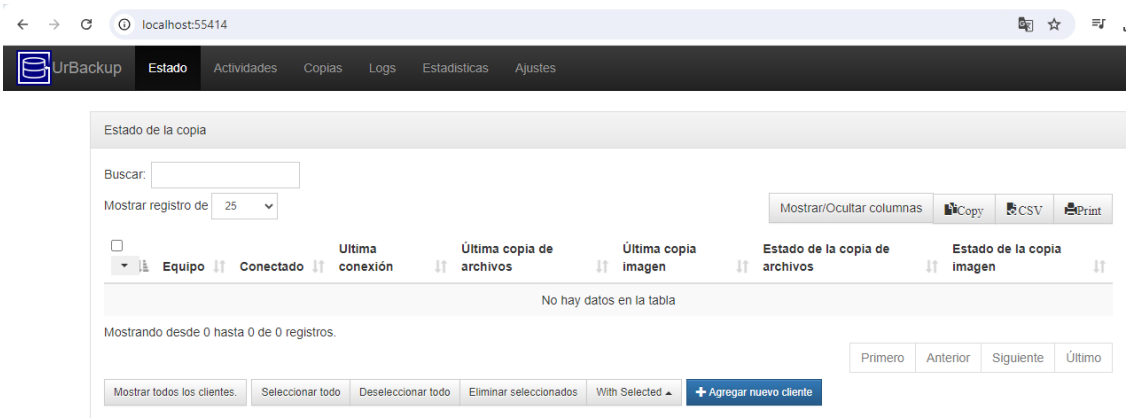
Anexo 85 *Exclusiones clic en Agregar exclusión*



Anexo 86 *Ubicación de la carpeta de respaldos*

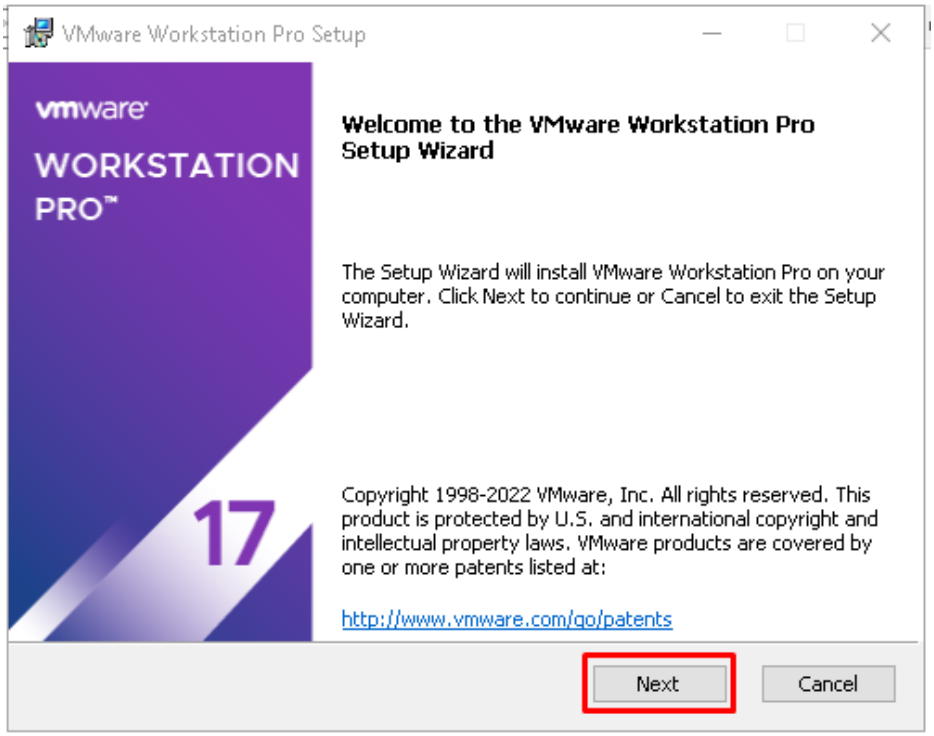


Anexo 87 *Carpeta agregada en exclusión*



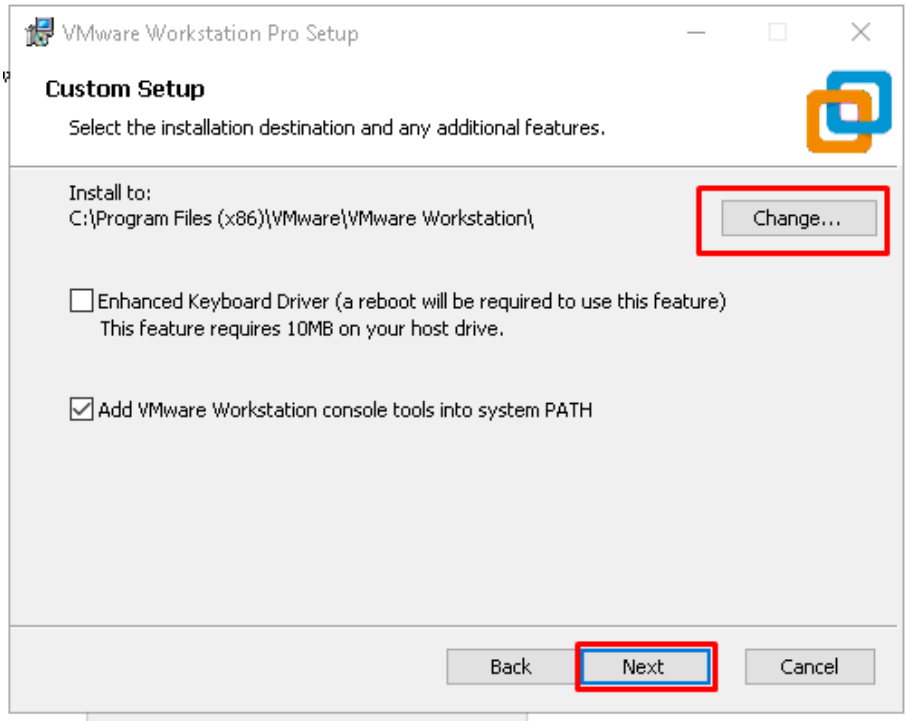
Anexo 88 *Instalación completa UrBackup Server*

Anexo 89 *Descarga de VMware Workstation 17 Pro for Windows*

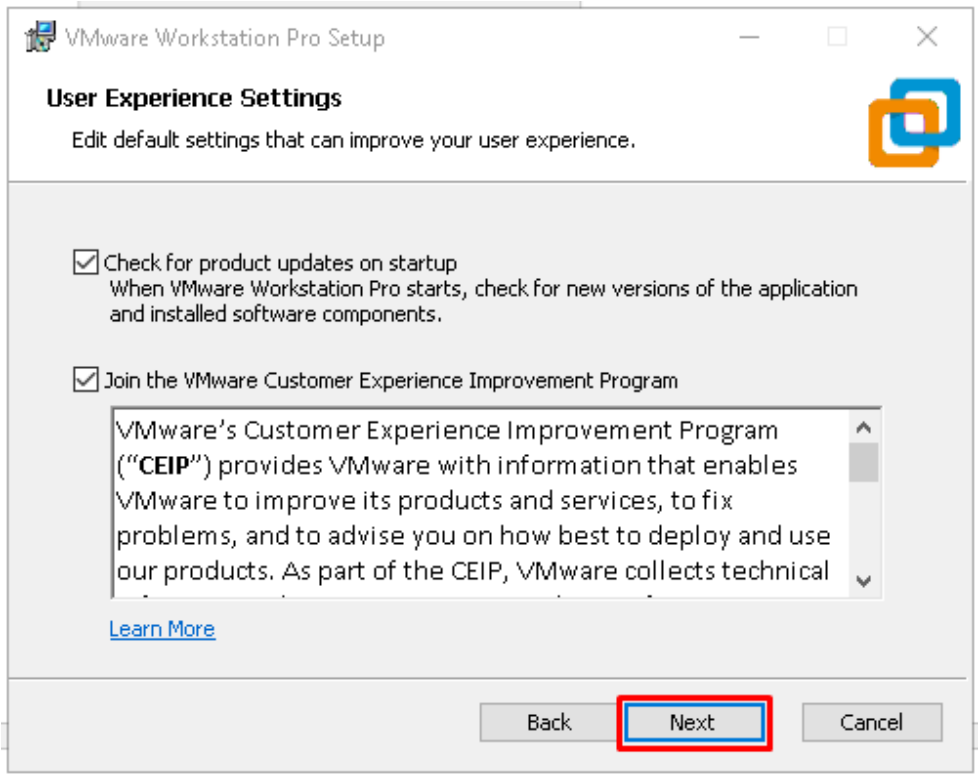


Anexo 90 *Inicio del instalador de VMware Workstation Pro 17*

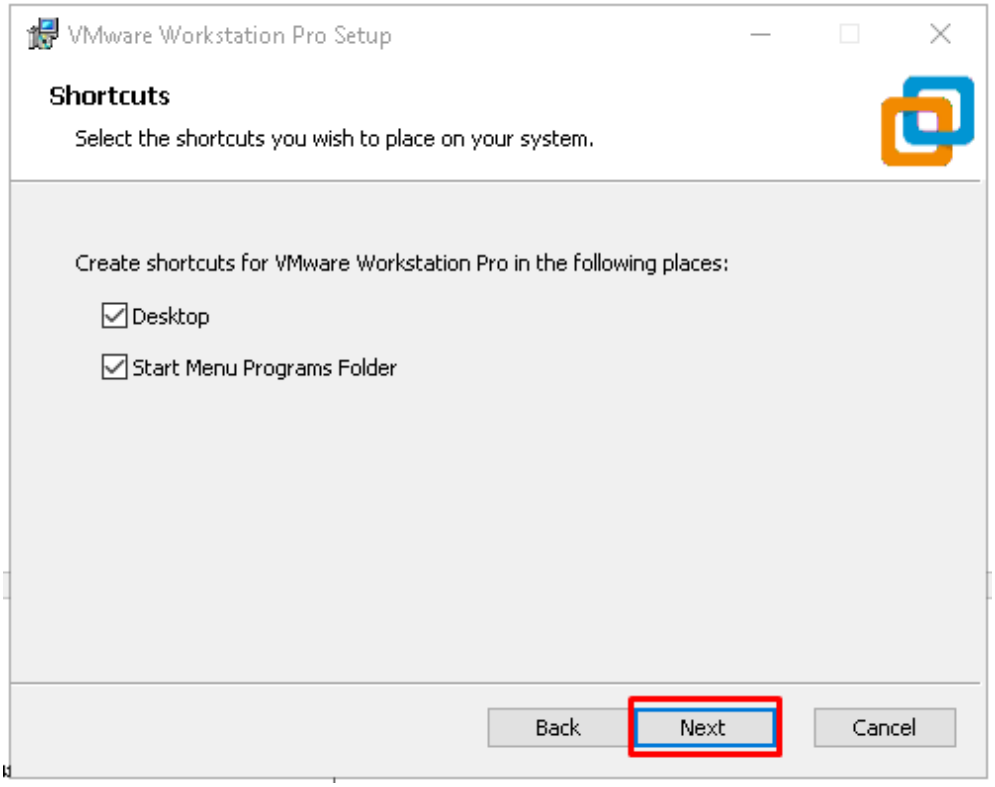
Anexo 91 *Acepto los términos de licencia VMware Workstation Pro Setup*



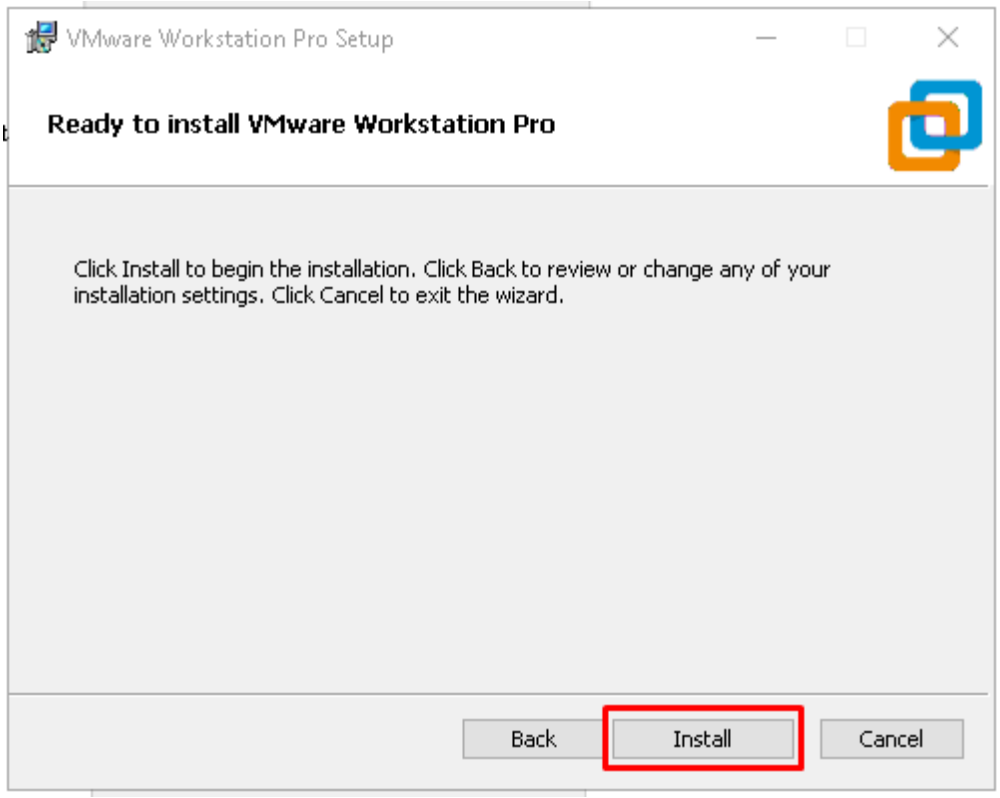
Anexo 92 *Habilitar el PATH en VMware Workstation Pro Setup*



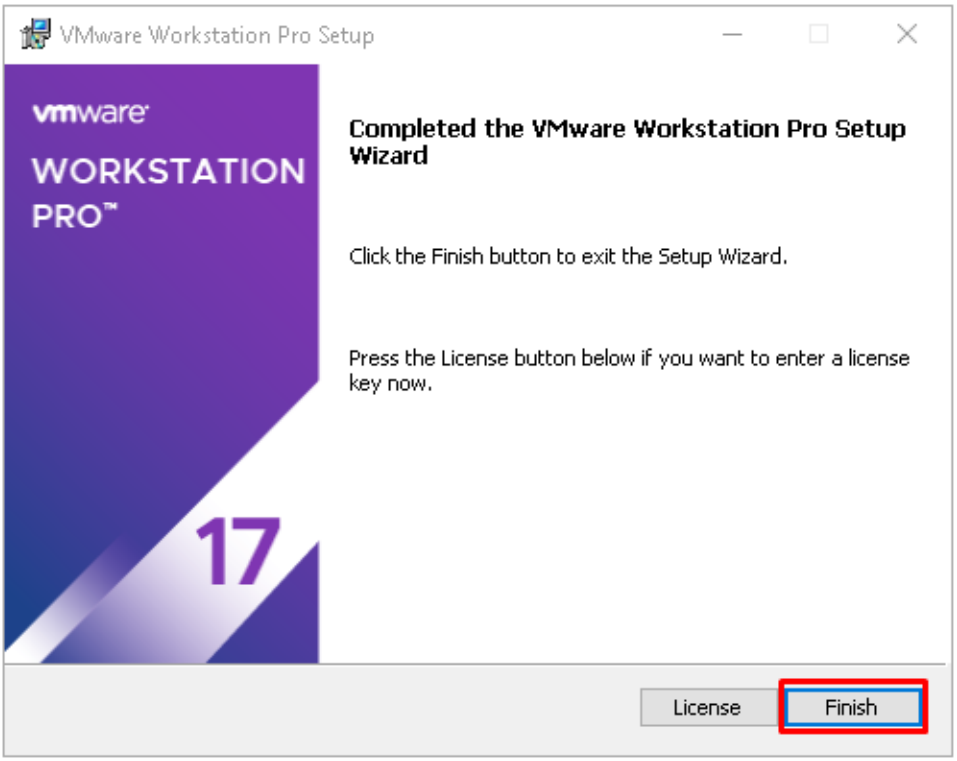
Anexo 93 *Configuración de experiencia del usuario VMware Workstation*



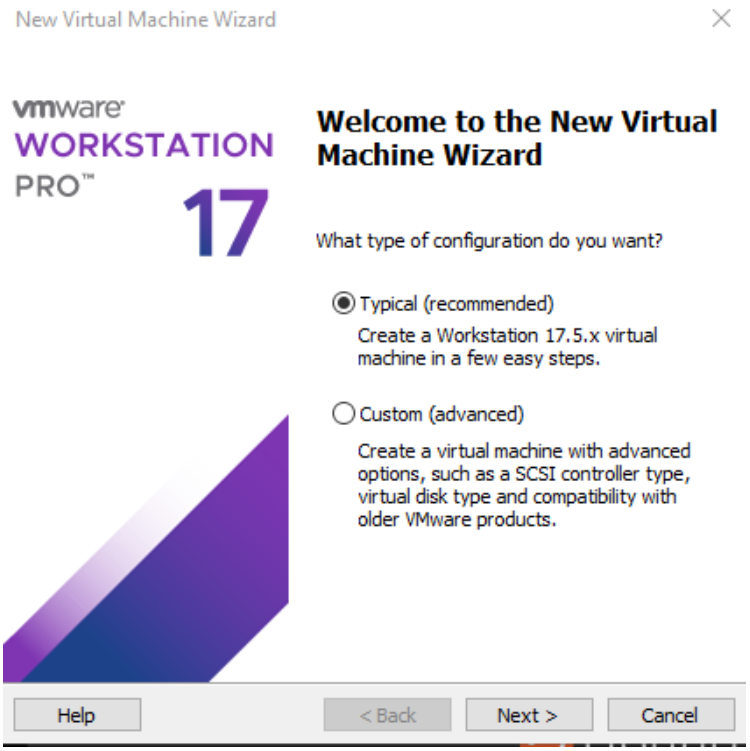
Anexo 94 *Configuración de los accesos directos en VMware Workstation Pro*



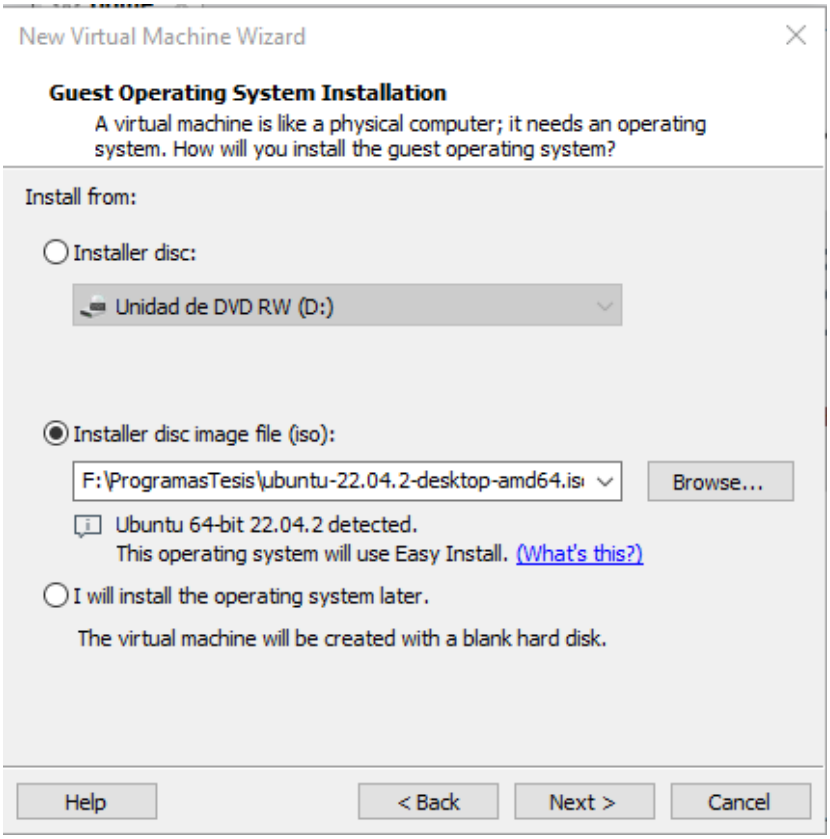
Anexo 95 *Botón de instalación de VMware Workstation Pro*



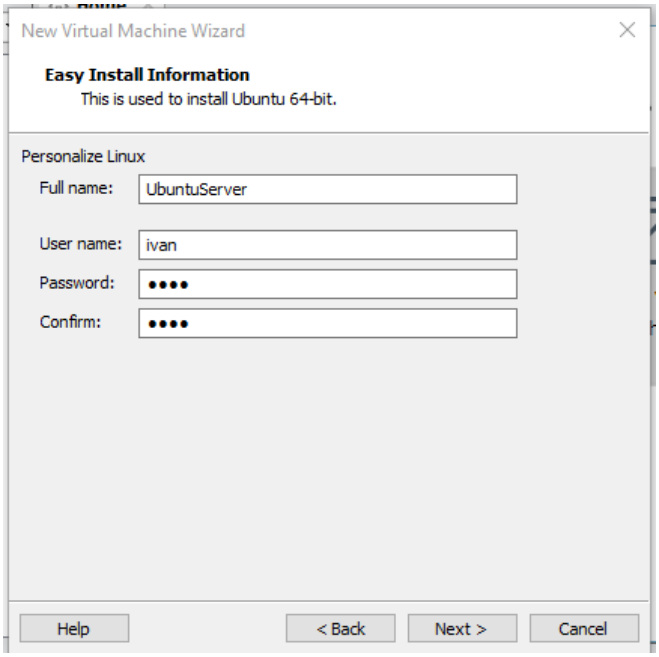
Anexo 96 *Finalización de la instalación de VMware - Elaboración propia.*



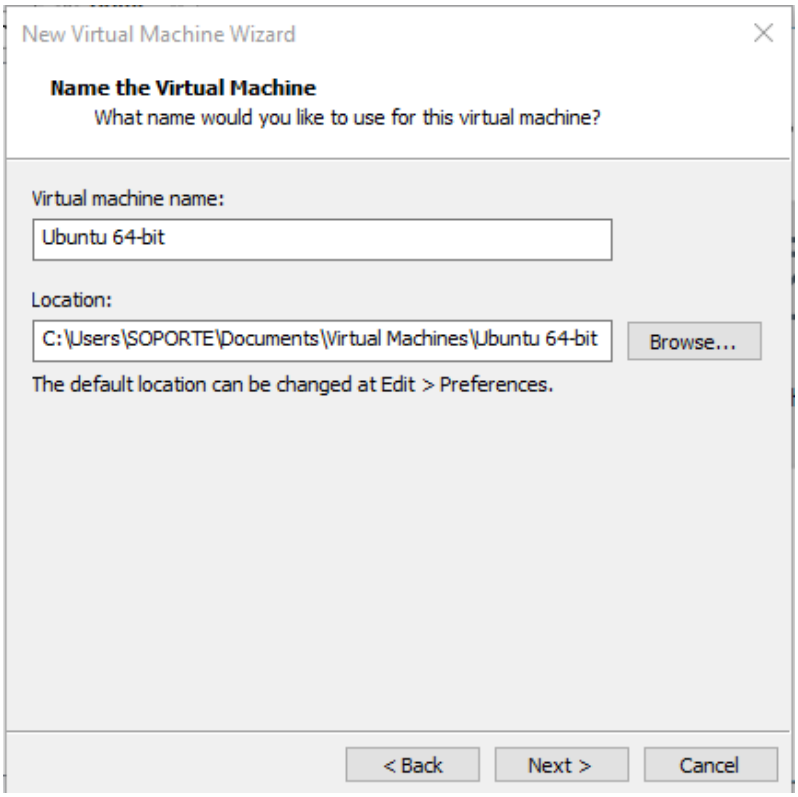
Anexo 97 *Instalación recomendada de asistente de máquina virtual*



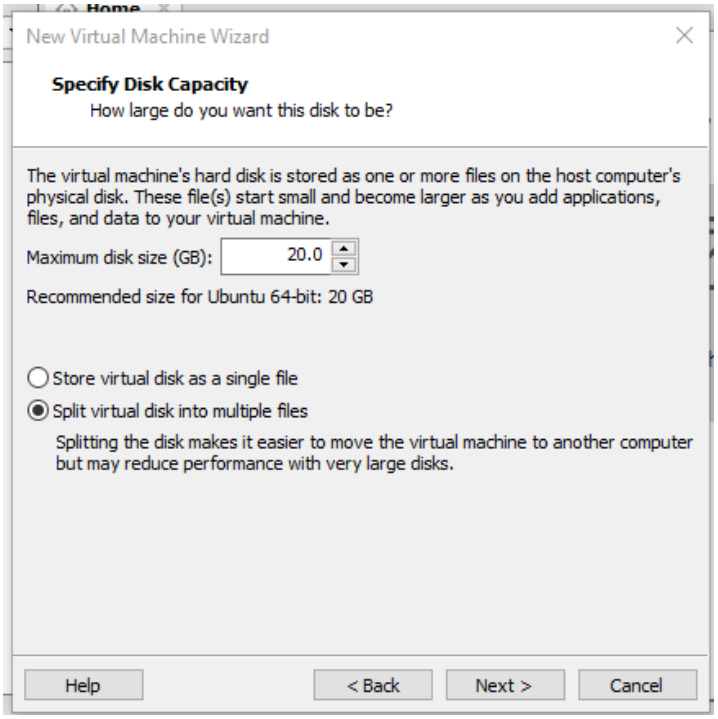
Anexo 98 *Ubicación de la imagen ISO Ubuntu 22*



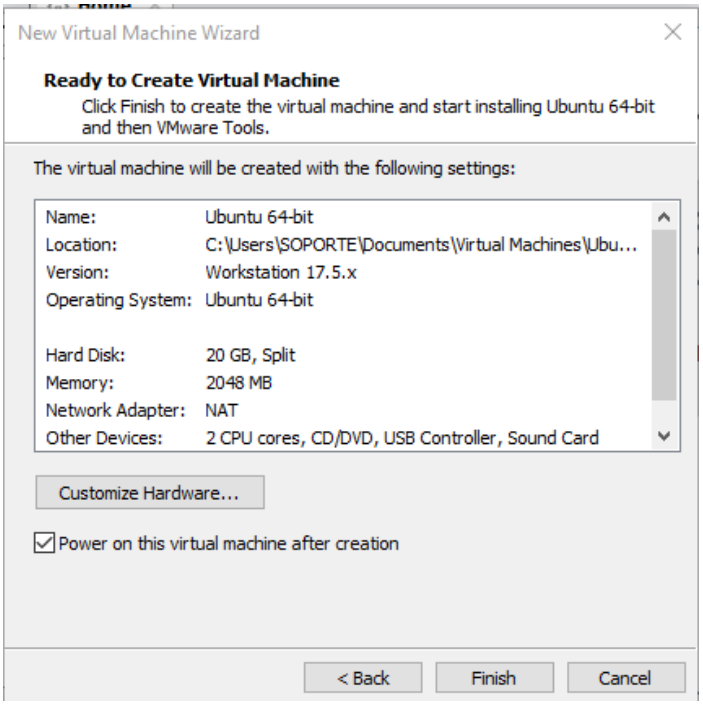
Anexo 99 *Nombre y usuario de Ubuntu 22*



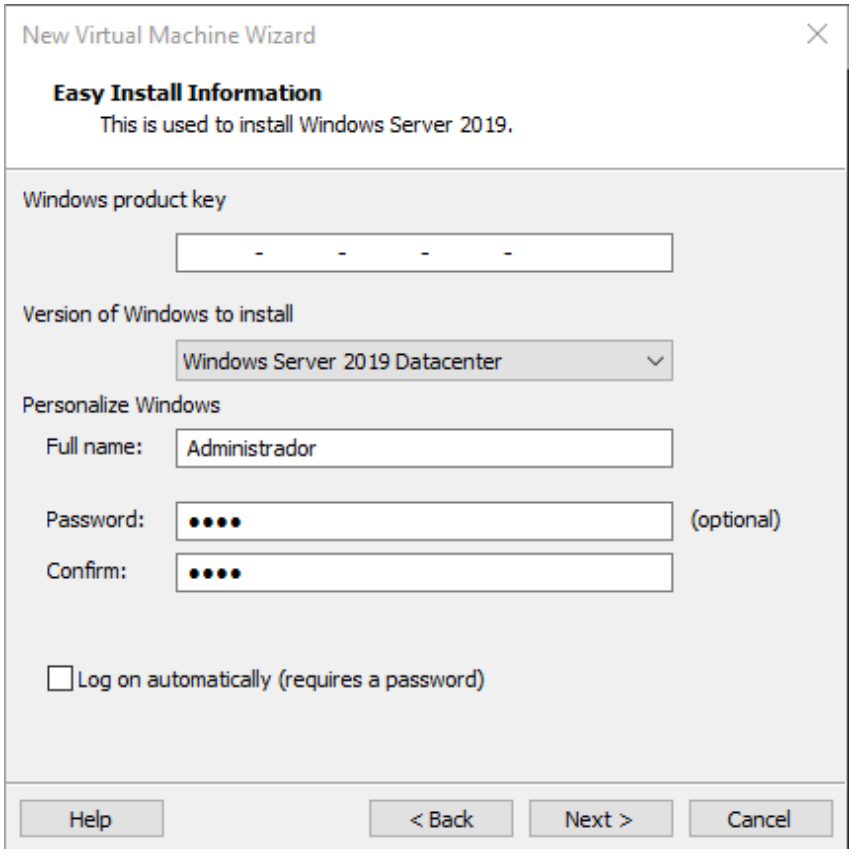
Anexo 100 *Asignar nombre a la máquina virtual*



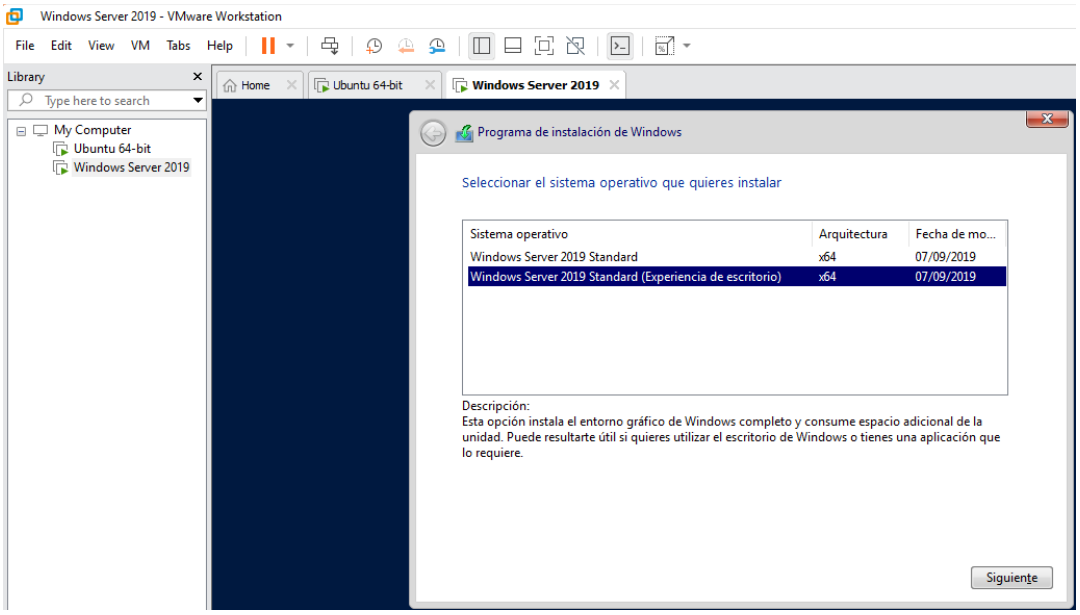
Anexo 101 *Tamaño de almacenamiento de la máquina virtual*



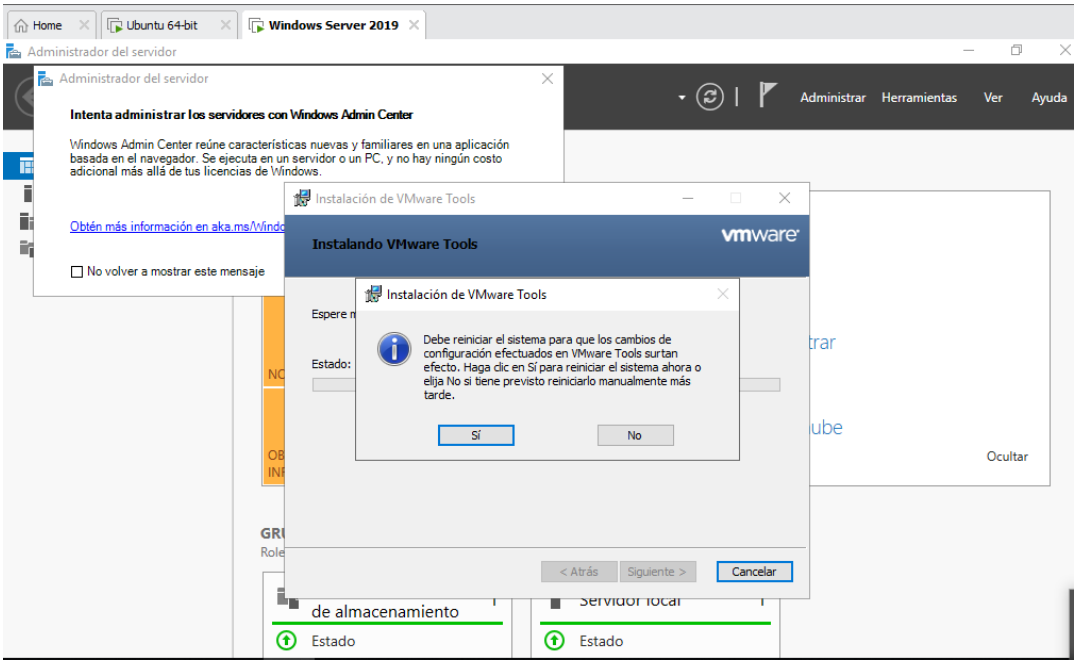
Anexo 102 *Verificar datos de la máquina virtual*



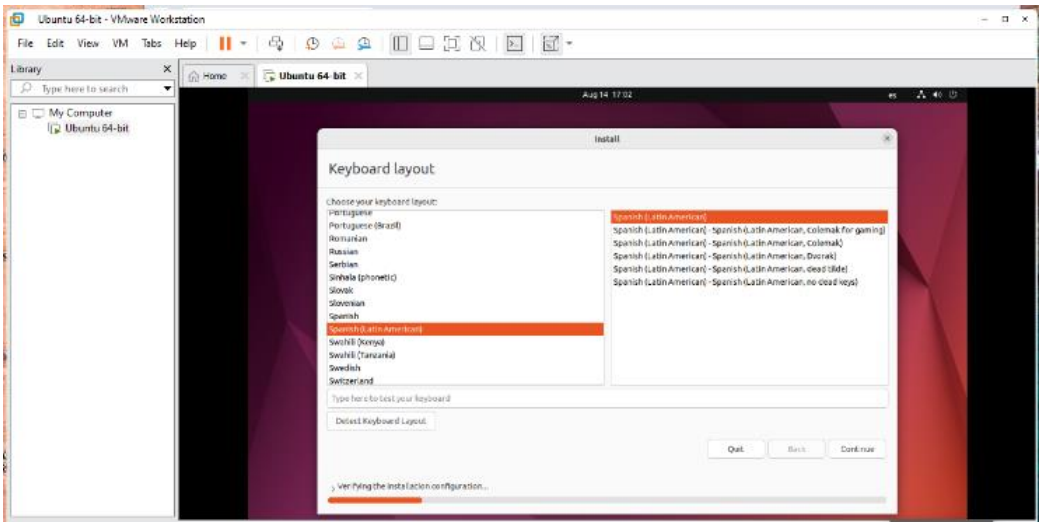
Anexo 103 *Ingreso de clave de producto Windows Server 2019*



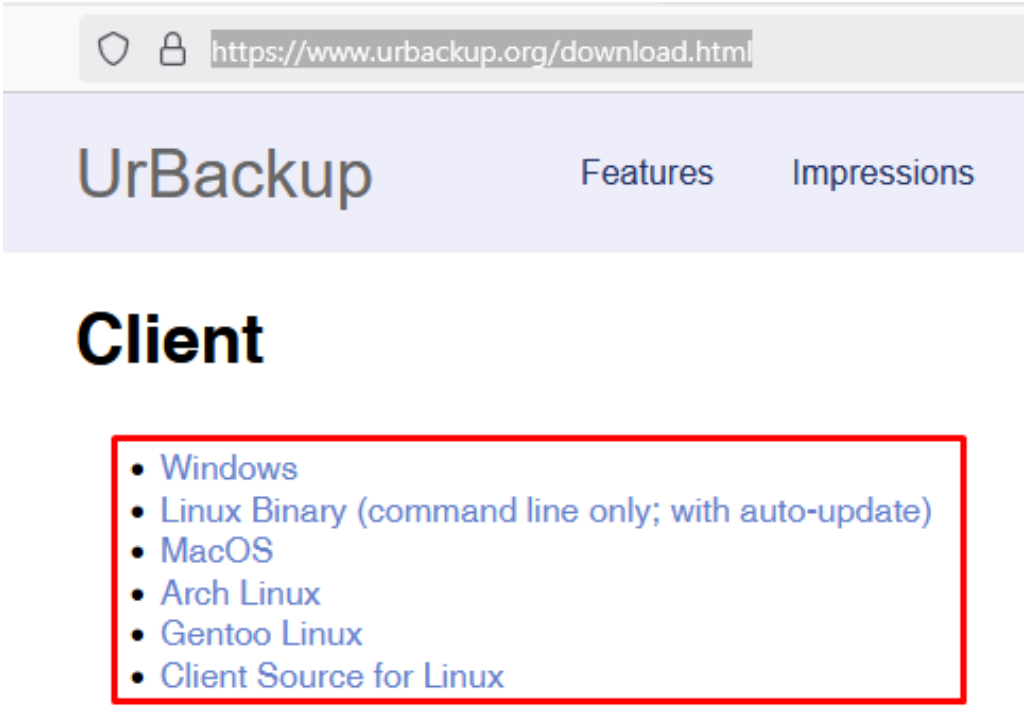
Anexo 104 *Inicio de instalación de Windows Server 2019*



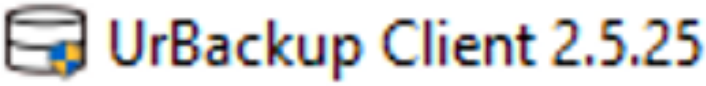
Anexo 105 *Instalación de VMware tools*



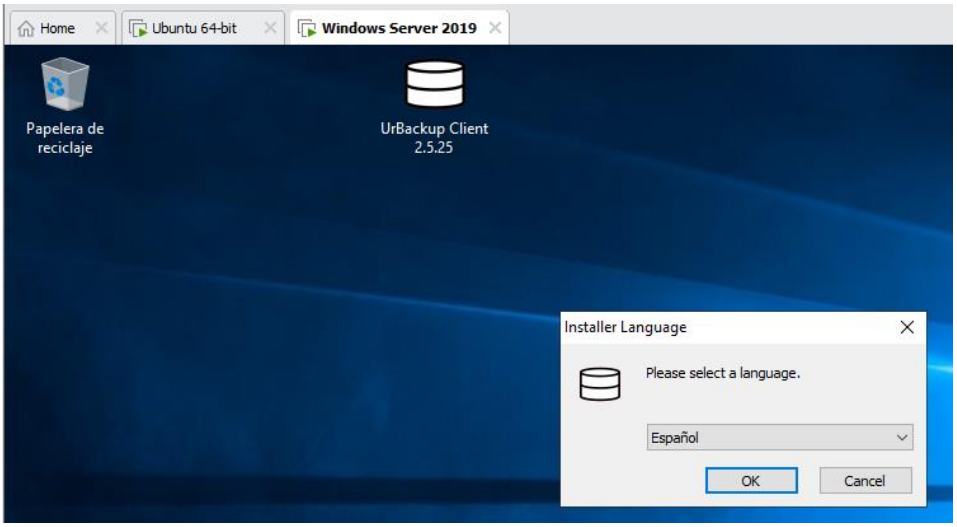
Anexo 106 *Selección de idioma Ubuntu 22*



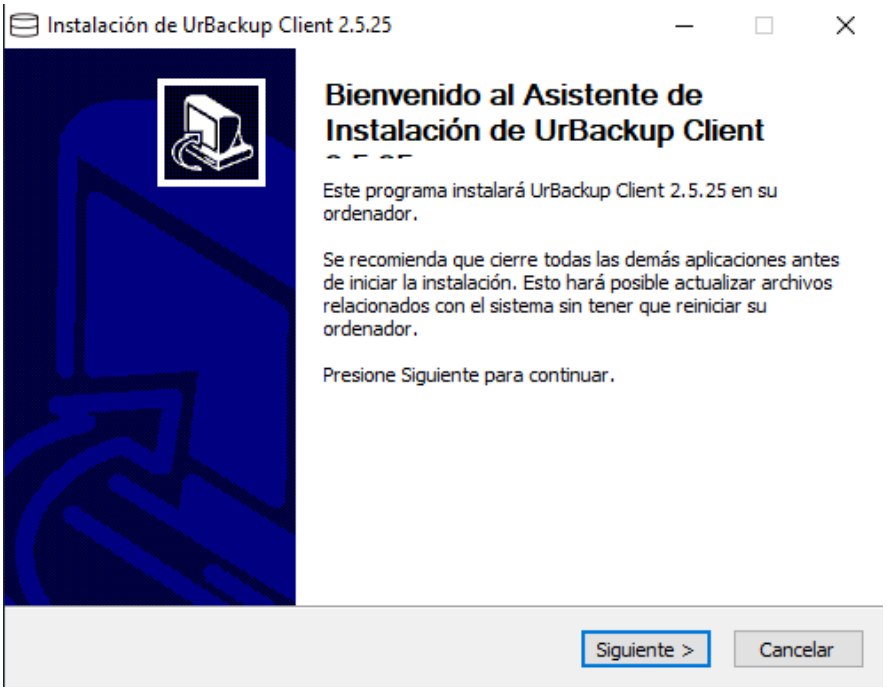
Anexo 107 *Descarga de UrBackup Cliente para Windows*



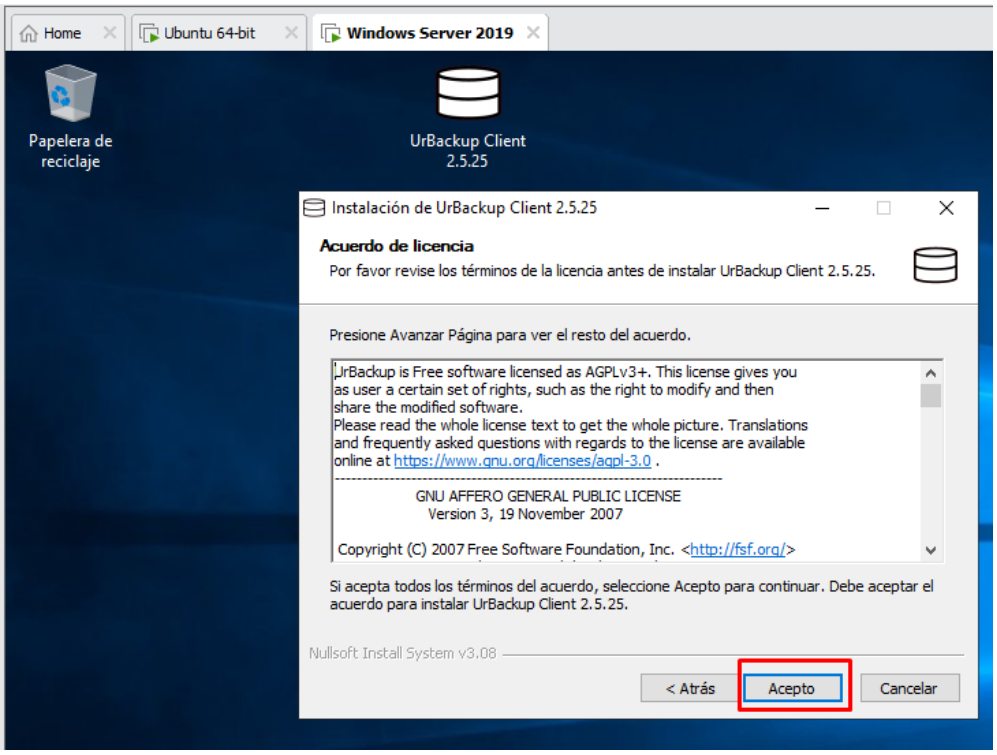
Anexo 108 *Instalador de UrBackup cliente*



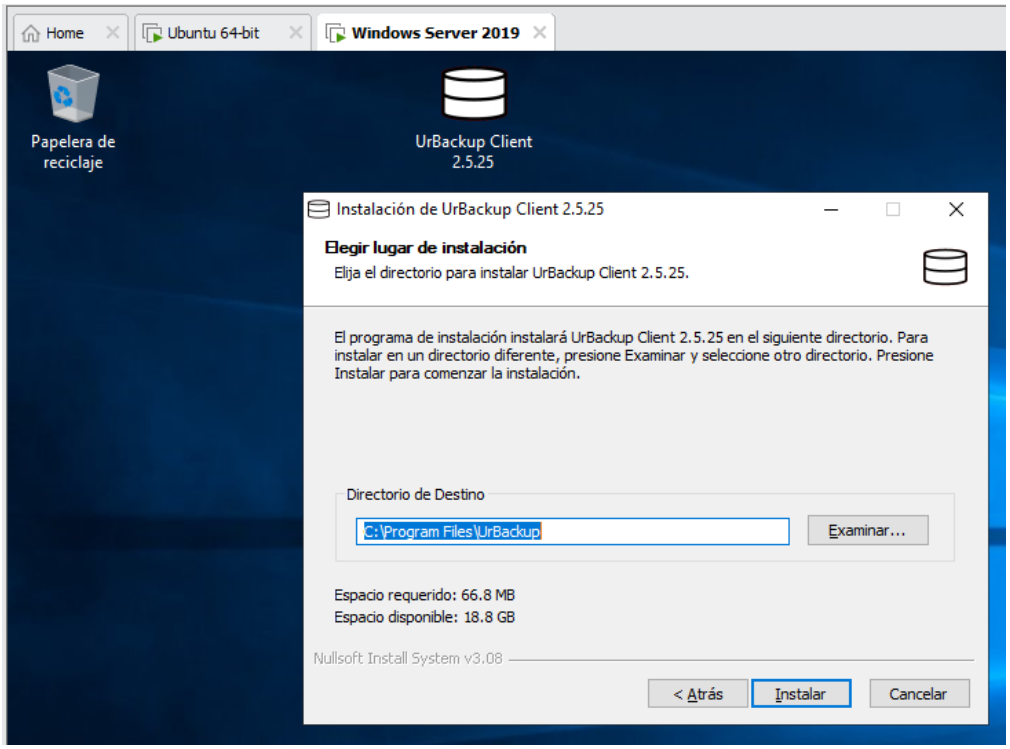
Anexo 109 *Selección del Idioma de UrBackup Cliente*



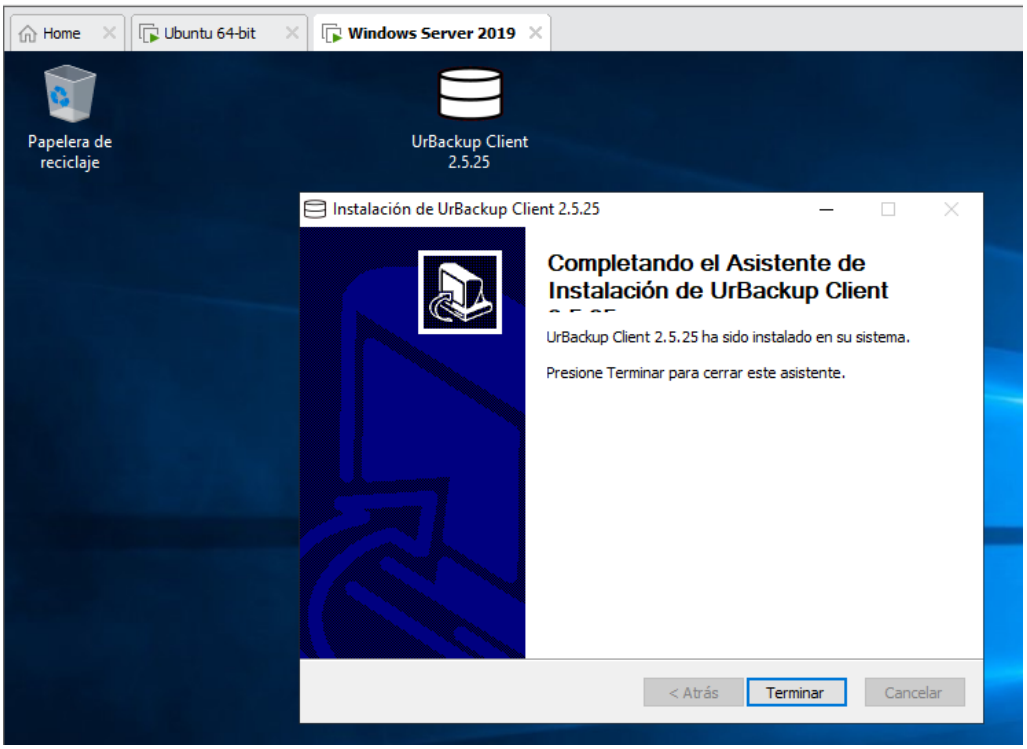
Anexo 110 *Bienvenido al asistente de instalación de UrBackup Cliente*



Anexo 111 *Acuerdo de licencia*



Anexo 112 *Elegir lugar de instalación*



Anexo 113 *Instalación finalizada del asistente de UrBackup Cliente*

```
root@ivan-virtual-machine:/home/ivan# apt install build-essential "g++" libwxgtk
3.0-gtk3-dev "libcrypto++-dev" libz-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

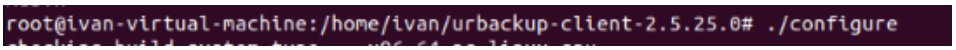
Anexo 114 *Comando para instalar dependencias para UrBackup cliente*

```
root@ivan-virtual-machine:/home/ivan# tar xzf urbackup-client-2.5.25.tar.gz
root@ivan-virtual-machine:/home/ivan# ls
Desktop    Music      snap                      urbackup-client-2.5.25.tar.gz
Documents  Pictures   Templates                 Videos
Downloads  Public     urbackup-client-2.5.25.0
root@ivan-virtual-machine:/home/ivan#
```

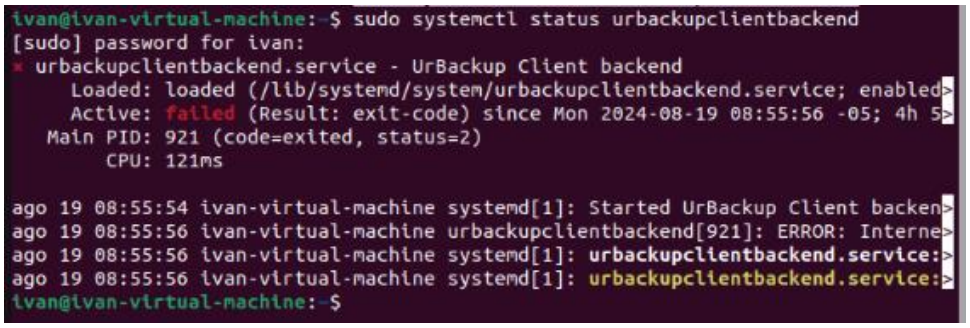
Anexo 115 *Descargar y descomprimir UrBackup cliente*

```
root@ivan-virtual-machine:/home/ivan# cd urbackup-client-2.5.25.0
root@ivan-virtual-machine:/home/ivan/urbackup-client-2.5.25.0#
```

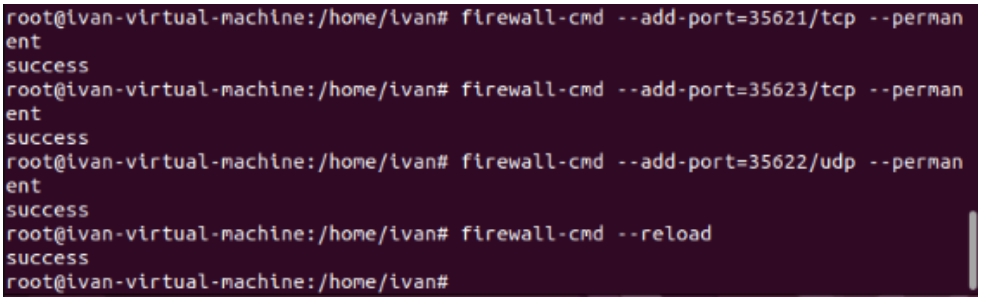
Anexo 116 *Ingreso a la carpeta UrBackup Cliente*



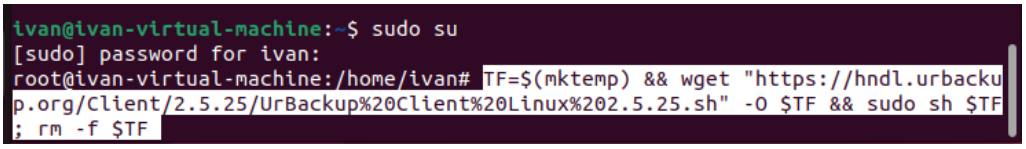
Anexo 117 *Comando a configurar antes de instalar UrBackup Cliente*



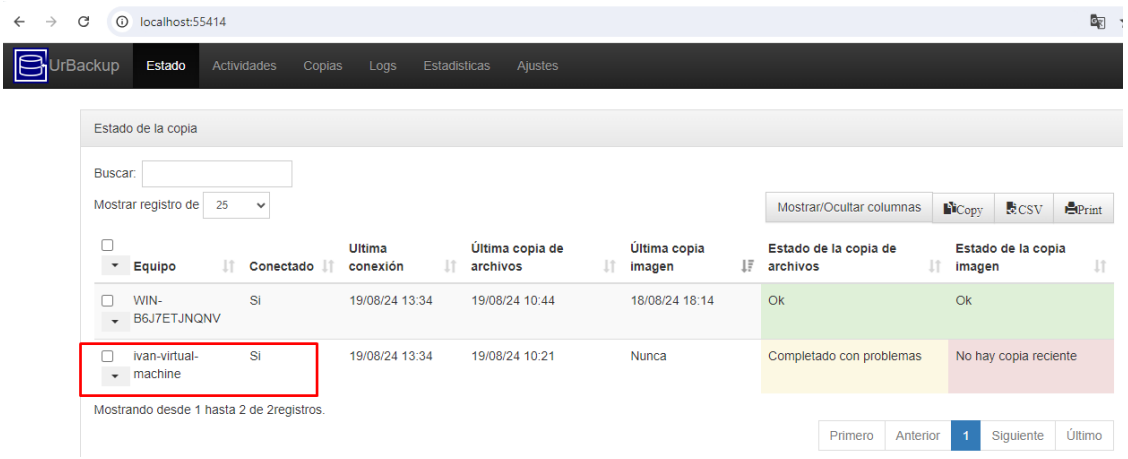
Anexo 118 *Estado activo de UrBackup Cliente*



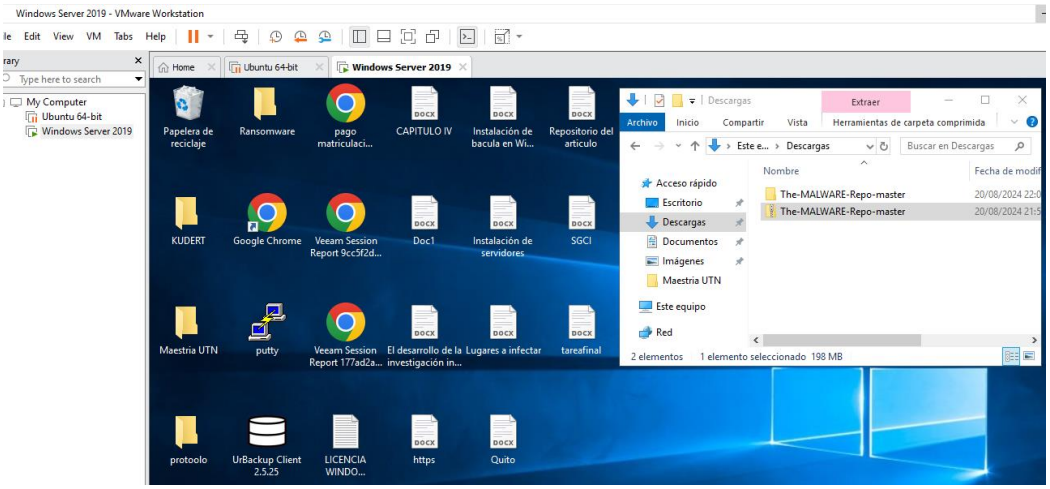
Anexo 119 *Habilitar puertos en Firewall*



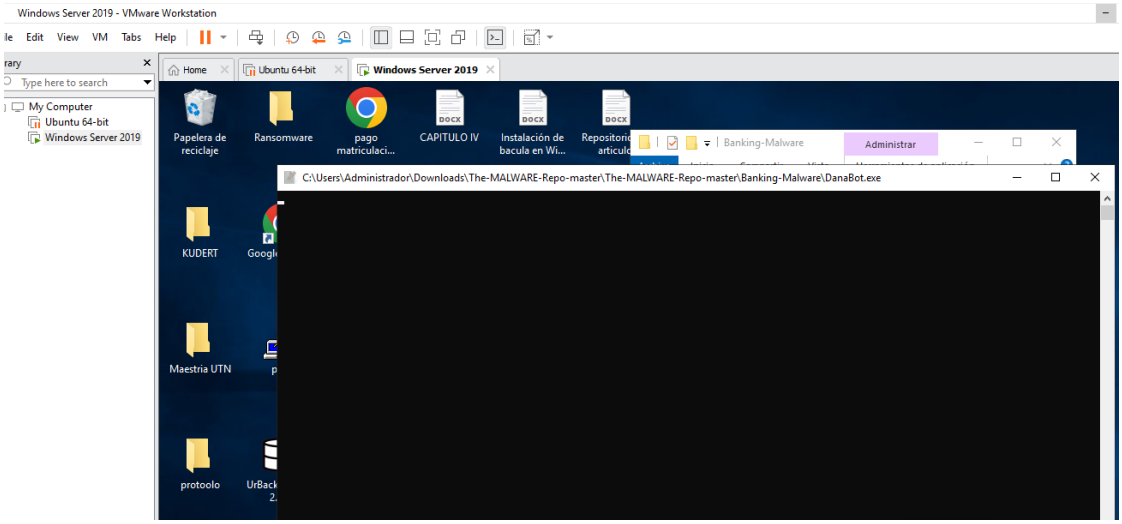
Anexo 120 *Instalar UrBackup cliente*



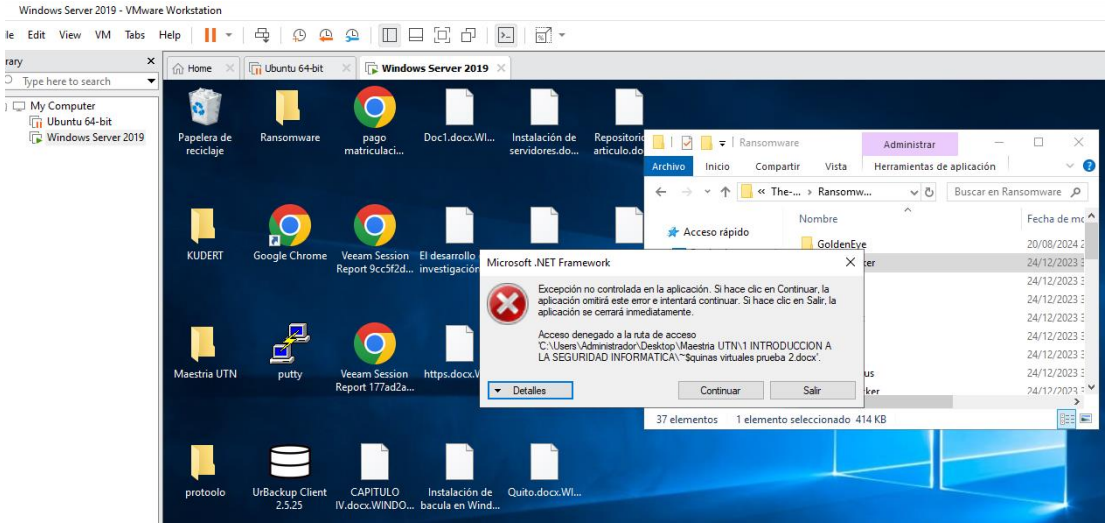
Anexo 121 *Conexión de UrBackup Server y UrBackup client*



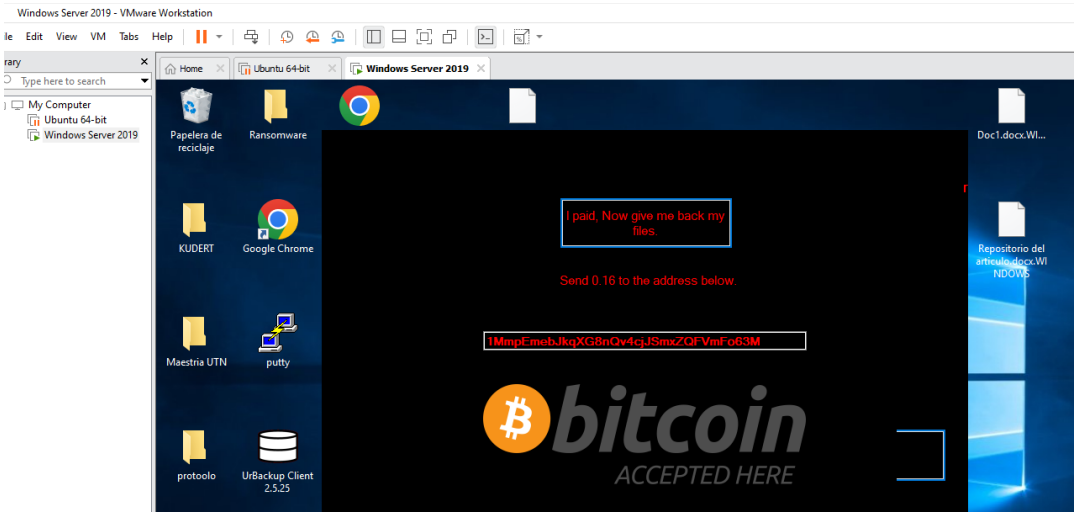
Anexo 122 *Paquete de malwares para Windows Server 2019*



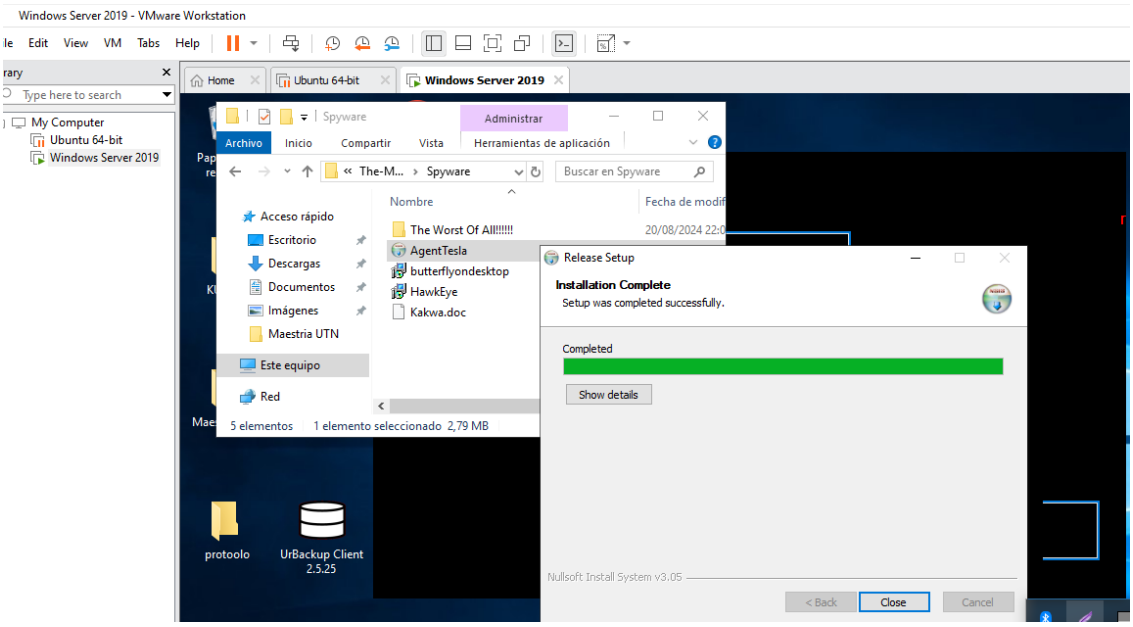
Anexo 123 *Infección de máquina virtual Windows Server 2019 con Banking-Malware Danabot.exe*



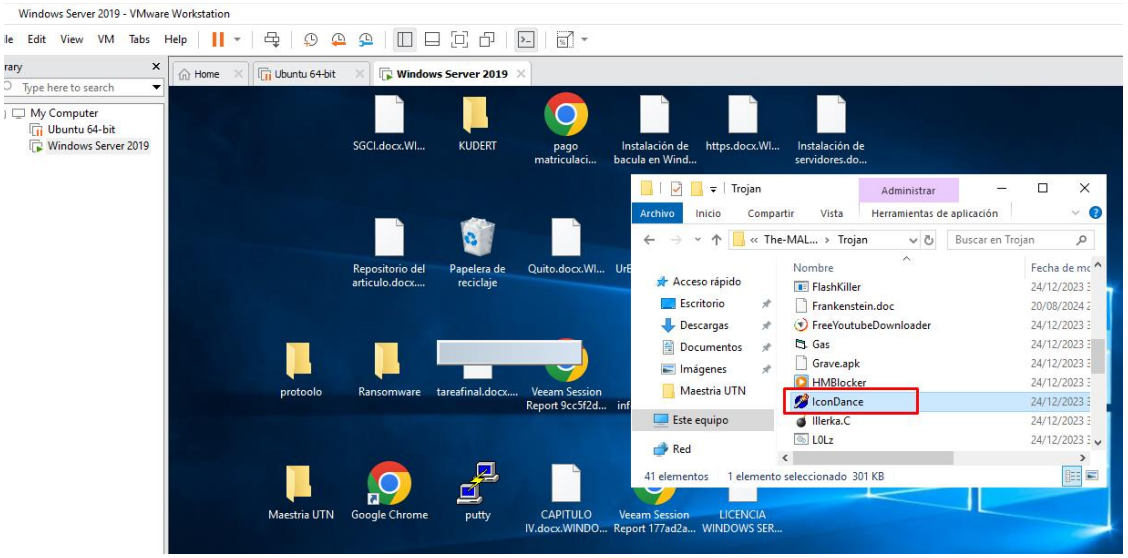
Anexo 124 *Infección de máquinas virtuales Windows Server 2019 con Ransomware $uckyLocker.exe*



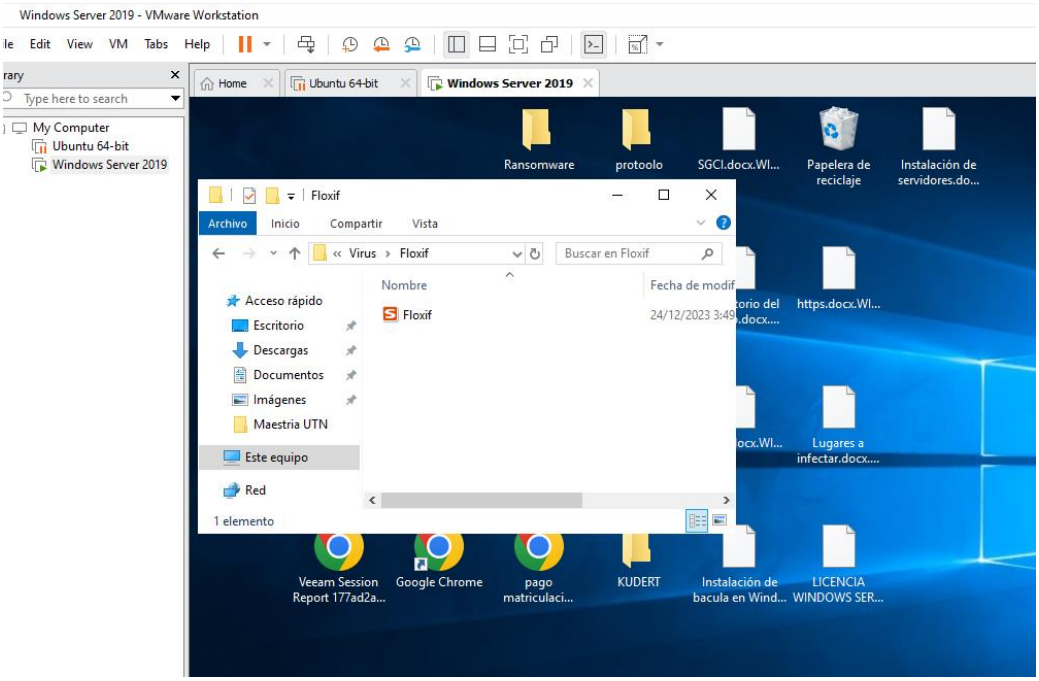
Anexo 125 *Archivos infectados con Ransomware $uckyLocker.exe*



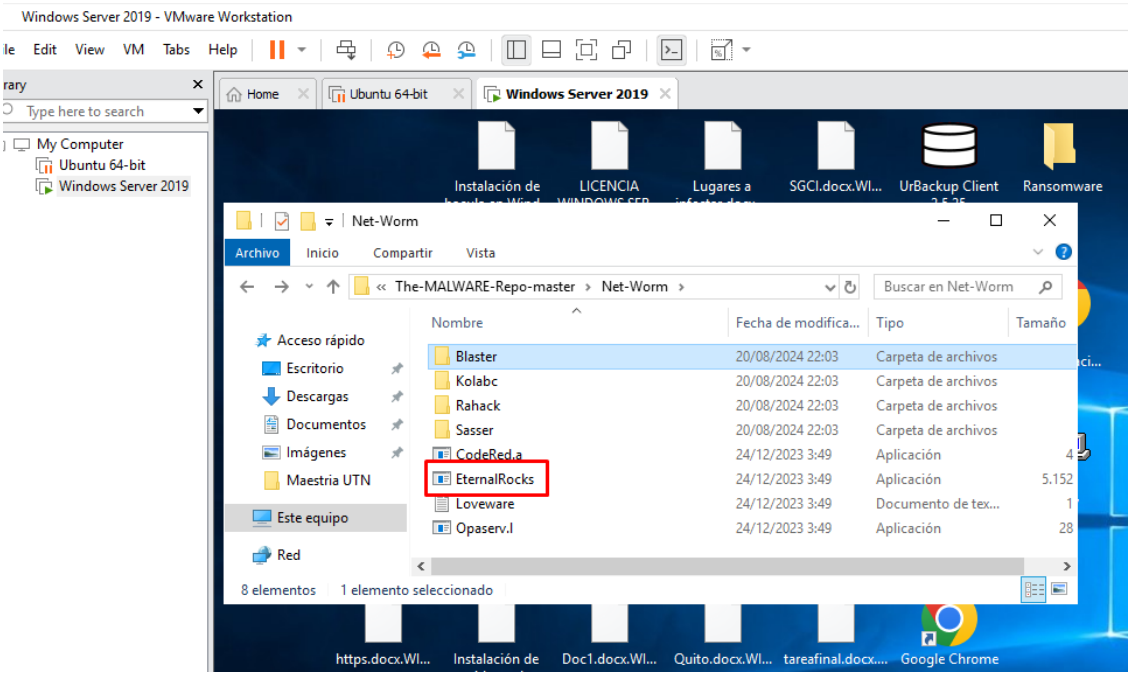
Anexo 126 *Infección de máquinas virtuales Windows Server 2019 con Spyware Agenttesla.exe*



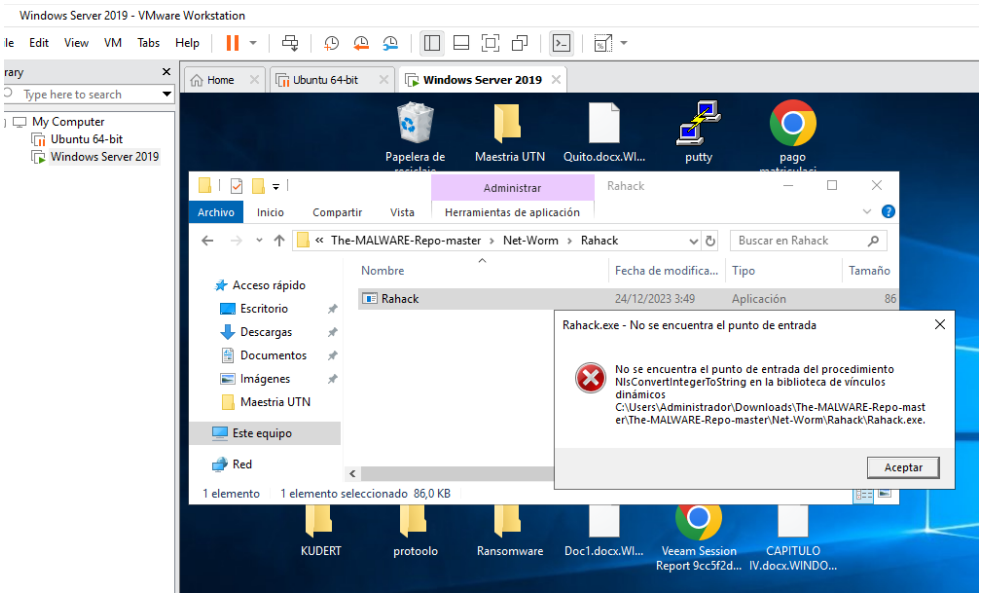
Anexo 127 *Infección de máquinas virtuales Windows Server 2019 con Trojan IconDance.exe*



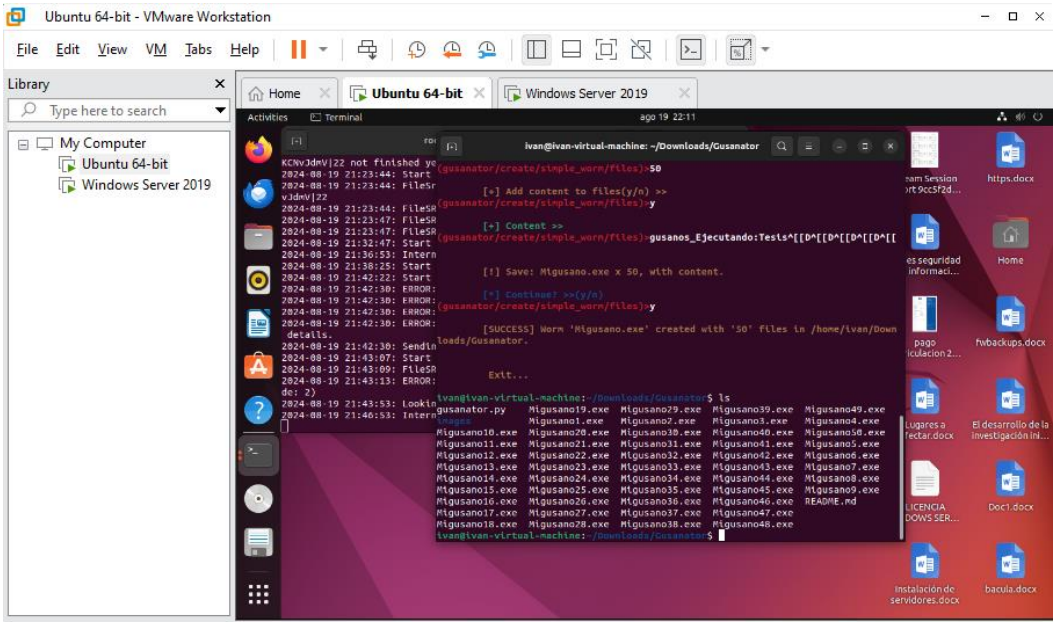
Anexo 128 *Infección de máquinas virtuales Windows Server 2019 con Virus Floxif.exe.*



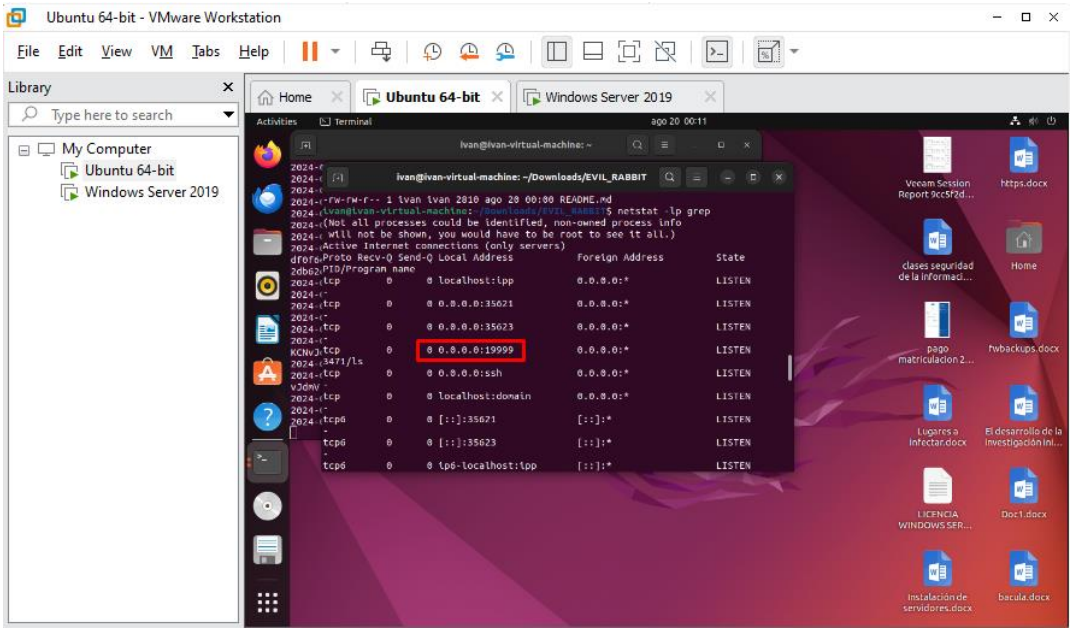
Anexo 129 *Infección de máquinas virtuales Windows Server 2019 con Net Word EternalRocks.exe*



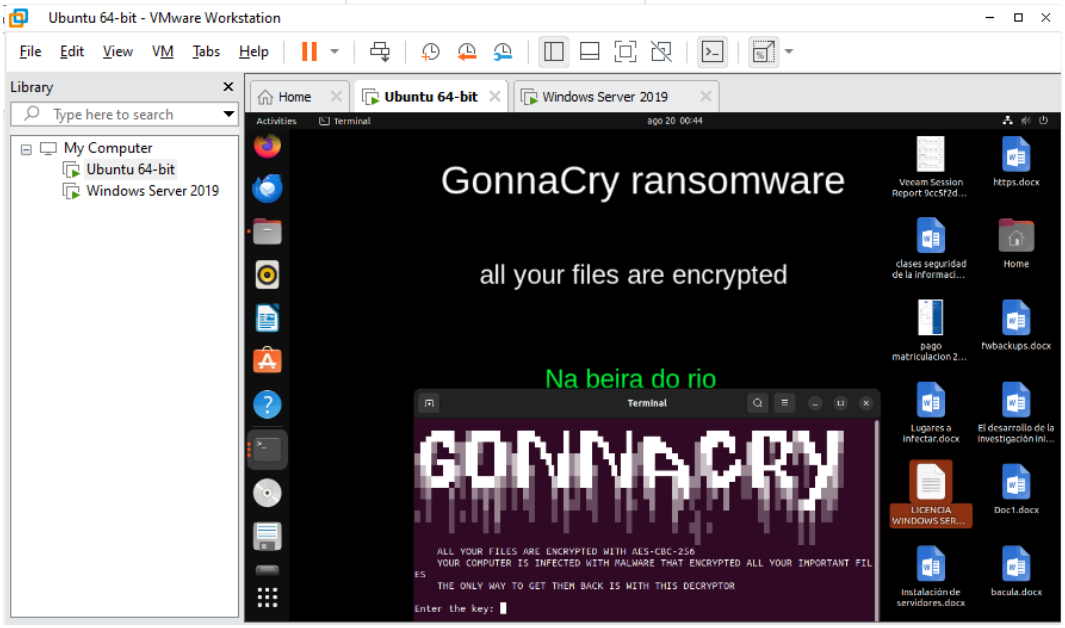
Anexo 130 *Infección de máquinas virtuales Windows Server 2019 con Net Word Rahack*



Anexo 131 *Gusanator instalado en Ubuntu 22*



Anexo 132 *EvilRabbit instalado en Ubuntu 22*



Anexo 133 *Gonnacry instalado en Ubuntu 22*

GLOSARIO DE TÉRMINOS

Amenaza interna: Riesgo o daño causado por un individuo o grupo dentro de una organización que tiene acceso legítimo a los sistemas o redes.

Ataque de inyección SQL: Técnica utilizada por atacantes para introducir código malicioso en las consultas SQL de una base de datos, permitiendo el acceso no autorizado a datos.

Ataque de troyanos: Tipo de ataque cibernético en el cual se introduce un programa malicioso que parece ser legítimo, pero que permite a los atacantes tomar control de un sistema.

Ataques cibernéticos: Acciones maliciosas realizadas para acceder, alterar o destruir datos, sistemas o redes a través de medios digitales.

Backup: Copia de seguridad de datos realizada para proteger la información frente a pérdidas accidentales o ataques cibernéticos.

BS 7799-2: Norma que proporciona directrices para la gestión de la seguridad de la información en organizaciones.

Canal TLS: Protocolo que garantiza la seguridad de las comunicaciones a través de internet mediante el cifrado de los datos transmitidos.

Claves criptográficas: Secuencias de datos utilizadas para cifrar y descifrar información en sistemas de seguridad.

Cloud: Tecnología de computación en la nube que permite almacenar y acceder a datos y aplicaciones a través de internet.

Ciberdelincuente: Persona que comete actos ilegales mediante el uso de tecnología y redes informáticas.

Ciberseguridad: Conjunto de prácticas, tecnologías y políticas destinadas a proteger los sistemas, redes y datos frente a ataques y amenazas cibernéticas.

Conexión SSH: Protocolo de comunicación seguro utilizado para acceder y gestionar sistemas de manera remota a través de una red.

Copias de seguridad: Procedimiento para crear una copia de los datos importantes con el fin de restaurarlos en caso de pérdida o daño.

Cross-site scripting: Vulnerabilidad de seguridad en aplicaciones web que permite a los atacantes insertar código malicioso en sitios confiables.

Día cero: Vulnerabilidad de seguridad recién descubierta que aún no tiene solución, lo que la hace especialmente peligrosa para los sistemas.

Dump y/o GNU: Herramientas utilizadas para generar volcados de memoria o información del sistema, a menudo empleadas en el análisis forense digital.

DNS: Sistema de nombres de dominio que traduce direcciones web legibles por humanos en direcciones IP utilizadas por los equipos de red.

Errores tecnológicos: Fallos o problemas en sistemas tecnológicos que pueden causar malfuncionamiento o vulnerabilidades de seguridad.

Gartner: Empresa de investigación y consultoría que proporciona análisis y recomendaciones sobre tecnologías de la información.

Gusano: Tipo de *malware* que se replica a sí mismo y se propaga a través de redes, infectando otros sistemas sin intervención humana.

Hyper-V: Plataforma de virtualización desarrollada por Microsoft para crear y gestionar máquinas virtuales en servidores.

IP: Protocolo de internet que asigna direcciones únicas a cada dispositivo conectado a una red.

Imagen ISO: es un archivo que contiene una copia exacta (o "imagen") de todo el contenido de un sistema de archivos, como el de un CD, DVD, Blu-ray, o incluso una unidad de almacenamiento USB, en un solo archivo.

ISO 22301: Norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la continuidad del negocio.

Linux: Sistema operativo de código abierto utilizado en servidores, ordenadores personales y dispositivos móviles.

Malware o software malicioso: Programas diseñados para dañar, interrumpir o robar información de un sistema informático.

Maquina física: Computadora o servidor que opera sin virtualización, ejecutando software directamente sobre su hardware.

Máquina virtual: Entorno simulado que permite ejecutar un sistema operativo y aplicaciones como si fuera una máquina independiente, pero sobre hardware compartido.

Open PGP: Estándar de cifrado y firma digital para proteger la privacidad de la información en correos electrónicos y archivos.

Open source: Software cuyo código fuente es accesible y libre para ser modificado, distribuido y utilizado por cualquiera.

Phishing: Técnica fraudulenta que utiliza engaños, como correos electrónicos falsos, para robar información personal o financiera de los usuarios.

Proxmox: Plataforma de virtualización de código abierto para gestionar servidores y máquinas virtuales.

Ransomware o secuestro de datos: Tipo de *malware* que bloquea el acceso a los archivos del usuario y exige un rescate para liberarlos.

Red LAN: Red de área local que conecta dispositivos dentro de un área geográfica limitada, como una oficina o un edificio.

Red NAT: Traducción de direcciones de red, una técnica utilizada para modificar las direcciones IP en los paquetes de datos de una red privada.

Root: El usuario con privilegios más altos en sistemas operativos Unix o Linux, con

acceso completo a todos los archivos y configuraciones. **Rootkits**: Conjunto de herramientas diseñadas para ocultar la presencia de ciertos procesos o programas maliciosos en un sistema comprometido.

Terminal en Linux: Interfaz de línea de comandos en sistemas operativos basados en Linux para interactuar con el sistema mediante comandos.

Tipos de cifrados: Métodos y algoritmos utilizados para transformar datos legibles en una forma cifrada y segura.

Troyano: *Malware* que se presenta como un programa legítimo pero que permite a un atacante acceder a un sistema sin el conocimiento del usuario.

VMware: Plataforma de virtualización que permite crear y gestionar máquinas virtuales sobre un servidor físico.

VMware Backup Replication: Herramienta de VMware que permite crear copias de seguridad y replicar datos de máquinas virtuales en entornos virtualizados.

Windows: Sistema operativo desarrollado por Microsoft, ampliamente utilizado en dispositivos personales y de oficina.

Xen, KVM: Tecnologías de virtualización de código abierto que permiten crear y gestionar máquinas virtuales en servidores.

Zeroday: (Otro nombre para Día Cero) Vulnerabilidad de software recién descubierta sin parche de seguridad disponible.

SSL: Protocolo de seguridad utilizado para establecer una conexión cifrada entre un servidor web y un navegador.

vCloud: Plataforma de virtualización y nube desarrollada por VMware que permite a las empresas crear, gestionar y operar aplicaciones en la nube.

vSphere: Plataforma de virtualización de VMware utilizada para gestionar máquinas virtuales y recursos en un centro de datos.

UrBackup: Software de backup de código abierto que permite realizar copias de seguridad de sistemas y archivos de manera eficiente.

Xen, KVM: Plataformas de virtualización de código abierto utilizadas para ejecutar múltiples máquinas virtuales en un solo servidor físico.