UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas open sourcepara PyMES

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Laymito Lozano, Jesus Martin (orcid.org/0000-0002-5833-8376)

Ocampo Gutierrez, Jhonattan Walter (orcid.org/0000-0002-9362-5231)

ASESOR:

Mg. Saboya Rios, Nemias (orcid.org/0000-0002-7166-2197)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA - PERÚ

2022

UNIVERSIDAD CÉSAR VALLEJO

Dedicatoria

Dedicado a mi esposa Katherine y a mis padres quienes confiaron en mí y me apoyaron siempre brindándome su apoyo incondicional.

Ocampo Gutierrez Jhonattan Walter

Dedico el presente trabajo a mi esposa Lourdes y mis hijos Valeria y Franco por todo el apoyo incondicional que me brindaron en esta experiencia universitaria.

Laymito Lozano Jesús Martín

Agradecimiento

Agradecemos a Dios por permitirnos culminar este proyecto y a nuestra familia por haber apostado en nuestra educación profesional. Esta tesis representa un arduo trabajo, por lo que agradecemos a la empresa New Fashion Perú y a nuestro asesor Mg. Nemias Saboya, por todo el apoyo brindado.

Índice de Contenidos

Índice de tablas

Índice de figuras

Resumen

El propósito de la presente tesis consistió en implementar un método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source para las PyMES. Se aplicó la metodología aplicada pre experimental con enfoque cuantitativo. Por otro lado, se consideró 3 dimensiones de la seguridad de información con 12 indicadores de evaluación. Estos indicadores fueron evaluados en 2 momentos, el primero fue antes de la implementación del método y el segundo fue en un periodo de 15 días, por medio de una lista de cotejo., validado por los expertos. La información obtenida favorece a las dimensiones analizadas, pues se implementó la prueba no paramétrica Wilcoxon, donde los resultados demostraron que fueron significativos con sig menor que el $\alpha = 0.05$. Se concluyó que la implementación el método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source para las PyMES contribuye de manera favorable en la confidencialidad, integridad y disponibilidad de los datos de los servidores de la empresa.

Palabras clave: seguridad de información, cloud, mirror server, integridad, confidencialidad

Abstract

The purpose of this thesis was to implement an information security method based on Mirror Server technology in the cloud with Open Source tools for SMEs. The pre-experimental applied methodology with quantitative approach was applied. On the other hand, 3 dimensions of information security with 12 evaluation indicators were considered. These indicators were evaluated in 2 moments, the first one was before the implementation of the method and the second one was in a period of 15 days, by means of a checklist, validated by the experts. The information obtained favors the dimensions analyzed, since the nonparametric Wilcoxon test was implemented, where the results showed that they were significant with sig less than $\alpha = 0.05$. It was concluded that the implementation of the information security method based on Mirror Server technology in the cloud with Open Source tools for SMEs contributes favorably to the confidentiality, integrity and availability of data on the company's servers.

Keywords: information security, cloud, mirror server, integrity, confidentiality.

I INTRODUCCIÓN

La seguridad de información en las organizaciones es una necesidad debido a los grandes cambios y revoluciones tecnológicas en la informática y las telecomunicaciones que se han generado en los últimos años, (las redes sociales, reuniones virtuales, los equipos móviles, los satélites, etc.) toda esta transformación digital ha generado también un impacto económico e impacto social. (Moncada, Israel ,2018)

El tema de seguridad de Información en las pymes es el objetivo a tratar y de poder mostrar una solución eficaz para poder garantizar la confidencialidad, integridad y disponibilidad de los sistemas en este tipo de empresas; por lo cual se desea proponer un método de seguridad de información basado en tecnología de Servidores Espejos, específicamente en la nube con herramientas Open Source para PyMES, con la finalidad de dar una solución a dicho problema, presentado generalmente en la mayoría de las medianas y pequeñas empresas. (Armando et al. 2017)

En la actualidad las pymes han empezado a evaluar lo importante que es adquirir un sistema de seguridad de información, así como un buen uso de sus activos tecnológicos, los cuales buscan protegerlos ante una intrusión, falla técnica, desastre natural, etc. Con esto se pretende mejorar el uso de herramientas para realizar y aplicar una solución de seguridad aceptable de acuerdo con sus necesidades. En el mundo la mayoría de las empresas han aumentado los presupuestos en ciberseguridad para prevenir ataques a sus equipos mediante la red, sin embargo, hay empresas pequeñas que aún les cuesta entender lo primordial que es proteger la seguridad de su información, sin embargo, lo ven como un gasto adicional que no desean asumir. (Serrano Quevedo, Molina Chalacán, Zúñiga Paredes, et al., 2020)

Los problemas identificados en la tesis son los siguientes; la falta de conocimiento de los riesgos que pueden ocurrir en los activos tecnológicos de la empresa, la falta de presupuesto para adquirir una solución de protección de la información, y el poco interés en obtener un respaldo de la información.

En este trabajo de investigación se pretende implementar un método que ayudará a ver el problema, determinar la causa y brindar una solución. Además, se da a

conocer cuál es el objetivo general, así como los específicos. Se define las hipótesis y las justificaciones de la tesis. Adicionalmente, se listan los posibles riesgos que pueden hacer peligrar la culminación de la tesis.

La problemática de la investigación se basa en ¿Cómo influye el método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source para PyMES?, esta formulación puede ser resuelto desde el uso de una herramienta open source mediante servidores espejos en la nube, y en base a lo descrito se formulan los siguientes problemas específicos, ¿Cómo influye el método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source en la confidencialidad de la seguridad de información en las PyMES?, ¿Cómo influye el método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source en la integridad de la seguridad de información en las PyMES?, ¿Cómo influye el método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source en la disponibilidad de la seguridad de información en las PyMES?

El objetivo general de esta investigación es Determinar cómo influye el método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source para PyMES, Tal mejora debe incluir un metodo que cumpla con mejorar la seguridad de la información de las pymes, y como objetivos específicos, tenemos el determinar cómo influye el método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source en la confidencialidad, integridad y disponibilidad en la pyme.

Para la presente investigación, se acudió a la revisión de fuentes de tipo primaria, es decir, libros, tesis similares al tema de estudio y artículos de investigación. Esto debido a que la seguridad de información en la nube abarca muchos temas sobre la seguridad de los datos.

Para dar respuesta a la interrogante del proyecto de investigación se planteó la siguiente hipótesis: El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source influye en la seguridad de información para PyMES, de tal manera tenemos la siguientes

hipótesis especificas: El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source influye en la confidencialidad, integridad y disponibilidad de la seguridad de información en las PyMES

La investigación por realizar se justifica en cuatro ámbitos:

Teórica, porque va ligada a las inquietudes de nosotros, los investigadores por profundizar los enfoques teóricos con el fin de colaborar con los conceptos en una línea de investigación, además se detecta un espacio incompleto en este campo científico y la conducción de esta tesis permitió completar los conceptos. (Musallam, Fauzi, Nagu 2019)

Práctica, porque nuestro estudio generará aportes directos o indirectos y también prácticos que se relacionan al problema real del estudio, ofrece un concepto amplio, que ayudará a resolver un problema de respaldo de la información, con estrategias y con la práctica que contribuirán con la solución. (Musallam, Fauzi, Nagu 2019)

Metodológica, porque la propuesta desarrolla un nuevo método para obtener un conocimiento amplio, válido y confiable. Además, esta metodología permitirá incluir otras maneras de experimentar una o más variables. (Musallam, Fauzi, Nagu 2019)

Económica, porque el tema de investigación presentado ofrece una solución en bajos costos en comparación con otras soluciones, logrando así que los nuevos emprendedores incrementen la seguridad de su información en sus pymes. (Musallam, Fauzi, Nagu 2019)

Finalmente se concluyó que la implementación de un servidor alterno de replicación tendrá la posibilidad de ejecutar las mismas tareas del principal, y que, en caso de fallo en el servicio, éste no se vea afectado y la empresa con sus usuarios puedan continuar con sus labores de forma casi inmediata sin causar retrasos en la operación y en la producción.

II MARCO TEÓRICO

Antecedentes

Para la presente tesis se muestran los estudios utilizados tanto nacionales como internacionales.

Antecedentes Internacionales

En ecuador, sobre todo en los últimos 5 años, las pymes han ido en crecimiento en su cartera de inversión y producción y esto ha generado que se promueva más empleo, sin embargo en el tema de seguridad de información se ha ido dejando de lado y esto ha generado pérdidas por los ataques causado por un hacker que usan métodos para encriptar la información y luego pedir un rescate, y esto pasa por no implementar métodos que resguarden la información que se tiene en la organización, las pymes no le prestan mucha importancia porque lo ven como un gasto y no como un beneficio, así mismo no cuentan con personas capacitadas para contrarrestar cualquier ataque o perdida de información, no cuentan con una buena infraestructura de red, no cuentan con programas de protección, sus servidores son físicos y se encuentran expuestos ante cualquier ataque o catástrofe que pueda ocurrir. (René Zuña Macancela, Edgar, 2019)

En el estudio realizado por Ranulfo Cuesta Quinteros, el sistema que detecta los intrusos mediante la red de honeynet sobre ipv6, es un sistema de seguridad que ayuda a las pymes en resguardar sus tecnologías de información. Esta herramienta es usada para la seguridad informática y verificar si hay algún comportamiento sobre algún atacante externo en la red. La finalidad de esta tesis es evidenciar las pruebas experimentales de los ciber ataques. (Ranulfo Cuesta Quintero, 2018)

Este documento aporta una solución importante que evita la intrusión de atacantes a la red donde se implementa, está basado en el uso de herramientas tecnológicas, los cuales brindaron resultados de detección completa de diversos ataques e intrusiones a la red, resultados que se obtuvieron a través de pruebas experimentales.

Antecedentes Nacionales

En el estudio de investigación titulado Uso de mecanismos que contrarrestan ataques cibernéticos en base de datos y servidores web, el autor se enfocó en comparar las diferentes plataformas de seguridad capaces de controlar los ciber ataques, con la intención de atrapar la información de los hackers y potenciar la seguridad en los servers del web service y la data base. Este ataque fue analizado e implementado con diferentes mecanismos de seguridad en la red previamente diseñados, establecidos por el investigador, el primer mecanismo consiste en un clon de red espejo virtual (Honeynet) de autocontenido. También se elaboró un segundo mecanismo Snort en Kali Linux. En esta investigación el autor pudo estudiar y analizar el impacto de diferentes ataques, enfocándose en el tiempo del servidor no disponible, el mecanismo Honeynet fue el más rápido, logró un tiempo de 0.8 seg., mientras que Snort logró 1 seg. También encontró que el mecanismo Snort logró el tiempo más rápido de respuesta con 3.8 seg., y por otro lado Honeynet obtuvo 3.6 seg. de reacción. El desempeño de estos mecanismos por ataques fue de un 97,4% de precisión, 99,3% de sensibilidad, 96% de especificidad y un 98,2% de precisión en el mecanismo Honeynet de autocontenido virtual de III generación, Snort tuvo el 97,8% de precisión, 97% de sensibilidad, 96,5% de especificidad y 98% de precisión. (Izquierdo, Tafur, 2017)
En esta investigación el autor muestra su experimentación con un problema real en las cuales encontró vulnerabilidades en los servidores web y Sql, para lo cual implementa un espejo de red virtual llamado Honeynet de auto-contenido. También implementó un segundo mecanismo Snort en Kali Linux, los cuales brindaron seguridad a los servidores principales en la organización donde se instaló.

Los autores Farfán, Blas y Pedro, Deyner de la UCV Trujillo-Perú con su investigación titulado: ¨Implementación De Un Servidor De Dominio Espejo Para La Mejora de Disponibilidad web del Colegio La Asunción De Trujillo¨, manifiestan en su tesis que el objetivo es mejorar la disponibilidad web del sitio web del colegio La Asunción de Trujillo, para realizar esta evidencia se contó con el uso de herramientas web gratuitas y de alta disponibilidad el estado actual del parámetro disponibilidad, posteriormente se diseñó e implemento un servidor tipo espejo para

mejorar las condiciones y finalmente volver a medir el requerimiento no funcional de disponibilidad. El tipo de investigación fue no experimental con enfoque cualitativo, finalmente se concluyó y observó una mejora del 2.5466% respecto a la disponibilidad web del servidor, asegurándose una mejora respecto a la competencia y suponiendo una mejora económica para la institución por sobre los otros colegios de la región., (Farfán, Blas y Pedro, Deyner de et al., 2021)

En esta investigación los autores muestran la implementación del servidor tipo espejo se realizó sobre la arquitectura actual de la institución educativa particular “La Asunción” de Trujillo, 2021 como solución en la mejora de seguridad de su plataforma web. Para ello se aplicó una metodología basada en la practicidad y el control de tiempos, sin descuidar la calidad de la infraestructura, esto con el fin de tener un respaldo de la información del servidor web en caso ocurra un percance informático, para ello se contó con el uso de herramientas gratuitas lo cual ocasionó un ahorro por parte de la entidad educativa y a su vez obtuvo una solución de protección a su información web.

Bases teóricas

Definición del término pyme

Denominado también como “Pequeña y mediana empresa”, son entidades independientes con alta presencia en el mercado. Son agentes con culturas, intereses, estrategias y espíritu emprendedor específico. Para efectos de esta tesis se tomará como PYME a la empresa New Fashion Perú. (Valdevit, Mayer, Barafort, et al., 2019)

Las pymes en el Perú

Las pymes son pequeñas y medianas empresas y son organizaciones que se encuentran en contaste desarrollo y cumplen un rol muy importante en el mercado laboral, brindando trabajo a más personas y generando un valor agregado para la industria.

Actualmente las pymes no le brindan mucha importancia a su seguridad de información de sus datos que tienen en sus servidores, piensan que es un gasto en

vez de un beneficio, por lo cual no optan por implementar sistemas de seguridad, las pymes creen que un antivirus es suficiente para resguardar su información. (Damián López, et al., 2020)

Las pymes normalmente suelen ser empresas familiares, no están sujetas de crédito, ni instituciones públicas o privadas, su mercado es local y la mayoría de su personal no son calificados para ocupar los puestos y el sueldo no son bien remunerados.

Una característica es su instalación que se va adaptando mediante las necesidades que tienes la empresa, es decir que la mayoría de sus procesos son manuales y semi mecánicos, tiene más procesos de producción en mano de obra que de equipos (Melisa Osores, et al., 2016).

Ventajas y desventajas de las pymes:

Ventajas:

- Genera empleos
- Se va adaptando a la tecnología
- Su producción local es básica
- Planificación y organización no necesita mucho dinero invertido
- Las ventas de sus productos es un precio justo y competitivo
- Cuenta con una organización que les permite adaptarse al mercado
- Asimilan y se adaptan a las tecnologías

Desventajas:

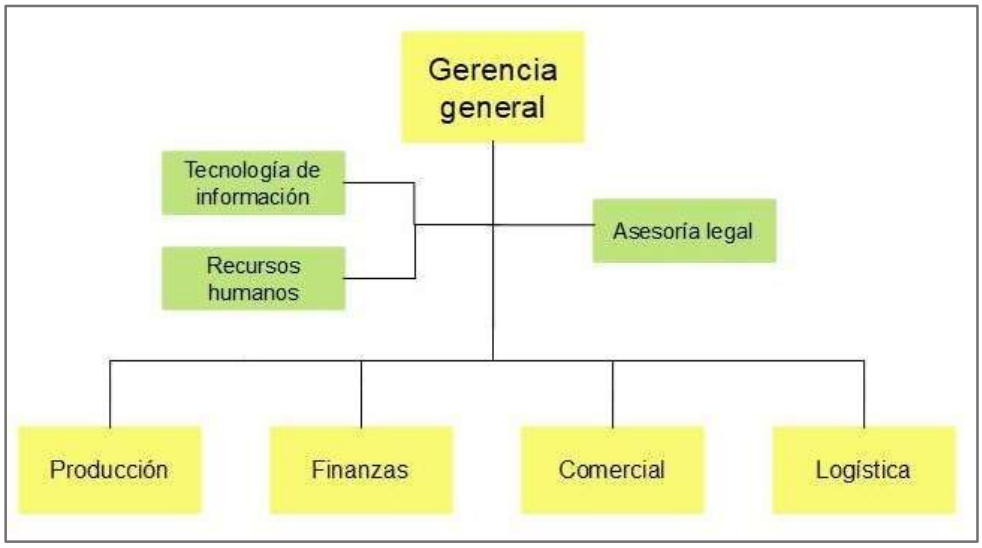
- Tienen problemas con la inflación y la devaluación
- No está organizado para soportar crisis económicas
- Falta de recursos financieros
- Las posibilidades de crecer son muy bajas
- Tienen una gran tensión política, ya que los grandes empresarios tratan de eliminarlos para no tener competencia.
- La administración no está al 100% especializada para llevar un buen control de su empresa.
- No utilizan las utilidades para mejorar en equipos

- No pueden financiar gastos de capacitación del personal
- No tienen innovación tecnológica

Organigrama de una pyme:

Toda empresa está constituida por un organigrama que subdivide varias áreas, cada área cumple un rol distinto y es súper importante el manejo de la seguridad de información de sus datos. (Frey Arrieta, Mytzy,Loayza García, Mariella Patricia, 2018)

Figura 01: Organigrama general de una Pyme



Fuente: Elaboración Propia

Gerencia General: tiene acceso a todos los datos que hubiera en la empresa, ya que él es el encargado de revisar los informes, ver cómo va el estado de la empresa, es el que acepta los requerimientos, el que brinda la aprobación para cualquier productos que tiene la empresa, por lo cual su seguridad de información debe de cumplir con los tres pilares que son la confidencialidad, disponibilidad e integridad para que su información siempre este protegida ante cualquier circunstancia que pueda ocurrir. (Yagual, Tatiana 2018)

Tecnología de información: Es el área encargada de gestionar los activos, recursos, y sistemas a la empresa, es que se encarga de configurar los usuarios, se encarga de ver por los servidores de la empresa, se encarga de la infraestructura de la red de la empresa , es el que tiene acceso a todos los datos después de gerencia general, el área de TI se encarga de mantener la integridad de los datos, como la disponibilidad de toda la información ante cualquier problema que pueda ocurrir , siempre debe de brindar la confidencialidad de los sistemas en la empresa. (Yagual, Tatiana, 2018)

Recursos Humanos: Es el encargado de gestionar la plantilla del personal, como la planilla de la empresa, lo cual brinda una gran vulnerabilidad de los datos, ya que, si se llega a pasar algún inconveniente con los sistemas, este podría generar gran pérdida económica a la empresa y a la vez podría ser multado por no llevar un buen control de los datos de la empresa, lo cual es fundamental que cuente con los tres pilares de la seguridad de la información. (Yagual, Tatiana, 2018)

Asesoría Legal: Toda pyme debe de contar con un abogado que brinde el respaldo de cumplir los derechos de cada trabajador como de la organización, lo cual tiene acceso a los datos de la empresa como los empleados que trabajan en la organización, lo cual también es requisito fundamental que cuente con los tres pilares de la seguridad de la información.

Producción: El área de producción es el encargado de producir los equipos de la empresa, lo cual maneja bastante información mediante carpetas compartidas en red, lo cual hace que sea un área bastante vulnerable ante cualquier ataque de red o el mal uso ético de algún trabajador lo cual podría generar una gran pérdida económica si se perdiera alguna información, lo cual es fundaméntela que cuenta con los tres pilares de la seguridad de la información. (Frey Arrieta, Mytzy,Loayza García, Mariella Patricia, 2018)

Finanzas: El área de finanzas está encargada de recibir y gestionar las facturas de la empresa o de los clientes, lo cual aquí se ve reflejado mucho el tema de costo y

presupuesto lo cual hace que sea un área bastante vulnerable en perdida de información y a su vez pérdida económica, en muy importante que esta área pueda contar con los tres pilares de la seguridad de la información ya que es un área que ve directamente temas económicos. (Yagual, Tatiana, 2018)

Comercial: El área comercial es el área de ventas, es el encargado de registra los pedidos y de captar clientes, lo cual tiene accesos a distintos recursos compartidos, como carpetas en red, impresoras, wifi y está expuesto a cualquier ataque mediante la red o correo y es un gran problema porque la mayoría de vendedores no cuenta con mucha experiencia en tecnología lo que los hace blanco de ciberataques o perdidas de datos, es un área que debe contar con los tres pilares de la seguridad de la información.

Logística: El área de logística en el encargado de generar las órdenes de compra y subirlo al sistema para que las demás áreas puedan facturas y hacer los pedidos, lo cual tiene acceso a los diferentes sistemas que tiene la organización y los datos están expuesto ante cualquier ataque o problema que pueda incurrir en la empresa, lo cual es fundamental que pueda contar con los tres pilares de la seguridad de la información. (Frey Arrieta, Mytzy,Loayza García, Mariella Patricia, 2018)

Las pymes con el pasar de los años han ido mejorando en la eficiencia del negocio, lo cual ha hecho que las empresas puedan confiar en contar con servidores en la nube, y esto los ayude ante un ciber ataque, daño físico o desastre natural. Según un estudio explica que las TI han mejorado en la preparación de desastres, alrededores del 34% de las organizaciones han ido implementando sus servidores a la nube o están en proceso de virtualizar sus sistemas para tener una mejor seguridad de sus datos. (Delina Aguilar Tun, et al., 2016)

Las pymes y la tecnología de información

Para que las Pymes logren desarrollarse, se necesita contar con una importante inversión económica, y también con innovación y tecnología. El aporte de la tecnología es una forma de realizar las cosas eficientemente, por eso cualquier procedimiento utilizado por la PYME debe de buscar paralelamente el

perfeccionamiento. (Serrano Quevedo, Molina Chalacán, Zúñiga Paredes, et al., 2020) Las PYMES adoptan o hacen uso de la TI para:

- Lograr con eficiencia un mayor acceso a la información
- Mejorar internamente su administración.
- Mejorar la gestión de su producción y el control de Calidad
- Facilitar la cooperación y alianzas con otras empresas para alcanzar economías de mayor nivel.
- Descubrir nuevas estrategias y oportunidades de negocios.

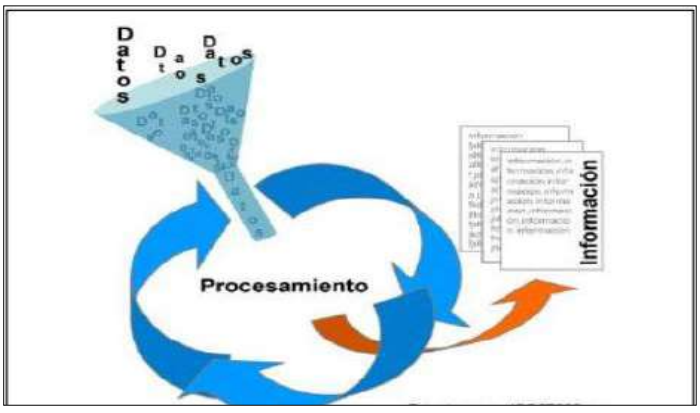
Seguridad de la información

La seguridad de la información es un mecanismo de prevención ante amenazas que se pueden presentar en la red, la seguridad garantiza la continuidad del negocio, minimizando las vulnerabilidades que puedan existir en distintas formas, puede ser impresa, recolectada digitalmente, pueden ser imágenes o puede ser una conversación. (Guerra et al. 2021)

La seguridad de la información resguarda y protege los datos de una organización con una forma adecuada a fin de establecer las dimensiones de confidencialidad, integridad, y disponibilidad de los datos que se almacenan en las organizaciones.

Para garantizar el funcionamiento de seguridad de información se debe de tener un proceso documentado, sistemático, conocido por toda la empresa. Ver figura 01

Figura 02: Sistema de gestión de seguridad de información.



Fuente: ISO 27001

La información es un activo fundamental de toda empresa y debe estar resguardada de una manera adecuada. La seguridad de la información protege la continuidad del negocio, protege los datos de la empresa, Maximiza las oportunidades de negocio y minimiza los daños que pueden ocurrir en el transcurso de los años. (de Negocios et al. 2019)

Es un conjunto de medidas preventivas que ayudan a las organizaciones de los sistemas tecnológicas a proteger sus datos buscando mantener la confidencialidad, disponibilidad e integridad de su información. (Yagual, Tatiana 2017)

Si definimos la seguridad de la información seria como un conjunto de sistemas y procesos que ayudan a preservar los datos de una organización, sin embargo, para que una organización este protegido debe contar con los tres pilares de la seguridad de la información. (Yagual, Tatiana 2017) como se muestra en la figura N.º 03

Figura 03: Pilares de la Seguridad de Información

Fuente: Elaboración Propia

La confidencialidad: Asegura que solo las personas autorizadas puedan contar con el acceso a la información, garantiza que los datos no sean divulgados a otras entidades o personas que no trabajen en la empresa, se refiere a la privacidad de los datos almacenados en el sistema, este principio es muy importante para las empresas porque la mayoría de los datos pasan por equipos físicos donde es muy fácil poder perder información y por ello es fundamental que la confidencialidad de los datos este sumamente protegida. (Arango Mayorga, Karol Noemí,Oropeza Egoavil, Liliana,2017)

La confidencialidad busca prevenir el acceso a la información de forma controlada, es un principio fundamental que la información tenga un nivel de tratamiento que prevenga su divulgación no autorizada. La disponibilidad informática es la característica de proteger la fiabilidad y el acceso a los datos y recursos que maneja una organización. (Pedro Hernández, et al., 2018)

Integridad: Asegura que los datos, procesos y métodos son exactos y correctos, brinda la protección que la información no sea manipulado con actos maliciosos por personas no autorizadas, se refiera a la valides de los datos almacenados en el sistema, este principio garantiza los datos transportados o almacenados, asegurando que no haya ninguna alteración, pérdida o destrucción de la información ya sea de forma intencionada o accidental. (Colonia, P, et al., 2019)

Disponibilidad: Asegura la fiabilidad de la información y que los datos se encuentren disponible cuando lo requieran, la disponibilidad es una característica que brinda una fiabilidad en los datos y accesos oportunos por parte de los usuarios autorizados, la disponibilidad asegura que se pueda recuperar la información en el momento que se necesite evitando su bloqueo o pérdida, y pueda ser utilizado solamente por personas autorizadas en el momento que sea requerido. (Quiroz S. & Macías, et al., 2017).

Modelo PHVA O PDCA:

Es un modelo que ayuda a resolver problemas mediante procesos que permiten implementar cambios para tener una mejora continua, aborda analiza y soluciona problemas en organizaciones. El ciclo PHVA es un proceso de mejora continua que es flexible e iterativa. (Vidaurre peche sarita,2018)

El ciclo PDCA :

- Simplificar y mejorar un proceso de trabajo repetitivo
- Mejora y simplifica los procesos de un trabajo continuo.
- Desarrolla los procesos de nuevos negocios.
- Se implementa mejoras continuas.

- Se crean nuevos cambios y se reflejan resultados inmediatos.
- Los erros disminuyen y aumentan buenos resultados.
- Se dan soluciones múltiples constantemente.

El modelo PHVA tiene 4 pasos:

Planificar:

El primer paso es planificar las mejoras o procesos que se necesitan para cualquier proyecto, esto incluye todo tipo de información como: (Carmen Huamán Rodriguez,2021)

- Objetivos del proyecto
- Identificar los activos de la empresa
- Métricas de éxito
- Entregables o resultado final del proyecto
- Participantes del proyecto
- Cronograma del proyecto

HACER:

Después de haber planificado lo necesario que se va en función al proyecto el siguiente paso es ponerlo a prueba mediante varios tipos de propuesta o procedimientos que se acoplen a una solución para el proyecto. Calderón Arateco, et al., 2020

ACTUAR:

El siguiente paso consta en implementar las mejoras para que el proyecto tenga un funcionamiento exitoso. (QUIROZ CUADROS, 2019)

VERIFICAR:

El siguiente paso es la verificación de los procesos implementados se encuentren en funcionamiento y cumpla con lo necesario para que el proyecto sea exitoso Calderón Arateco, et al., 2020

El modelo PDCA (Plan, Do, Check, Act) tiene cuatro niveles que ayudan a mejorar los procesos de cualquier organización. En la figura 04 se muestra el ciclo PDCA

Figura 04: El ciclo PDCA

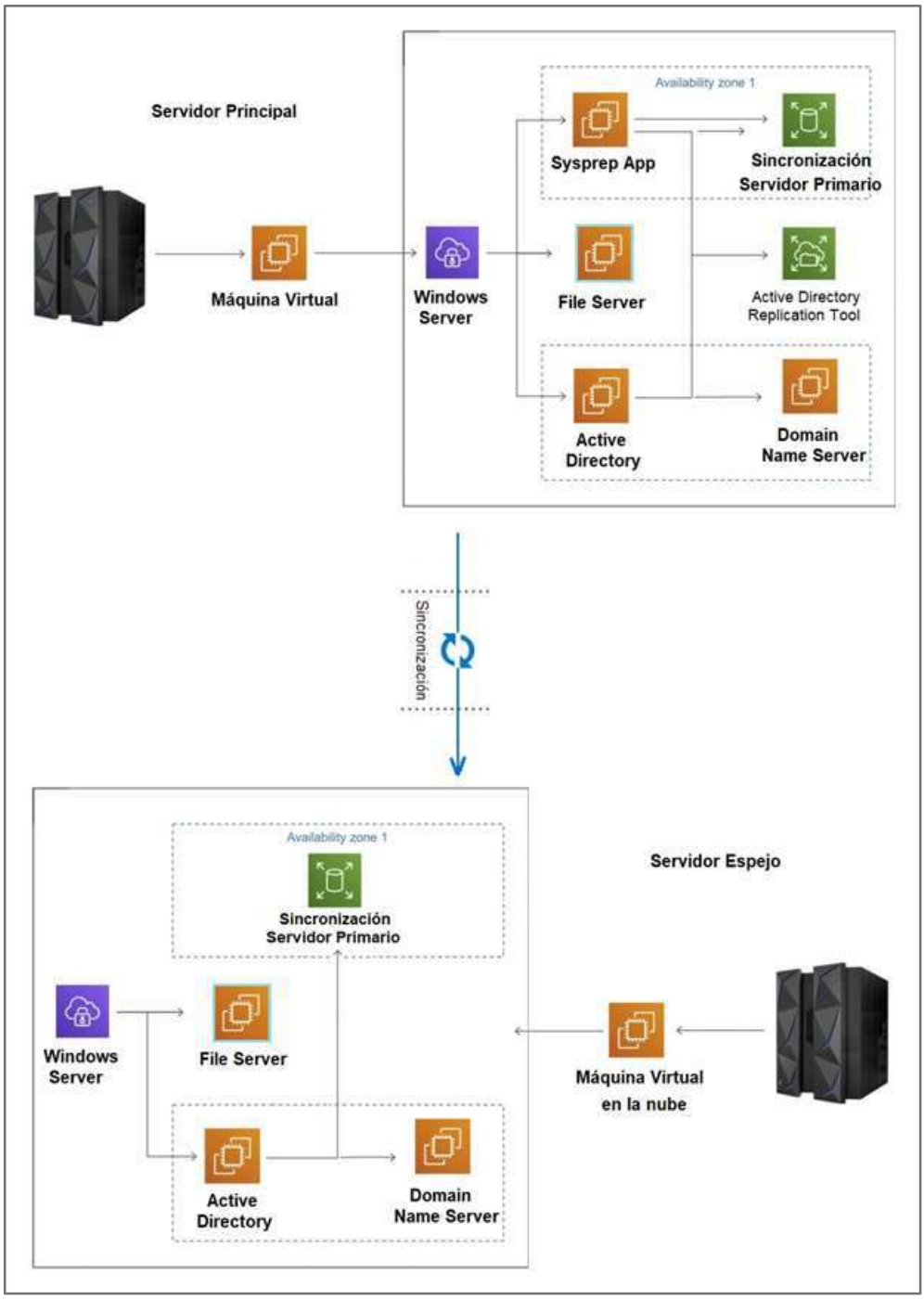
Fuente: Elaboración Propia

Arquitectura del servidor en la nube

En el siguiente gráfico se mostrarán los componentes de esta solución como son, el servidor principal alojado en una máquina virtual, el Windows Server que se instala en la misma, con la presencia importante del Directorio Activo y el DNS, y también el servidor espejo que para la práctica será instalado localmente también en una máquina virtual, en gráfico identifica claramente los elementos que forman parte de la arquitectura de un servidor espejo. Moreno Alvarado, et al., 2018

Este método de solución de un Servidor Espejo se caracteriza y lo diferencia de otros sistemas similares en contar en su arquitectura con un file server, es decir no solo va a ser un servidor de Directorio Activo, DNS y DHCP sino también un entorno que compartirá archivos con los demás usuarios de la red. July paola moreno alvarado, 2018 En la figura N.º 05 se visualiza la arquitectura de un servidor físico y de un servidor en la nube.

Figura 05 Arquitectura de un Servidor Espejo en la nube



Fuente: Elaboración propia

Son componentes tecnológicos que se combinan para construir una nube, donde los recursos se unen para hacer una virtualización y se comparten mediante la red. La arquitectura cuenta con componentes que incluyen: (Pierre armando rodríguez farías,2017)

- La plataforma Front-end: que es el cliente o dispositivo utilizado para acceder a la nube.
- Una plataforma Back-End: Aquí se encuentra los servidores y el almacenamiento de la información.
- Un modelo de distribución basado en la nube
- Una red

Todos estos componentes forman una arquitectura informática que brindan a los clientes la facilidad de manejar su red en un ambiente más protegido, cuidado y fiable para los datos de su organización.

Ventajas de la arquitectura en cloud:

Una de las ventajas de tener tu servidor en la nube es que permite eliminar o reducir cualquier riesgo en las tecnologías de información, brindando una mayor solución ante cualquier problema ocurrido en la red. (Serik, Mukhambetova, Yeskermessuly,2019)

La arquitectura de nube suele trasladar los recursos de TI a la nube publica, esto elimina la posibilidad de tener servidores físicos y almacenamiento locales

Los servidores en la nube dependiendo de la cantidad de servicios son mucho más económicos, no es necesario contar con un espacio físico, existen distintos planes de acuerdo a las necesidades, los cuales cuentan con mantenimiento y seguridad constante. .(Gutierrez Najarro, Jhon Edwin, 2021)

Los servidores cloud, son actualizados constantemente sin invertir demasiado tiempo y dinero en ellos.

Si la empresa está en constante crecimiento y necesita ampliar los recursos y capacidades en sus servidores, la mejor opción son los servidores en la nube, ya que aumentar los recursos se hacen de manera fácil, de manera rápida y sin largas esperas. (Loo Cuya 2018)

Los servidores en la nube pueden ampliar o disminuir sus recursos dependiendo de las necesidades de la empresa.

Un Servidor espejo es una réplica de un servidor ya existente, se utiliza principalmente como una medida de seguridad para salvaguardar la información que hay en el servidor principal. Aquí nace la importancia de los Servidores espejo ya que son útiles cuando el servidor original deja de funcionar por alguna falla técnica, ciber ataque, etc., ya que así el usuario puede continuar usando el servicio que su servidor principal le brinda, por ejemplo, servidor de directorio activo, de base de datos, de archivos, de correo, etc., (Hillmann, 2016)

Medios de Respaldo

Servidor Espejo: Un Servidor Espejo es la réplica de la información que tiene un servidor principal, su función es brindar seguridad a los datos que tiene una organización respaldándolo en otro servidor. Esta réplica nos ayuda a proteger los datos o base de datos que existe en los servidores de una empresa, ya que mantiene una alta disponibilidad de la seguridad de información que se manejan en las Pymes. (Hillmann, 2016)

Requerimiento para un servidor espejo:

- Procesador: Core™ i3-54 o Xeon® E3-1230 V3 y versiones posteriores
- Memoria RAM: 16GB
- Velocidad tarjeta de Red: 1Gbps
- Sistema Operativo: Windows Server 2016, 2019, Linux.

También es posible implementar servidores espejos con 12Gb de RAM, pero hemos optado por lo indicado, para que sea mejor durante el proceso ver Tabla 01.

Tabla 01: Tipos de servidores espejos

Servidor espejo sin balanceo	Servidor espejo con balanceo de software
Un servidor espejo es simplemente el que se encarga de hacer una copia igual que el servidor principal, muchas empresas utilizan este tipo de servidor espejo sin balanceo ya que solo lo utilizan como un sistema de sincronización, solo le asignan la misma IP del servidor principal, ante una caída del servidor principal, el espejo toma el lugar del principal y todo sigue funcionando correctamente.	El fail over permite tener un balance de forma inteligente, que permite que el tráfico de red se equitativamente mediante un Robin Dns. Como mínimo es necesario contar con 2 servidores que aporten al balance de los softwares informáticos (aplicación, DNS, etc.).

Fuente: Elaboración propia

Enfoques conceptuales

Herramientas Open Source

Una herramienta open source son programas libres de código abierto que son usados para la administración de diversos desarrolladores o administradores de red, estas herramientas ayudan a que los administradores de red puedan mejorar un inconveniente encontrado en sus redes mediante instalaciones que brinden una solución rápida, eficaz y sin ningún costo adicional. (Espino Timón, Martínez Fontes, 2017)

Estas herramientas han sido de gran uso en los últimos tiempos, ya que han brindado soluciones rápidas a inconvenientes de grandes impactos, por lo cual la empresa Microsoft también desarrollo herramientas de software libre que ayuden al usuario a dar soluciones tecnológicas en sus sistemas, sin ningún costo alguno, una de sus herramientas es sysprep que es gratuita y ayuda en la configuración de un servidor espejo en la nube.

Sysprep

Es una herramienta gratuita de Windows server que ayuda a la clonación de servidores principales de una organización, esta herramienta interactúa con los procesos de la red principal, y es muy usado para la creación de servidores espejos que permiten tener un respaldo de sus servidores y datos de las organizaciones. (Jorge López, 2021)

Servidor

Un servidor funciona a través de la red informática, el modelo más conocido es el cliente – servidor, el cliente puede ser un ordenador o una ampliación que requiera del uso del servidor para su función, por lo cual un servidor dispone la información demandada siempre y cuando el cliente tenga acceso autorizado a los datos del sistema. (Moreno Alvarado, 2018)

Tipos de Servidor

Los tipos de servidores son el servidor de dominio, el mail server, el file server, el DB server, web server, entre otros. En la siguiente Tabla, se muestra algunos de servidores más comunes.

Tabla 02: Tipo de Servidores

Nombre del Servidor	Funciones
Active Directory Server	Contiene una un conjunto de servicios y una BD que conectan a los usuarios con los recursos de red que necesitan para realizar sus actividades de estudio o laborales. Este directorio contiene información crítica de los usuarios y las computadoras que hay y quién puede hacer qué cosa de acuerdo a políticas establecidas.
Mail Server	Es el server que administra, almacena y delibera todas las operaciones de envío y recepción de los correos electrónicos entre la organización y sus clientes.
Proxy Server	Es el server que actúa de intermediario como medida de protección entre el servidor y el que usuario que realiza la petición de tal forma que

	el servidor no conoce quién es el cliente que está realizando esa petición.
Web Server	Gestiona y almacena toda la documentación HTML y se encarga de enviar dicha información a los clientes que la solicitan.
DB Server	Brinda servicios de gestión y almacenamiento de las bases de datos a sus clientes.
Clúster Server	Son servidores especializados en el almacenamiento de la información con gran capacidad que impide evitar la pérdida de información por problemas de otros servidores.
File Server	Servers encargados de almacenar y gestionar toda la información de los archivos texto de los usuarios de la red.
Servidores de imágenes y videos	Servidores de gran capacidad para almacenar y gestionar imágenes y videos, permitiendo administrarlos de forma eficiente para su uso en otros servidores, principalmente en el servidor web.

Fuente: Elaboración propia.

Cloud Computing

Es una tecnología que aporta a las TIC, una manera de poder facilitar el acceso de sus datos y de poder proteger sus servidores en la nube, esta tecnología pretende ser una alternativa ante servidores locales (físicos), permite tener una mejor gestión de toda tu infraestructura de red. (Barreda Ramírez, Lima -Perú 2017)

La computación en la nube ofrece a las personas y a las empresas la capacidad de obtener una gran variedad de recursos de computación con buen soporte, que sea seguro, de fácil acceso y bajo costo. (Alonso Tenorio Trigoso,2017)

Características esenciales:

a. Se solicita una especie de autoservicio, con un acceso amplio a la red, con recursos agrupados, crecimiento rápido y servicio medido.

b. Modelos de servicios: Como por ejemplo IASS, PASS y SASS.

c. Modelos de implementación: Las nubes públicas, privadas e híbridas.

El cloud computing es el uso de una red de servidores conectados a internet, es una virtualización ilimitada que protege los datos de información de una organización, permite dar acceso a los usuarios y gestionar las políticas de seguridad, a su vez brinda arquitecturas orientadas a servicios de las TIC. (Panfilova et al. 2021)

Los Beneficios de la Nube

La estabilidad y flexibilidad, trabajar desde cualquier lugar, reducción de costos en infraestructura, recuperación de datos antes algún incidente o desastre natural, actualizaciones automáticas, control de incidencias, disponibilidad de información en todo momento, procesos agiles, monitores de los proyectos, ubicación y dependencia del dispositivo, mejora la eficiencia, Archivos bien documentados, gastos de capital minimizados. (IDG, 2020).En la Tabla 03 se muestra la diferencia de los beneficios de las nubes públicas, privadas e híbridas:

Tabla 03: Tipos de Nube

	Nube Pública	Nube Privada	Nube Híbrida
Escalabilidad	Muy Amplia	Limitada	Muy amplia
Seguridad	Buena, depende de las medidas de seguridad del proveedor del servicio	Segura, el almacenamiento es local	La más segura, las opciones de integración permiten añadir todas las capas adicionales de seguridad
Rendimiento	Bajo o medio	Muy alto	Alto, el contenido activo se guarda en el caché de las instalaciones
Confiabilidad	Media, depende de La conexión a Internet y la calidad de servicio del proveedor	Alta, toda la infraestructura se encuentra en las instalaciones	Media-Alta, el caché se encontraría en las instalaciones, pero dependerá en cierta medida de conexión y disponibilidad

Costos	Muy bajos, al ser un tipo de pago de acuerdo al uso y evita gastos en infraestructuras de almacenamiento local	Bajos, pero requiere de altos costos de recursos locales como espacio para un data center, energía eléctrica o el sistema de enfriamiento	Bajos, ya que permite trasladar los recursos de almacenamiento al modelo de pago por uso

Fuente: Elaboración propia

Microsoft Azure

Es una plataforma de virtualización que pertenece a la familia de Microsoft que brinda beneficios de poder tener un respaldo de información de los datos de una organización, es público y pago por uso, permite hacer una implementación rápida como también tener una administración de todo el sistema, además ofrece máquinas virtuales para el desarrollo de un servidor espejo de cualquier organización, aquí se puede almacenar cualquier proyecto informático y cuenta con muchas aplicaciones para el buen uso de las tecnología de información. (Serik, Yeskerme suly, 2019)

Aplicaciones en Azure

Azure brinda gran capacidad de aplicaciones empresariales con los beneficios mostrados a continuación:

- Migración de los servidores a la nube con un entorno sólido, amigable, fácil estabilidad y sobre todo con una seguridad de respaldo de toda la información. (Ruiz Caldas, 2019)
- Mayor rendimiento de trabajo en la nube con una productividad del 100 % en almacenamiento y con más 80, 000 operaciones por segundo, lo cual brinda una mayor estabilidad en el sistema, brindando mejores resultados para el buen uso de la seguridad de información. (Vera-Rivera, Perez-Gutierrez, Urbina, 2016)

- Simplifica los datos y entorno de modelos empaquetados con el fin de que se ejecuten de forma inmediata y eficaz, estos modelos son mecanismos que son manipulables y flexibles para el manejo de las aplicaciones como Dynamics AX o Sharp point. (VMware, 2016)

- El soporte brindado por Azure es de nivel uno ya que cuenta con una gran eficiencia que permite a diferente herramientas, marcos o lenguajes de programación un buen funcionamiento en la nube y una optimización de los recursos del sistema.

- Azure ofrece los mejores precios para la optimización de los recursos del sistema, nos brinda soluciones distintas para el buen uso de las aplicaciones a un bajo costo, se puede tener licencia por uso que permite solo pagar en el momento que se utiliza la aplicación. (Macha Tejeda 2018)

Ventajas de Azure Cloud: Las ventajas que ofrece Azure es la reducción de costos de adquirir equipos físicos, ofrece almacenamiento en la nube de forma ilimitada, mantenimiento 24 x 7, gran facilidad de uso de la nube, copias y respaldo de toda la información de la empresa, Recuperación de archivos ante cualquier incidente ocurrido en la organización, fiabilidad de toda la información almacenado en los servidores, accesibilidad a los datos de forma rápida. (Martha Liliana Quevedo,2018)

Máquinas Virtuales

Las máquinas virtuales son ordenadores de software que ayudan a ejecuta sistemas operativos para el uso de algún requerimiento de una organización, también son usadas para trabajar en la nube mediante herramientas libres que permitan hacer un respaldo de todo tu servidor principal y de esa manera llevar una protección de la seguridad de información de los datos de la empresa. (Microsoft Azure, 2017)

III METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de Investigación

La presente tesis es aplicativa por ende se enfoca en la causa del evento físico y se orienta en brindar explicación de porqué ocurren los fenómenos de una organización. (Hernández Gracia, 2018)

La tesis es aplicada porque determina los procesos de la seguridad de información, mediante las dimensiones de confidencialidad, integridad, disponibilidad que ayuden a establecer procedimientos del buen uso de los sistemas informáticos.

Enfoque de Investigación:

La tesis es de enfoque cuantitativo porque observa la realidad, la describe, plantea el problema y valida la información de un sistema para hacer una mejora de procesos. (Armando, 2017)

Diseño de la Investigación

El diseño en este estudio es el Pre-Experimental, en este diseño se emplean variables independientes y dependientes que permiten estudiar los resultados de las intervenciones. (Cisneros, 2019)

La variable dependiente de la tesis observa el efecto de la variable independiente y este proceso se representa de la siguiente manera:

GE: 01 x 02

Dónde:

G.E. Estudiantes de la empresa New Fashion

01: Implementación de un servidor espejo usando herramientas open source en la nube (pre test).

X: Implementación del servidor espejo

02: Implementación de un servidor espejo usando herramientas open source en la nube (Post test)

3.2. Variables y operacionalización

Variable dependiente: Seguridad de Información

Son una serie de fracciones que se constituyen entre sí. Los procedimientos de los pilares de la seguridad de la información constituyen el porcentaje de la confidencialidad, integridad y disponibilidad de la información. (Mendoza, Garza, 2017)

Definición operacional:

La implementación del servidor espejo se empleará para resguardar la información que actualmente tienen las pymes en sus servidores y tomaremos en cuenta las dimensiones de los pilares de la seguridad de la información. (Torres-Rodríguez, Monroy-Muñoz, 2020)

La confidencialidad, integridad y disponibilidad, estas dimensiones ayudarán a proteger la seguridad de la información ante cualquier riesgo que pueda ocurrir en las pymes. En la tabla 04 podremos ver la matriz de operacionalización

UNIVERSIDAD CÉSAR VALLEJO

Tabla 04: Operacionalización de la variable dependiente Seguridad de Información

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	DATOS	INSTRUMENTO
Seguridad de información	La finalidad en la seguridad de la información es un concepto de medidas preventivas que ayudan a resguardar los datos de los sistemas en las organizaciones (Juan A. Figueroa-Suárez, n.d. 2018))	Esta variable utilizará la técnica de observación y el instrumento de lista de cotejo para determinar las dimensiones de los pilares de la seguridad de la información, que son la confidencialidad, integridad y disponibilidad.	Confidencialidad	Incidentes de acceso indebido a los documentos.	Incidentes de acceso indebido.	Observación Lista de Cotejo
				Control de documentos	Accesos indebidos a los documentos	
				Contraseñas	Claves de seguridad	
				Seguridad de datos	Datos controlados	
				Fugas de información	Equipos portátiles.	
				Soporte de los datos de información	Soportes deinformación.	
			Integridad	Incidentes en la integridad de los documentos	Incidentes de impacto a la integridad más comunes	Observación Lista de Cotejo
				Frecuencia de incidentes en la integridad de los datos de información	Incidentes de impacto en la integridad.	
				Integridad de documentos y control.	Documentos y controlde versiones.	
			Disponibilidad	Seguridad Física y del entorno	Disponibilidad de los activos	Observación Lista de Cotejo
				Incidentes en la disponibilidad de la información	Disponibilidad de documentos comunes	
				Disponibilidad de servicios de información	Vectores de pérdida de disponibilidad de información.	

Fuente: elaboración propia.

3.3. Población

La población que se usó para desarrollar el proyecto de investigación se basó en la recolección de la información que se hizo a la empresa New Fashiòn, La primera visita que se hizo a las instalaciones se pudo observar los déficit que tenía sobre la seguridad de la información de sus datos, la segunda visita que se hizo a la empresa fue para seguir evaluando como se encontraba respaldados sus datos de los sistema de la organización, la tercera visita fue para validar que todo lo revisado y evaluado este de forma correcta y no hayamos tenido ningún indicador que se haya olvidado evaluar.

Muestra:

La muestra es un subconjunto de la población total, en la tesis se empleó la fórmula de la técnica de muestreo aleatorio simple la cual se determina a continuación: (Soto Abanto, 2018)

En la tesis la muestra fue el total de resultados de la evaluación de las tres visitas que se hicieron a la empresa donde se evaluó las 7 áreas que tenía la pyme lo cual se usó la lista de cotejo que contenía las dimensiones de confidencialidad, integridad y disponibilidad de la seguridad de su información.

3.4. Técnicas e instrumentos de recolección de datos

Es el procedimiento que ayuda a la investigación a percibir un acontecimiento y recoger información sobre el problema, cuenta con instrumentos que ayudan a proteger la información como, por ejemplo: un cuestionario, una entrevista, una filmadora, una lista de cotejo, etc., son factores que permiten llevar un registro más eficiente durante la investigación. (Hernández & Carpio, et al., 2019).

En la presente tesis se utilizó la observación como técnica ya que brinda un contacto directo con el problema y así ayuda a recoger toda la información necesaria que tiene la organización, para esta técnica se tuvo contacto directo con las áreas involucradas de la pyme, las cuales fueron Gerencia, Logística, Producción, Sistemas, Comercial, Finanzas y recursos Humanos.

En la presente investigación se usó la lista de cotejo, que permite evaluar o verificar la presencia o ausencia de procedimiento, conocimientos y actitudes sobre la seguridad de la información, se utilizó tres dimensiones los cuales fueron la confidencialidad, integridad y disponibilidad, cada dimensión contenía indicadores que ayudaron a poder evaluar la empresa mediante las siguientes posibilidades: “Si Cumple, Cumple Parcialmente, No Cumple”.

Validez de expertos:

Es el método de validación útil que ayuda a verificar la fiabilidad de la tesis, teniendo en cuenta expertos en la materia que ayuden a validar que se cumpla con todos los estándares para la implementación de la tesis. (Vergara Quiroz, Gladis, et al., 2017)

La tesis ha sido evaluada por docentes que tienen gran experiencia en la materia, los cuales se considera los criterios de valoración, calificar la precisión, la objetividad, motivación, empatía, solides, relación, optimismo, y la metodología a fin de verificar los procedimientos de la seguridad de información en las pymes, En la tabla N°06 se muestra la validez que se obtuvo en la tesis.

Tabla 05: Validez de expertos

Experto	Confidencialidad de Seguridad de información	Integridad de Seguridad de información	Disponibilidad de Seguridad de información
Nemías Saboya Ríos	98%	98%	98%
Johan Alarcón Cajas	96%	96%	96%
Promedio	97%	97%	97%

Fuente: Elaboración propia.

3.5. Procedimientos

La implementación de la tesis se realizó de manera presencial en la empresa New Fashion Perú y para ello se emitió una carta de presentación al gerente de la empresa la cual fue aprobada mediante una carta de aceptación de la tesis que se adjuntó a los anexos. Se realizó también una reunión con el gerente general de la empresa y el jefe de producción de New Fashion Perú para pactar el inicio de las fechas de trabajo y la forma de colección de los datos de la lista de cotejo, este consentimiento también fue aprobado y firmado por gerencia. La lista de cotejo se realizó en tres ocasiones asistiendo de forma presencial a la empresa, estas visitas fueron monitoreadas por el jefe de Producción, lo que ayudó a tener un mejor control de los procedimientos de la lista de cotejo.

3.6. Método de análisis de datos

En la presente tesis se empleó el análisis descriptivo - comparativo, que se detallan a través de tablas de frecuencia simple, Adicionalmente, se aplicó pruebas de hipótesis de acuerdo con el comportamiento de los datos para el cumplimiento de ciertos supuestos que se indicó a los investigadores referente al tipo de prueba. La prueba empleada fue la no paramétrica, y se usó la prueba de Wilcoxon.

3.7. Aspectos éticos

En el trabajo de investigación se tomó en cuenta diferentes autores que aportaron información sobre cómo proteger la seguridad de información, así como también se usaron las diversas bases de datos brindadas por la UCV, en la tesis se utilizaron citas sobre las dimensiones de los pilares de la seguridad de la información, que ayudaron a efectuar los procedimientos de la lista de cotejo. Se asegura la veracidad de los resultados obtenidos de diferentes trabajos de investigación.

La tesis elaborada está libre de copia de cualquier trabajo de investigación, se garantiza el cumplimento de estándares propuestos por la UCV.

Se garantiza que todo información o resultado obtenido por la empresa se mantendrá en el anonimato y no será publicada, para respetar las normas y lineamentos de la información de la empresa.

Se empleará la ISO 690 para citar los autores que se usaron en la tesis de investigación, se mencionan en las referencias bibliográficas.

Se mantendrá en total confidencialidad los datos obtenidos por las áreas de la empresa.

IV RESULTADOS

Resultados descriptivos

Resultado descriptivo de nivel de confidencialidad

Los resultados obtenidos en el pre test, utilizando la lista de cotejo, dio como resultado que la empresa no cumplía en un 100.0%. Con estos datos, se plantearon e implementaron las mejoras mediante un método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source, que fortaleció a la empresa en la gestión de los incidentes de la seguridad de información, control de documentos, gestión de contraseñas, gestión de seguridad de datos, gestión de fugas de información y soporte de los datos de información. Teniendo como resultados en el post test, que el nivel de no cumplimiento disminuyó a un 0%, el nivel de cumplimiento parcialmente aumentó a un 14.3% y el nivel de cumplimiento aumentó a un 85.7% (ver tabla 06).

Tabla 06: Nivel de confidencialidad de la empresa

Niveles	Antes		Después	
	Frecuencia	Porcentaje	Frecuencia	Porcentaje
No cumple	7	100.0	0	0.0
Cumple parcialmente	0	0.0	1	14.3
Cumple	0	0.0	6	85.7
Total	7	100.0	7	100.0

Fuente: Elaboración propia

Resultado descriptivo de nivel de integridad

Los resultados obtenidos en el pre test, utilizando la lista de cotejo, dio como resultado que la empresa no cumplía en un 85.7% y cumplía parcialmente en un 14.3%. Con estos datos, se plantearon e implementaron las mejoras mediante un método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source, que fortaleció a la empresa en prevenir los incidentes la integridad de los documentos, en disminuir la frecuencia de incidentes en la integridad de los datos y en crear políticas de cumplimiento y control de los datos. Teniendo como resultados en el post test, que el nivel de no

cumplimiento disminuyó a un 0.0%, el nivel de cumplimiento parcialmente aumentó a un 28.6% y el nivel de cumplimiento aumentó a un 71.4% (ver tabla 07).

Tabla 07: Nivel de integridad de la empresa

Niveles	Antes		Después	
	Frecuencia	Porcentaje	Frecuencia	Porcentaje
No cumple	6	85.7	0	0.0
Cumple parcialmente	1	14.3	2	28.6
Cumple	0	0.0	5	71.4
Total	7	100.0	7	100.0

Fuente: Elaboración propia

Resultado descriptivo de nivel de disponibilidad

Los resultados obtenidos en el pre test, utilizando la lista de cotejo, dio como resultado que la empresa no cumplía en un 100.0%. Con estos datos, se plantearon e implementaron las mejoras mediante un método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source, que fortaleció a la empresa en prevenir la seguridad física de los servidores y del entorno donde se trabaja, se disminuyó los incidentes en la disponibilidad de la información y se mejoró los servicios de información. Teniendo como resultados en el post test, que el nivel de no cumplimiento disminuyó a un 0.0%, y el nivel de cumplimiento aumentó a un 100.0% (ver tabla 08).

Tabla 08: Nivel de disponibilidad de la empresa

Niveles	Antes		Después	
	Frecuencia	Porcentaje	Frecuencia	Porcentaje
No cumple	7	100.0	0	0.0
Cumple parcialmente	0	0.0	0	0.0
Cumple	0	0.0	7	100.0
Total	7	100.0	7	100.0

Fuente: Elaboración propia

Resultados inferenciales

Contraste de hipótesis de confidencialidad

Formulación de hipótesis

$\boldsymbol{H_0}$**:** El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source no contribuyó en la confidencialidad de la seguridad de información en las pequeñas y medianas empresas.

$\boldsymbol{H_a}$**:** El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source contribuyó en la confidencialidad de la seguridad de información en las pequeñas y medianas empresas.

Nivel de confianza

Para el presente estudio, se está teniendo en cuenta un nivel de confianza del 95% y un nivel de significancia del $\boldsymbol{\alpha = 0.05}$

Regla de decisión

Si $\boldsymbol{sig > \alpha}$., se acepta $\boldsymbol{H_0}$; Si $\boldsymbol{sig < \alpha}$, se rechaza $\boldsymbol{H_0}$

Prueba de estadística

Para la prueba se utilizó el estadístico de la prueba de Wilcoxon, debido a que la variable cualitativa ordinal, no requiere de la prueba de normalidad de los datos, ya que es una prueba no paramétrica y la fórmula se detalla a continuación:

$$T = Min[T(+), T(-)]$$

Donde determina que T se ajusta a una distribución normal por lo que se debe utilizar la siguiente fórmula:

$$Z = \frac{\mathrm{T} - \mathrm{n(n+1)/4}}{\sqrt{\mathrm{n(n+1)(2n+1)/24}}}$$

Resultados utilizando el programa estadístico SPSS 26.0

Los resultados obtenidos después de la evaluación de los datos, indicó que 7 áreas incrementaron su nivel de confidencialidad, y no hubo ningún área en reducir la confidencialidad. El rango negativo fue de ($\bar{x}$ = 4.00), resultado que es inferior al positivo ($\bar{x}$ = 0.00), lo que implica los resultados del post test fueron inferiores en 7 áreas, demostrando de esta manera que el método implementado, contribuyó en

incrementar la confidencialidad en la empresa New Fashion Perú. Asimismo, la suma de rango indica el resultado a favor de estudio (ver tabla 09).

Tabla 09**:** Rangos comparativos de la prueba de Wilcoxon para el nivel de Confidencialidad

Resultados de los indicadores de Confidencialidad		**N**	**Rango promedio**	**Suma de rangos**
Pre - Post	Rangos negativos	7	4.00	28.00
	Rangos positivos	0	0.00	0.00
	Empates	0		
	Total	**7**		

Fuente: Elaboración propia

Por otro lado, en la tabla 10 muestra los resultados obtenidos de la prueba de Wilcoxon a través de una aproximación de la normal Z, con resultados $\boldsymbol{Z = -2.530}$ donde el valor $\boldsymbol{sig = 0,011}$ siendo $\boldsymbol{sig < 0,05}$, de mostrando que los datos respecto a la confidencialidad del pre test y post test presentan diferencias significativas que favorecieron al estudio.

Tabla 10: Estadísticos de prueba de Wilcoxon para el nivel de Confidencialidad

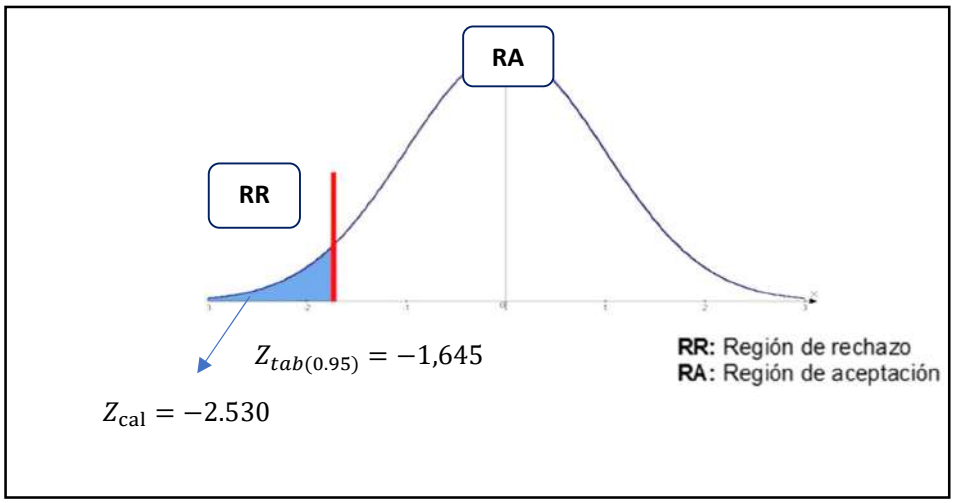
Prueba	**Pre - Post**
Z	-2,530
Sig. asintótica(bilateral)	0.011

Fuente: Elaboración propia

Distribución de la prueba estadística

Para lograr la decisión del contraste de hipótesis se requirió del uso de la distribución normal, representada como $\boldsymbol{Z_{tab} = (1 - \alpha)}$, en donde al reemplazar los valores se obtuvo $\boldsymbol{Z_{tab} = (0.95) = -1.645,}$ este resultado sirvió como límite para comparar el valor de $\boldsymbol{Z_{cal} = -2.530}$, el cual se comparó gráficamente utilizando la campana de Gauss que se visualiza en la figura 06

Figura 06 Campana de Gauss Nivel de Confidencialidad



Fuente: Elaboración propia

En donde, $\boldsymbol{Z_{cal} < Z_{tab}}$ y se encuentra en la región de rechazo, por lo que se decide a rechazar la hipótesis nula, concluyendo que, existe evidencia estadística que acredita que las áreas analizadas muestran resultados distintos y favorables para el estudio, es decir, que después de aplicar el método de ingeniería, existe una mejora en el nivel de confidencialidad de la empresa con un 95% de confianza.

Contraste de hipótesis de integridad

Formulación de hipótesis

$\boldsymbol{H_0}$**:** El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source no contribuyó en la integridad de la seguridad de información en las pequeñas y medianas empresas.

$\boldsymbol{H_a}$**:** El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source contribuyó en la integridad de la seguridad de información en las pequeñas y medianas empresas.

Nivel de confianza

Para el presente estudio, se está teniendo en cuenta un nivel de confianza del 95% y un nivel de significancia del $\boldsymbol{\alpha = 0.05}$

Regla de decisión

Si $\boldsymbol{sig > \alpha}$., se acepta $\boldsymbol{H_0}$; Si $\boldsymbol{sig < \alpha}$, se rechaza $\boldsymbol{H_0}$

Prueba de estadística

Para la prueba se utiliza el estadístico de la prueba de Wilcoxon para muestras relacionadas, debido a que la variable seguridad de la información y la dimensión de integridad no cumplieron el supuesto de normalidad y la fórmula se detalla a continuación:

$$T = Min[T(+), T(-)]$$

Donde determina que T se ajusta a una distribución normal por lo que se debe utilizar la siguiente fórmula:

$$Z = \frac{\mathrm{T} - \mathrm{n}(\mathrm{n}+1)/4}{\sqrt{\mathrm{n}(\mathrm{n}+1)(2\mathrm{n}+1)/24}}$$

Resultados estadísticos de prueba utilizando el programa SPSS 26.0

Los resultados obtenidos después de la evaluación de los datos, indicó que 7 áreas incrementaron su nivel de integridad, y no hubo ningún área en reducir la integridad de la información. El rango negativo fue de ($\bar{x}$ = 4.00), resultado que es inferior al positivo ($\bar{x}$ = 0.00), lo que implica los resultados del post test fueron inferiores en 7 áreas, demostrando de esta manera que el método implementado, contribuyó en incrementar la integridad en la empresa New Fashion Perú. Asimismo, la suma de rango indica el resultado a favor de estudio (ver tabla 11).

Tabla 11: Rangos comparativos de la prueba de Wilcoxon para el nivel de Integridad

Resultados de los indicadores de Integridad		**N**	**Rango promedio**	**Suma de rangos**
Pre - Post	Rangos negativos	7	4.00	28.00
	Rangos positivos	0	0.00	0.00
	Empates	0		
	Total	**7**		

Fuente: Elaboración propia

Por otro lado, en la tabla 12 muestra los resultados obtenidos de la prueba de Wilcoxon a través de una aproximación de la normal Z, con resultados $\boldsymbol{Z = -2.428}$ donde el valor $\boldsymbol{sig = 0,015}$ siendo $\boldsymbol{sig < 0,05}$, de mostrando que los datos

respecto a la integridad del pre test y post test presentan diferencias significativas que favorecieron al estudio

Tabla 12: Estadísticos de prueba de Wilcoxon para el nivel de Integridad

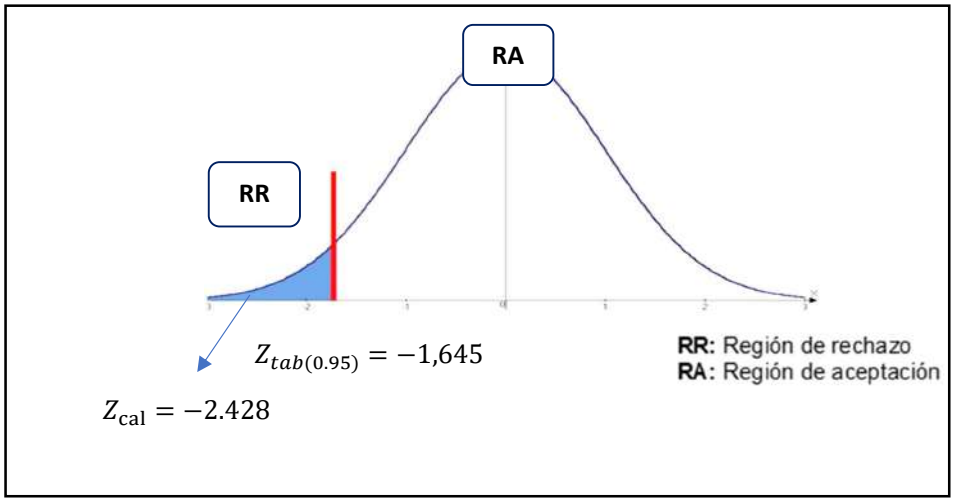
Prueba	Pre - Post
Z	-2,428
Sig. asintótica(bilateral)	0.015

Fuente: Elaboración propia

Distribución de la prueba estadística

Para lograr la decisión del contraste de hipótesis se requirió del uso de la distribución normal, representada como $\boldsymbol{Z_{tab} = (1 - \alpha)}$, en donde al reemplazar los valores se obtuvo $\boldsymbol{Z_{tab} = (0.95) = -1.645}$, este resultado sirvió como límite para comparar el valor de $\boldsymbol{Z_{cal} = -2.428}$, el cual se comparó gráficamente utilizando la campana de Gauss que se visualiza en la figura 07

Figura 07 Campana de Gauss Nivel de Integridad



Fuente: Elaboración propia

En donde, $\boldsymbol{Z_{cal} < Z_{tab}}$ y se encuentra en la región de rechazo, por lo que se decide a rechazar la hipótesis nula, concluyendo que, existe evidencia estadística que

acredita que las áreas analizadas muestran resultados distintos y favorables para el estudio, es decir, que después de aplicar el método de ingeniería, existe una mejora en el nivel de integridad de la empresa con un 95% de confianza.

Contraste de hipótesis de disponibilidad

Formulación de hipótesis

$\boldsymbol{H_0}$**:** El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source no contribuyó en la disponibilidad de la seguridad de información en las pequeñas y medianas empresas.

$\boldsymbol{H_a}$**:** El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source contribuyó en la disponibilidad de la seguridad de información en las pequeñas y medianas empresas.

Nivel de confianza

Para el presente estudio, se está teniendo en cuenta un nivel de confianza del 95% y un nivel de significancia del $\boldsymbol{\alpha = 0.05}$

Regla de decisión

Si $\boldsymbol{sig > \alpha}$., se acepta $\boldsymbol{H_0}$; Si $\boldsymbol{sig < \alpha}$, se rechaza $\boldsymbol{H_0}$

Prueba de estadística

Para la prueba se utiliza el estadístico de la prueba de Wilcoxon para muestras relacionadas, debido a que la variable seguridad de la información y la dimensión de integridad no cumplieron el supuesto de normalidad y la fórmula se detalla a continuación:

$$T = Min[T(+), T(-)]$$

Donde determina que T se ajusta a una distribución normal por lo que se debe utilizar la siguiente fórmula:

$$Z = \frac{\mathrm{T} - \mathrm{n}(\mathrm{n}+1)/4}{\sqrt{\mathrm{n}(\mathrm{n}+1)(2\mathrm{n}+1)/24}}$$

Resultados utilizando el programa estadístico SPSS 26.0

Los resultados obtenidos después de la evaluación de los datos, indicó que 7 áreas incrementaron su nivel de disponibilidad y no hubo ningún área en reducir la integridad de la información. El rango negativo fue de ($\bar{x}$ = 4.00), resultado que es inferior al positivo ($\bar{x}$ = 0.00), lo que implica los resultados del post test fueron inferiores en 7 áreas, demostrando de esta manera que el método implementado, contribuyó en incrementar la disponibilidad de la información en la empresa New Fashion Perú. Asimismo, la suma de rango indica el resultado a favor de estudio (ver tabla 13).

Tabla 13: Rangos comparativos de la prueba de Wilcoxon para el nivel de Disponibilidad

Resultados de los indicadores de Disponibilidad		**N**	**Rango promedio**	**Suma de rangos**
Pre – Post	Rangos negativos	7	4.00	28.00
	Rangos positivos	0	0.00	0.00
	Empates	0		
	Total	**7**		

Fuente: Elaboración propia

Por otro lado, en la tabla 12 muestra los resultados obtenidos de la prueba de Wilcoxon a través de una aproximación de la normal Z, con resultados $\boldsymbol{Z = -2.646}$ donde el valor $\boldsymbol{sig = 0,008}$ siendo $\boldsymbol{sig < 0,05}$, de mostrando que los datos respecto a la disponibilidad del pre test y post test presentan diferencias significativas que favorecieron al estudio

Tabla 14: Estadísticos de prueba de Wilcoxon para el nivel de Disponibilidad

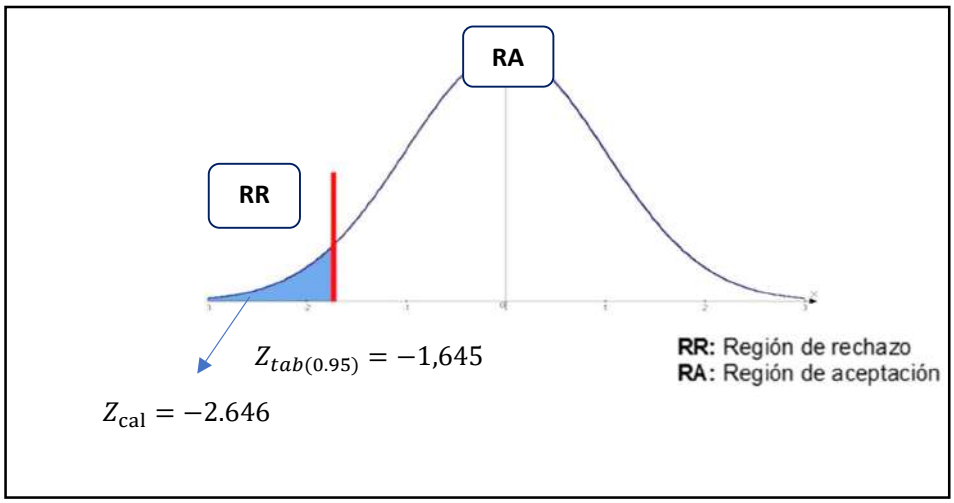
Prueba	**Pre - Post**
Z	-2,646
Sig. asintótica(bilateral)	0.008

Fuente: Elaboración propia

Distribución de la prueba estadística

Para lograr la decisión del contraste de hipótesis se requirió del uso de la distribución normal, representada como $\boldsymbol{Z_{tab} = (1 - \alpha)}$, en donde al reemplazar los valores se obtuvo $\boldsymbol{Z_{tab} = (0.95) = -1.645,}$ este resultado sirvió como límite para comparar el valor de $\boldsymbol{Z_{cal} = -2.646}$, el cual se comparó gráficamente utilizando la campana de Gauss que se visualiza en la figura 08

Figura 08 Campana de Gauss Nivel de Disponibilidad



Fuente: Elaboración propia

En donde, $\boldsymbol{Z_{cal} < Z_{tab}}$ y se encuentra en la región de rechazo, por lo que se decide a rechazar la hipótesis nula, concluyendo que, existe evidencia estadística que acredita que las áreas analizadas muestran resultados distintos y favorables para el estudio, es decir, que después de aplicar el método de ingeniería, existe una mejora en el nivel de disponibilidad de la empresa con un 95% de confianza.

V DISCUSIÓN

En el presente proyecto, como propósito de determinar la influencia de un método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source, orientado a resguardar y sincronizar los datos del sistema para la empresa New Fashion Perú, se obtuvieron como resultados en la confidencialidad de los datos el valor sig = 0.011< α = 0.05, en la integridad de los datos el valor sig = 0.015< α = 0.05 y en la disponibilidad de los datos el valor sig = 0.008< α = 0.05, a través de la prueba no paramétrica de Wilcoxon. Lo que demuestra que el método contribuyó favorablemente a respaldar y sincronizar los datos de los servidores. Esto significa que gracias a que los datos han sido sincronizados y resguardados en un servidor espejo con herramientas Open Source en la nube, ayudo a que la empresa esté protegida ante un eventual siniestro que perjudique la pérdida de sus datos del sistema, brindo mejoras en los niveles de confidencialidad, integridad y disponibilidad de sus datos. Demostrando de esta manera que es factible el rechazo de la hipótesis nula a favor de la alterna, lo que demuestra que el método influyó favorablemente en resguardar los datos del sistema. Estos resultados son respaldados por Guardia Tamara (2018), quien refiere que para proteger la seguridad de la información se debe desarrollar un método que permita minimizar los datos informáticos, que ayude a detectar las amenazas y vulnerabilidad que tiene el sistema, a fin de dar un tratamiento que ayude a mitigar los riesgos y aumentar la protección de los datos de la organización. De la misma manera Rene Zuña Macancela (2019), según su estudio, indica que para proteger los datos de las empresas es necesario implementar métodos que permitan salvaguardar la información y contar con sistemas de protección que brinden soluciones eficientes ante cualquier ataque mediante la red, daños físicos o catástrofe natural. Asimismo, los autores Farfán, Blas y Pedro, Deyner (2021), quienes indican en su tesis, que el objetivo es mejorar la disponibilidad web del sitio web del colegio La Asunción de Trujillo, para realizar esta evidencia usaron herramientas web gratuitas y de alta disponibilidad, el estado actual del parámetro disponibilidad, y posteriormente diseñaron e implementaron un servidor tipo espejo para mejorar las condiciones y finalmente volvieron a medir el requerimiento no funcional de disponibilidad. El tipo de investigación, que realizaron, fue no

experimental con enfoque cualitativo, y finalmente concluyeron y observaron una mejora del 2.5466% respecto a la disponibilidad web del servidor, asegurando así, una mejora respecto a la competencia y suponiendo una reducción de costos para la institución por sobre los otros colegios de la región.

En tal sentido y por lo que se mencionó anteriormente, se puede confirmar que es de mucha importancia aplicar métodos que ayuden a proteger la confidencialidad, integridad y disponibilidad de la información, ya que las empresas necesitan contar con los datos del sistema en línea, y estar protegidos ante cualquier ataque que impida contar con los datos del sistema, para que faciliten la toma de decisiones de la empresa.

VI CONCLUSIONES

Se puede implementar un método de seguridad basado en Servidores Espejos en la nube, utilizando herramientas Open Source que ayudan a respaldar la información de los datos del servidor físico a la nube.

El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source, ayudó a que la empresa tenga el soporte para proteger la información de sus servidores, realizando copias de seguridad de los datos semanalmente; además mejoró en la gestión de seguridad de datos y en reducir las fugas de información limitando las capacidades de los usuarios para que no puedan acceder a información confidencial de la empresa. Se obtuvo un incremento en el nivel de cumplimiento de confidencialidad de 0.0% a 85.7 %, lo que demostró que la implementación del método ayudó favorablemente en proteger y gestionar los datos del sistema.

Ayudó a que la empresa encuentre los datos en forma completa y precisa en los servidores; también, a que cuente con un método de seguridad ante algún incidente generado con su información y de que cada usuario esté capacitado con los procedimientos a seguir ante cualquier mal acto en contra de la integridad de los datos de la empresa. Se obtuvo un incremento en el nivel de cumplimiento de integridad de 0.0% a 71.4 %, lo que demostró que la implementación del método ayudó favorablemente en proteger los datos del sistema.

Asimismo, con este proyecto se logró que la empresa cuente con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos y que, ante un desastre natural o daño físico ocasionado por algún usuario a los datos del sistema de la empresa, este se encuentre protegido y almacenado en los servidores espejos con copias de seguridad que respaldan la disponibilidad de los datos de la empresa. Se obtuvo un incremento en el nivel de cumplimiento de disponibilidad de 0.0% a 100%, lo que demostró que la implementación del método ayudó favorablemente en contar con una eficiente administración de sus datos en sus servidores.

RECOMENDACIONES

Se sugiere ampliar la investigación científica a mayor número de tiempo (periodos de evaluación), con la finalidad de poder fortalecer el método aplicado en este proyecto, consiguiendo así un mejor resultado en los porcentajes de cumplimiento en la seguridad de la información mediante servidores espejos.

Por otro lado, se sugiere que para la investigación se pueda utilizar una mayor muestra o población de mayor tamaño, con la finalidad de que la implementación del método de seguridad de información de los datos pueda ser aplicada para medianas y grandes empresas.

Asimismo, se sugiere reconstruir o implementar medidas importantes que ayuden a proteger la seguridad de autentificación y acceso a datos, según los lineamientos y directivas de la seguridad de la información, a fin de resguardar el acceso a la información de la empresa.

Finalmente, para las futuras investigaciones relacionadas a la presente tesis, se recomienda que se implementen métodos de respaldo de información de los datos del sistema, utilizando otras normas de seguridad de información, considerando factores y estándares de seguridad de información, a fin de proteger los datos de la empresa.

REFERENCIAS

Calderón arateco laura lorena, 2020. Seguridad informatica y seguridad de informacion. Artículo seguridad de la información. 2020.

Cisneros, isaac, 2019. Diseño de investigación: in: diseños de investigación.

Colonia, pedro jesús, 2019. Propuesta de un sistema de gestión de seguridad de la información con normas iso 27001 para la municipalidad distrital de la buena vista alta - casma; 2017.

Damián lópez, víctor gerónimo, 2020. Emprendedores y pymes en el perú. Economía & negocios. 2020. Vol. 2, no. 1. Doi 10.33326/27086062.2020.1.903.

De un servidor de dominio espejo para la mejora de, implementación, farfán, blas, cruz zaldívar, de la, pedro, deyner and -perú, trujillo, no date. Facultad de ingenieria escuela academico profesional de ingenieria de sistemas.

Espino timón, carlos and martínez fontes, xavier, 2017. “análisis predictivo: técnicas y modelos utilizados y aplicaciones del mismo - herramientas open source que permiten su uso. 26/27. 2017. Vol. I, no. Principio activo y prestación ortoprotésica.

Guerra, erick, neira, harold, díaz, jorge l. And patiño, janns, 2021. Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. Información tecnológica. October 2021. Vol. 32, no. 5, pp. 145–156. Doi 10.4067/s0718-07642021000500145.

Hernández, carlos e. And carpio, natalia, 2019. Introducción a los tipos de muestreo. Alerta revista científica del instituto nacional de salud. 2019. Vol. 2, no. 1. Doi 10.5377/alerta.v2i1.7535.

Hernández gracia, josé francisco, 2018. Tipos de investigación. Boletín científico de la escuela superior atotonilco de tula. 2018. Vol. 5, no. 9. Doi 10.29057/esat.v5i9.2885.

Hernandez, sergio daniel, 2018. El reto de la era digital: privacidad y confidencialidad de la información de pacientes. Revista gen. 2018. Vol. 72, no. 1.

Hillmann, peter, uhlig, tobias, rodosek, gabi dreo and rose, oliver, 2016. Modeling the location selection of mirror servers in content delivery networks. In: proceedings - 2016 ieee international congress on big data, bigdata congress 2016. 2016. Doi 10.1109/bigdatacongress.2016.68.

Idg, 2020. 2020 cloud computing study • idg. Estudio de computación en la nube 2020. 2020.

Izquierdo, j and tafur, t, 2017. Mecanismos de seguridad para contrarrestar ataques informaticos en servidores web y base de datos. Universidad señor de sipán. Online. 2017. Pp. 86–90. Retrieved from: http://repositorio.uss.edu.pe/handle/uss/4062

Jorge l., 2021. Sysprep en windows 2016/2019. . 12 february 2021.

Maquera quispe, henry george and serpa guillermo, paola nhataly, 2019. Gestión de activos basado en iso/iec 27002 para garantizar seguridad de la información. Ciencia & desarrollo. 2019. No. 21. Doi 10.33326/26176033.2017.21.736.

Mendoza, j. And garza, j. B., 2017. La medición en el proceso de investigación científica: evaluación de validez de contenido y confiabilidad. Revista innovaciones de negocios. 2017. Vol. 6, no. 11. Doi 10.29105/rinn6.11-2.

Microsoftazure, 2017. Qué es virtualización. Azure.microsoft.com. 2017.

Panfilova, elena, lukyanova, anna, pronkin, nikolay and zatsarinnaya, elena, 2021. Assessment of the impact of cloud technologies on social life in the era of digitalization. International journal of interactive mobile technologies. 2021. Vol. 15, no. 21, pp. 144–157. Doi 10.3991/ijim.v15i21.22985.

Quiroz, silvia and macías, david, 2017. Seguridad en informática: consideraciones. Dominio de las ciencias, issn-e 2477-8818, vol. 3, nº. Extra 3, 2017, págs. 676-688. 2017. Vol. 3, no. 3.

Ranulfo cuesta-quintero, fabián, anderson coronel-rojas, luis, rico-bautista, dewar, barrientos-avendaño, edwin, oscar josé montañez-vergel, ing and carlos mario páez-noriega, ing, no date. Sistema de detección de intrusos a través de una red

honeynet para entornos de red cableada sobre ipv6 intrusion detection system through a honeynet network for network environments wired on ipv6. .

Ruiz caldas, angel. Junior., 2019. Migración de servidores a la nube de microsoft azure para mejorar la continuidad de los servicios de ti, de la fiduciaria en el año 2018. Universidad san ignacio de loyola. 2019.

Serik, meruert, mukhambetova, meiramgul and yeskermessuly, alibek, 2019. Improving the content of a client-server technology training course: set up and collaborative implementation of local and cloud-based remote servers. International journal of emerging technologies in learning. 2019. Vol. 14, no. 21, pp. 191–204. Doi 10.3991/ijet.v14i21.10643.

Serrano quevedo, italo mecías, molina chalacán, luis javier and zúñiga paredes, andrea, 2020. Seguridad informática en las pymes de la ciudad de quevedo. Journal of business and entrepreneurial studies: jbes. 2020. Vol. 4, no. 2.

Sociedad, universidad y, rené zuña macancela, edgar, alberto arce ramírez, ángel, javier romero berrones, wilson, jorge soledispa baque, césar, macancela, zuña, ramírez, arce, berrones, romero and baque, soledispa, 2019. 59 analysis of the security of the information in the smes of the universidad agraria del ecuador. Guayaquil. Ecuador. Cita sugerida (apa, sexta edición). Online. 2019. Vol. 4. Retrieved from: https://orcid.org/0000-0002-9316-1262

Soto abanto, eloy, 2018. Muestreo y tamaño de muestra para una tesis. Tesis ciencia. 2018.

Tejena-macías, mayra a., 2018. Análisis de riesgos en seguridad de la información. Polo del conocimiento. 2018. Vol. 3, no. 4. Doi 10.23857/pc.v3i4.809.

Ticse capcha, richard oswaldo, maquera quispe, henry george and meza quintana, carlos, 2019. Evaluación del desarrollo de políticas de seguridad de información. Ciencia & desarrollo. 2019. No. 18. Doi 10.33326/26176033.2014.18.469.

Torres-rodríguez, agustín a. And monroy-muñoz, jesús i., 2020. El problema de la definición del problema de investigación. Boletín científico de la escuela superior atotonilco de tula. 2020. Vol. 7, no. 13. Doi 10.29057/esat.v7i13.5265.

Valdevit, thierry, mayer, nicolas and barafort, béatrix, 2019. ¿qué son las pymes? Communications in computer and information science. 2019. Vol. 42.

Vera-rivera, fredy humberto; perez-gutierrea, boris; and urbina, victor;, 2016. Modelo de nube híbrida (hybrid cloud) de infraestructura como servicio para mejorar el rendimiento de la plataforma sandbox - ufps. In: conferências iadis ibero-americanas computação aplicada 2016. 2016.

Vmware, 2016. ¿en qué consisten la tecnología de virtualización y las máquinas virtuales? Vmware.com. 2016.

UNIVERSIDAD CÉSAR VALLEJO

ANEXOS

Anexo 01: Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES	METODOS Y TECNICAS DE INVESTIGACION
PROBLEMA GENERAL ¿Cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source para PyMES? **PROBLEMAS ESPECÍFICOS** ¿Cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source en la **confidencialidad** de la seguridad de información para PyMES? ¿Cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source en la **integridad** de la seguridad de información para PyMES? ¿Cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source en la **disponibilidad** de la seguridad de información para PyMES?	**OBJETIVO GENERAL** Determinar cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source para pymes. **OBJETIVOS ESPECÍFICOS** **O1:** Determinar cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source en la confidencialidad de la seguridad de información para pymes **O2:** Determinar cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source en la integridad de la seguridad de información para pymes **O3:** Determinar cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source en la disponibilidad de la seguridad de información para pymes	**HIPÓTESIS GENERAL** El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source influye en la seguridad de información para PyMES **HIPÓTESIS ESPECÍFICOS** **H1:** El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source influye en la **confidencialidad** de la seguridad de información en las PyMES **H2**: El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source influye en la **integridad** de la seguridad de información en las PyMES **H3**: El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source influye en la **disponibilidad** de la seguridad de información en las PyMES	**VARIABLE INDEPENDIENTE:** El método basado en tecnología de servidores espejo en la nube . **VARIABLE DEPENDIENTE**: Seguridad de información **Indicadores:** **D1.** Confidencialidad - Gestión Incidentes de acceso indebido a los documentos. - Control de documentos. - Gestión de Contraseñas. - Gestión de Seguridad de datos. - Gestión de Fugas de información. -soportes de los datos de información. **D2.** Integridad - Incidentes en la integridad de los documentos. -Frecuencia de incidentes en la integridad de los datos de información. -Integridad de documentos y control. **D3.** Disponibilidad -Seguridad Física y del entorno -Incidentes en la disponibilidad de la información - Disponibilidad de servicios de información.	Métodos: Diseño: Aplicativo, Pre Experimental GE: 01 x 02 Donde: G.E. Estudiantes de la empresa New Fashion 01: Implementación de un servidor espejo usando herramientas open source en la nube (pre test). X: Implementación del servidor espejo 02: Implementación de un servidor espejo usando herramientas open source en la nube (Post test) Técnicas e Instrumentos de recolección de datos ▪ Observación ▪ Lista de cotejo

Fuente: Elaboración propia

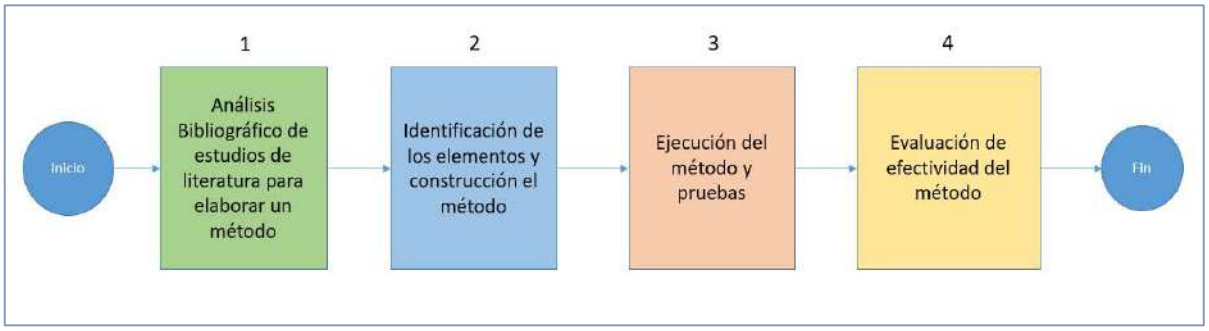
Anexo 02: Método de Seguridad de Información

Etapas para la construcción del Método de Seguridad de Información

Para la construcción del método de Seguridad de Información se basó, en el artículo titulado: Seguridad informática y seguridad de la información, del autor Calderón Arateco Laura Lorena de la Universidad Piloto de Colombia, el cual plantea soluciones de seguridad, basado en el modelo PDCA y los tres pilares de la Seguridad de la Información, en base a ello el método de la presente tesis tiene 4 etapas: análisis bibliográfico de estudios, identificación de los elementos que va a componer el método, realizar las pruebas, y evaluación de la solución. (Calderón Arateco Laura Lorena, et al., 2020)

En la siguiente figura se observa las etapas para la construcción del Método de Seguridad de Información. Ver Figura 01.

Figura 01: Etapas para la construcción del Método de Seguridad de Información, basados en el ciclo PDCA.



Fuente: Elaboración propia

Análisis Bibliográfico

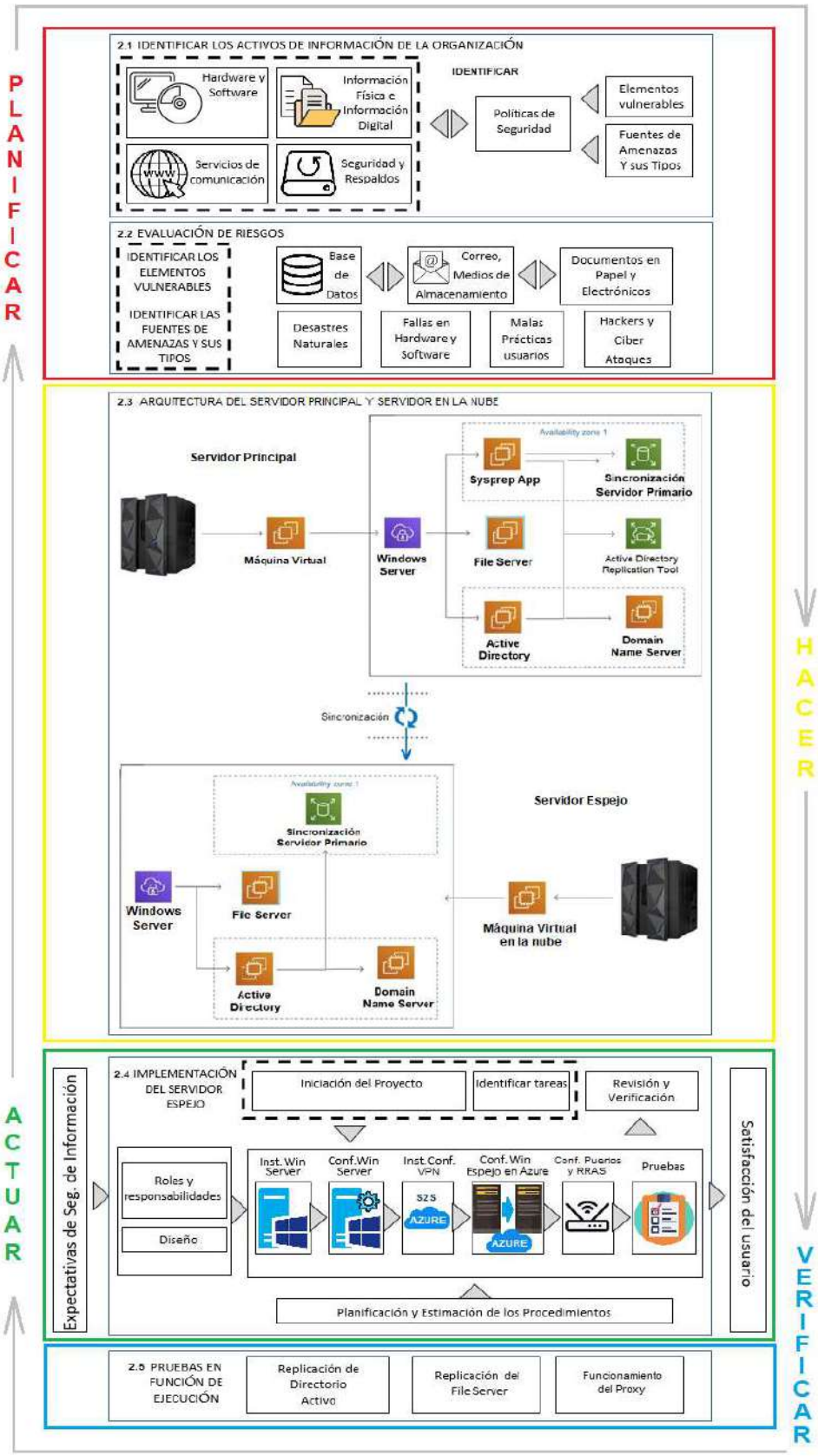
En esta etapa recopilamos parte de los artículos, libros, tesis que ayudaron a definir el método aplicado en esta Tesis para salvaguardar la Seguridad de la Información.

Nombre de articulos, libros, tesis	Autor	Año	Resumen
Diagnóstico de la aplicación del ciclo PHVA según la ISO 9001:2015 en la empresa INCARPALM	Juan Alberto Salazar-Garces Universidad Técnica de Machala - Ecuador	2020	La investigación de este artículo se enfocó en el objetivo de diagnosticar la implementación del ciclo PHVA de la Norma ISO 9001:2015 como guia de trabajo y mejora continua en la organización.
Metodología de la seguridad de la información como medida de protección en pequeñas empresas	Giovanny Bustamante Maldonado Jorge Andrés Osorio Cano	2016	La necesidad de proteger la información tiene cada vez mayor importancia para las empresas. En este contexto surgen los sistemas de gestión de la seguridad de la información (SGSI), La metodología recurrida se fundamenta en investigaciones relacionadas con la norma ISO 27001:2005 y su ciclo PHVA
Aplicación de la metodología phva para aumentar la productividad en el área de producción de la empresa envases gráficos s.a.c	Súa Yessenia Vargas Chunga. Natalia Lorena Viteri Guevara	2018	La metodología aplicada fue la metodología PHVA. Esta herramienta de mejora continua permite una mejora integral de la competitividad de los productos y servicios, en base a la mejora de la seguridad de su información, mejorando la calidad, reduciendo los costos, optimizando la productividad y aumentando la rentabilidad de la empresa u organización.

Método de Seguridad de información

El método que se va a utilizar está basado en el modelo PDCA y está clasificado en 4 fases: Planificar, Hacer, Actuar y Verificar. Ver figura 02.

Figura 02: Método de Seguridad de información basado en el ciclo PDCA



Fuente: Elaboración propia

PLANIFICAR

Identificar los activos de información de la Organización

Inventario de activos: se deben identificar todos los activos de la organización y tenerlo actualizado constantemente y de manera organizada. (Maquera Quispe, Serpa Guillermo, et al., 2019)

Hardware y software:

Pasos para el inventario del Hardware y Software:

- Inventariar el hardware y software con el programa de Microsoft Network Inventory Advisor
- El inventario debe contener lo siguiente:
- Año de adquisición de cada equipo de cómputo y software
- Tiempo de vigencia del software
- Fecha de mantenimientos preventivos y correctivos
- Verificar que todo el software este licenciado
- Identificar el uso de cada activo y su uso en la empresa
- Identificar al usuario del equipo
- Cada equipo debe de contener un sticker y un código de inventario.

Servicios de comunicación:

Pasos para el funcionamiento óptimo de los servicios de Comunicación:

- Verificar la fecha de renovación del Correo Electrónico
- Inventariar los routers y los switchs
- Contar con un VPN licenciado
- Contar con un cableado de red certificado
- Evaluar la velocidad del ancho de banda del Internet
- Verificar la caducidad del dominio y hosting de las páginas web
- Monitorear el firewall para el acceso a las páginas que usa cada empleado de la empresa.
- Bloqueo de puertos de comunicación que no se utilizan y solo habilitar los necesarios.

Información Física e Información Digital:

Aquí identificamos la información física que tiene la empresa como:

- Cotizaciones físicas
- Facturas impresas
- Guías de Remisión
- Inventario de equipos
- Manuales de instalación
- Contratos del personal
- Órdenes de compra
- Informes
- Reportes

Seguridad de Respaldo:

Aquí identificamos los activos y documentos que se necesita respaldar para proteger los datos de la empresa:

- Carpetas Compartidas
- Servidor de Dominio
- Base de datos
- Base de correos corporativos

Fuente de amenazas y sus tipos:

Aquí identificamos las amenazas que puede ocurrir en la empresa:

- Ciber ataque
- Infección en la base de datos
- Daños a equipos físicos
- Corto circuito
- Perdida de información en la red
- Clonación de cuentas de usuario
- Hackeo de claves de la empresa

Evaluación de riesgos

Es importante evaluar qué es lo que podría poner en peligro los activos de información. (Tejena-Macías, et al., 2018)

Identificar puntos vulnerables

- La Base de Datos
- El correo
- Los medios de almacenamiento
- Los documentos físicos y electrónicos.

Identificar las amenazas potenciales

- Desastres naturales
- Fallas de hardware y software
- Las malas prácticas de los usuarios
- Los hackers y ciber ataques.
- Examinar si el software puede ser hackeado
- Examinar si los puertos UDP están abiertos
- Determinar el impacto de las amenazas
- Revisar si los respaldos están funcionando correctamente

HACER

Despues de identificar los activos de informaciòn que tiene la empresa , el siguiente paso del metodo es hacer la arquitectura de un servidor espejo en la nube que nos ayuda a proteger la confidencialidad, integridad, disponibilidad de la informaciòn de los distintos servidores que tiene la organizaciòn, esto nos ayudara a tener en cuanta los pasos que tenemos que seguir para tener una buena implementaciòn del metodo de seguridad.

Paso 1:

Para poder empezar a sincronizar los servidores , primero debemos tener claro los punto:

- Capacidad de Memoria Ram del servidor Fisico: La memoria Ram debe cumplir con los mismos requisitos que tiene el servidor principal(fisico) en la nube
- Capacidad de espacio del Disco Duro : El disco duro debe contar con la misma capidad en la nube o tener mas espacio por si a un corto plazo la empresa empieza a crecer.
- Verificar que licencia de Windows Server tiene cada servidor y debe ser la misma licencia en la nube para que los datos se sincronizen de manera exitosa.
- Verificar los nucleos que se necesita para instalarlo en la nube

Paso 2:

Crear las maquinas virtuales en la nube con las mismas caracteristicas de los servidores fisicos.

- Debemos configurar la memoria Ram en la maquina virtual del azure
- Debemos configurar el espacio del disco que se va usar por cada maquina virtual en azure
- Debemos configurar los nucleos que se va utilizar por cada maquina virtual en azure.
- Debemos instalar la misma licencia de windows server que tienen los servidores fisicos en la empresa.

Paso 3:

Sincronizar el servidor fisico del active directory de la empresa a la nube mediante la herramienta open source “syspret”

La empresa New Fashion cuenta con 7 area las cuales estan divididos en:

- Gerencia : Que cuenta con 2 usuarios , los cuales son Gerencia General y Gerencia administrativa.

- Sistemas: Cuenta con 4 usuarios ,los cuales son el Jefe de sistema, Analista de sistemas, Asistente de sistemas y Practicante de Sistemas.

- Recursos Humanos: Cuenta con 4 Usuarios, los cuales son Jefe de Recursos Humanos, Analista de selecciòn , Asistenta Social y practicante.

- Asesoria Legal: Cuenta con 1 solo usuario el cual es el abogado de la empresa.

- Producciòn : Cuenta con 4 usuarios, los cuales son el Jefe de producciòn, Supervidor de Calidad, Analista de planificaciòn ,Asistente de producciòn.

- Finanzas: Cuenta con 4 usuarios, los cuales son ,el Jefe de finanzas, 1 analista contable, 1 asistente de finanzas, 1 analista de tesoreria.

- Comercial: En el area comercial se cuenta con 10 vendedores , de los cuales solo los jefes por areas tienen cuenta de usuario, los cuales son , el jefe de ventas nacional, el jefe de ventas norte, el jefe de ventas centro, el jefe de ventas sur.

- Logistica: El area de logistica cuenta con 4 usuarios, los cuales son el jefe de logistica, el analista de compras y 2 asistentes de logistica.

PASO 4:

Sincronizar las carpetas del flle Server del servidor fisico al servidor de la nube mediante una herramienta Open source llamada “ syspret”

Las carpetas que se cuenta en la empresa estan divididas por areas las cuales son :

- Gerencia: En estas carpetas se encuentran todo lo relacionado a las ventas generales , cotizaciones, ordenes de compra, y KPI'S que el area de gerencia necesita visulaizar para tener un reporte de como esta fluyendo el trabajo en la empresa.

- Sistemas: En esta carpeta se encuentra todo relacionado a inventarios de equipos de la empresa,carpetas sobre los sotfware que se utilizan en la empresa, cotizaciones sobre los productos adquiridos, manuales de instalaciòn y capacitaciòn para los empleados de la empresa.

- Recursos Humanos: En esta carpeta se encuentra todo lo relacionado a compras de utilizes de oficina , cotizaciones de productos, documentos de seguros, docuemntos de planillas, etc.

- Asesoria Legal: En esta carpeta se encuentran todos los documentos referidos a temas legales de la empresa.

- Producciòn: En esta carpeta se encunetran todos los documentos relacionado a planta, almacen y equipos que tienen en la empresa.

- Finanzas: En esta carpeta se encuentra documentos relacionados al area contable, facturas, guias de remisiòn, docuemntos emitidos a sunat , etc.

- Comercial: En esta carpeta se encuentra documentos relacionado a requerimientos de pedidos, seguimiento de pedidos y cartera de clientes.

- Logistica: En esta carpeta se encuentra documentos relacionados a ordenes de compra, cotizaciones, proveedores, seguimiento de pedidos, etc.

Paso 5:

Sincronizar el DNS de la empresa

- El DNS es una configuraciòn que se ejecuta en el servidor para poder habilitar la salida de internet a los usuarios que tengas autorizaciòn en la empresa

Paso 6:

Sincronizar los rangos de IP:

- Aquí se encuentran todas las IP fijas de la empresa , que fueron modificadas en el servidor como estaticas.

Paso 7:

Sincronizar la IP Inversa del servidor fisico al servidor en la nube

- Aquí se encuentra la IP inversas que sirve para hacer busqueda por nombre desde los servidores.

Paso 8:

Sincronizar las politicas de seguridad del servidor fisico a la nube

- Aquí se sincroniza todas la politicas creadas en el AD como en el file server por cada usuario del sistema.
- Las politicas pueden ser como se parte del miebro de algun grupo en el AD.
- Politicas de apagado de las maquinas de la empresa.
- Politicas de acceso al VPN de la empresa.
- Politicas de acceso a escritorio remoto.

ACTUAR

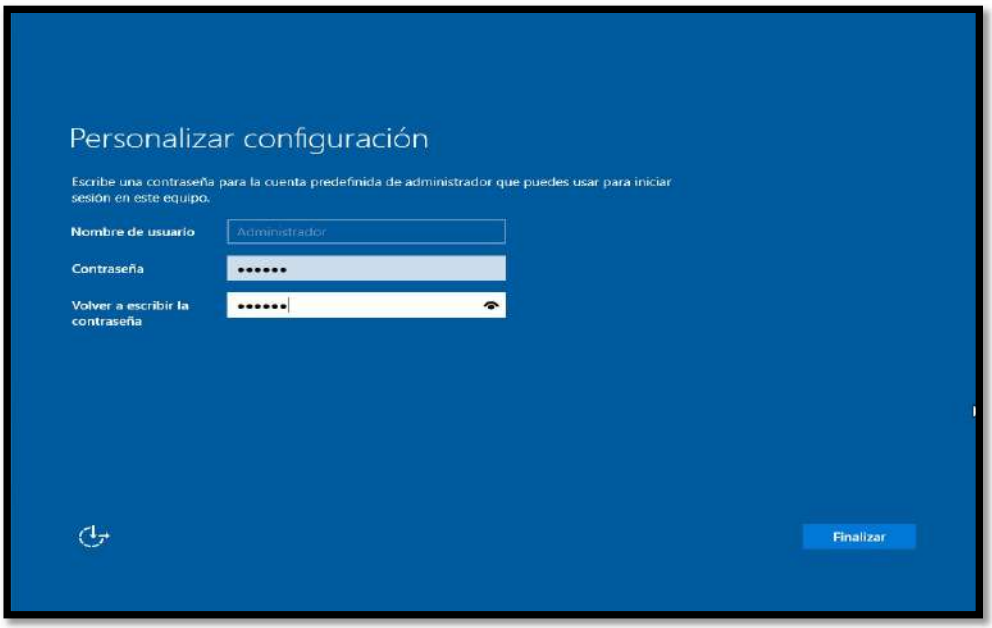
Implementación del Servidor Espejo

Instalación de Windows Server 2016 local, AD y DNS

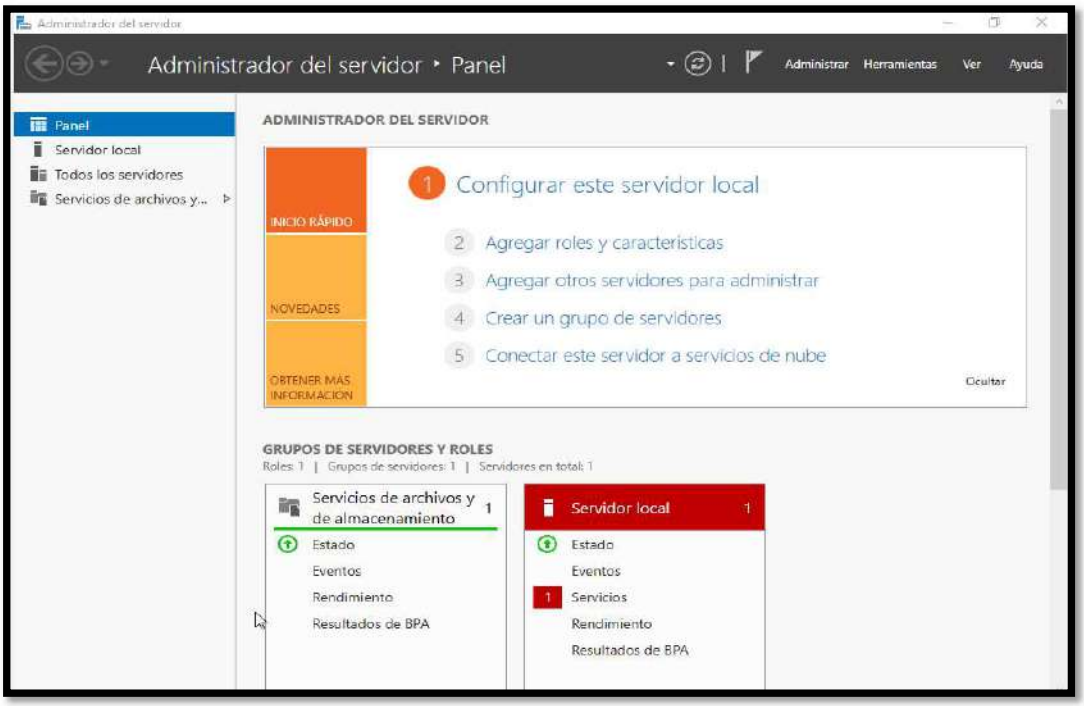
PASO 1: Instalación de Windows Server

Primero se debe obtener el ISO del Sistema Operativo Windows server 2016 y ejecutarlo, elegir el idioma y clic en siguiente.

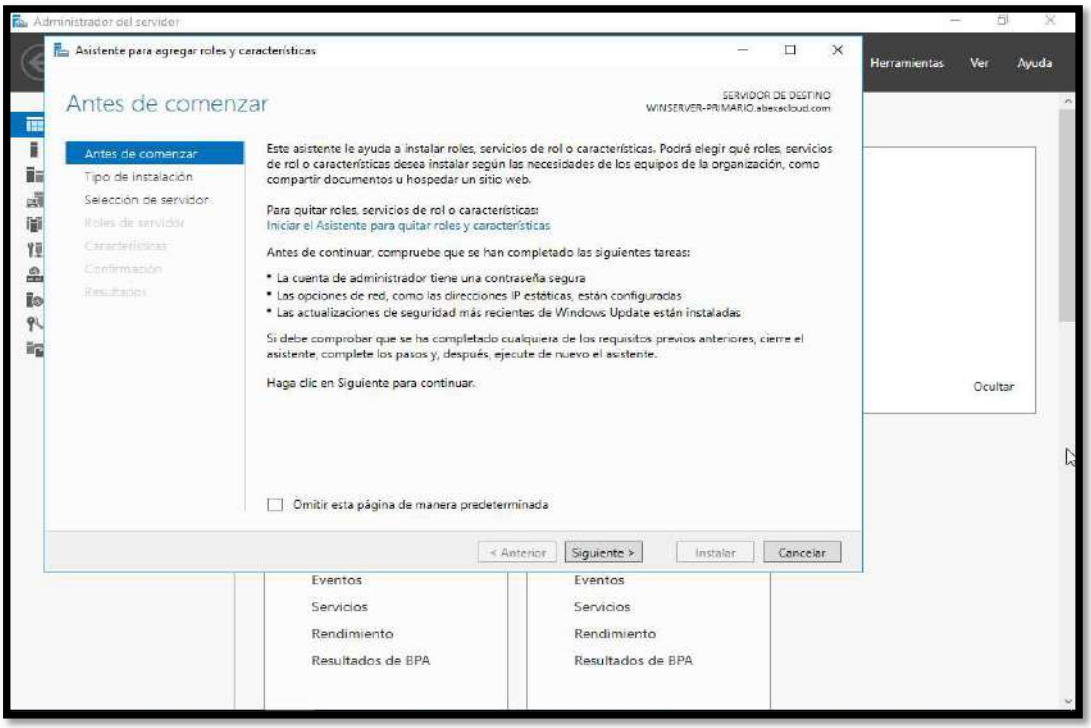
- Se inicia el proceso de instalación
- Colocar una contraseña para la cuenta Administrador



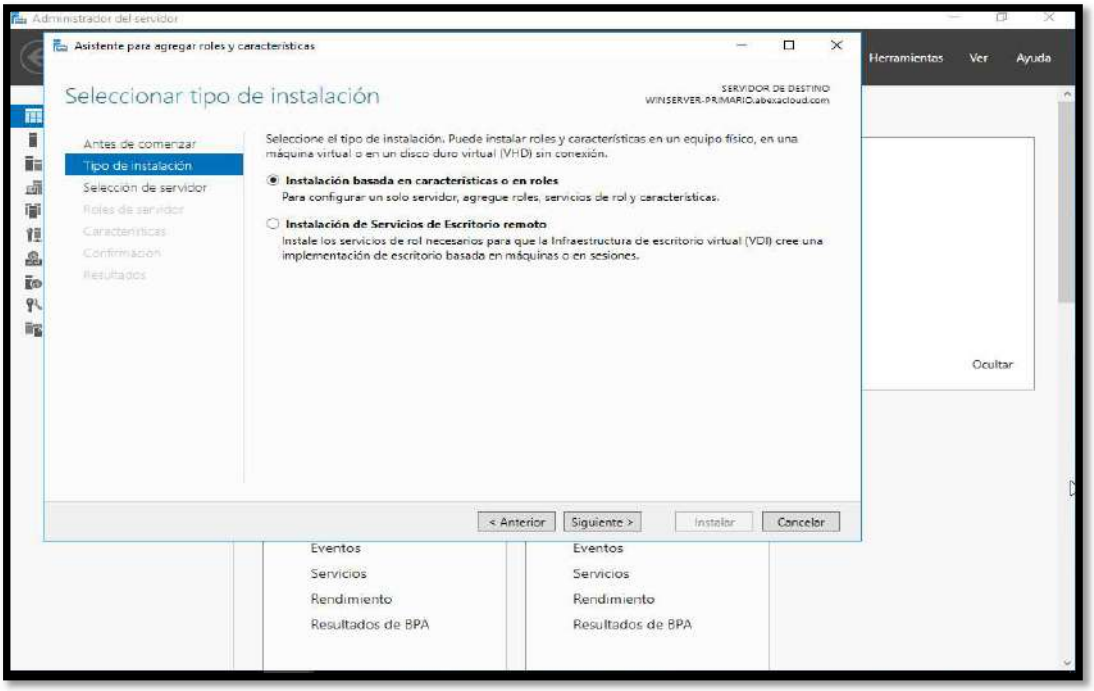
- Clic en Agregar roles y características para instalar el DNS y AD



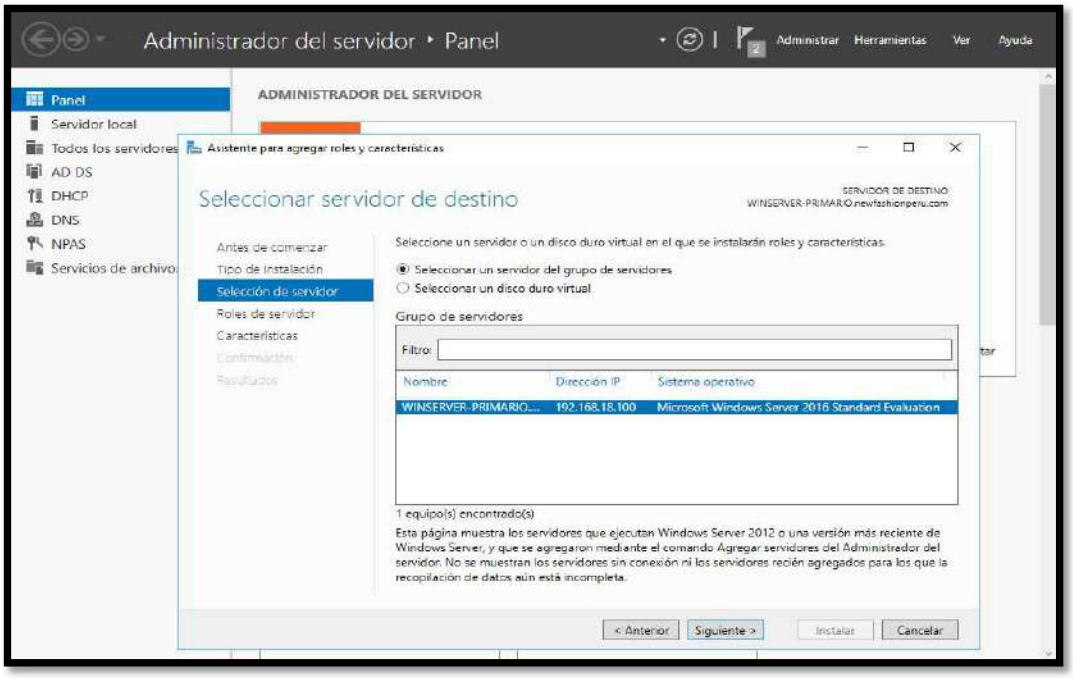
- Clic en siguiente



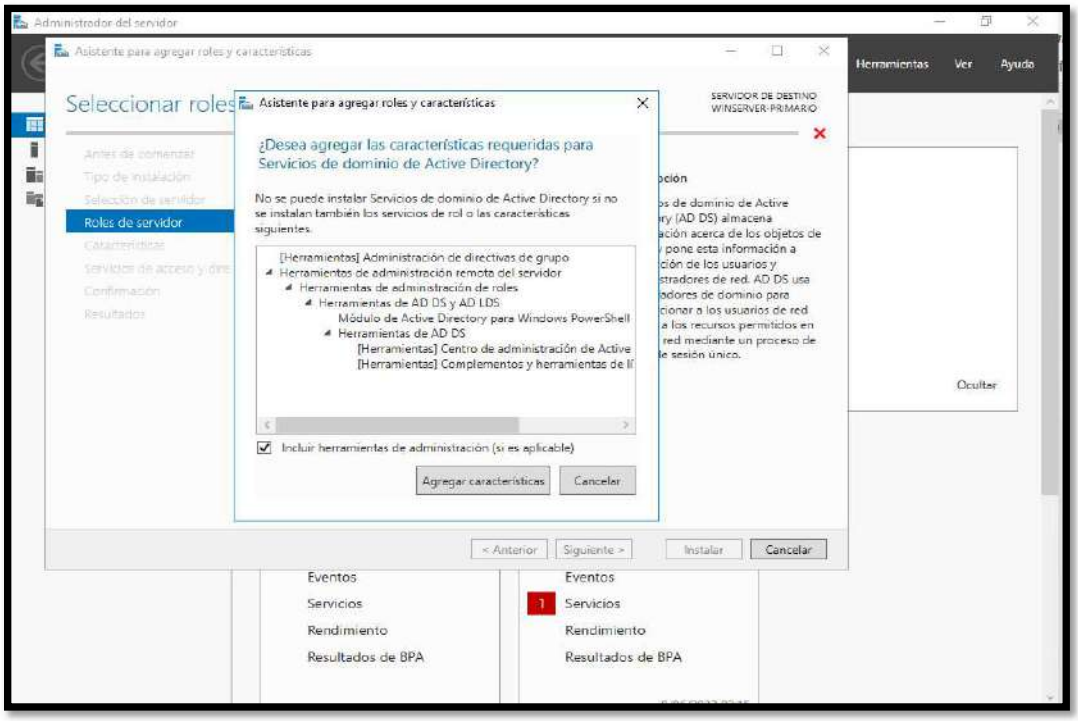
- Clic en siguiente



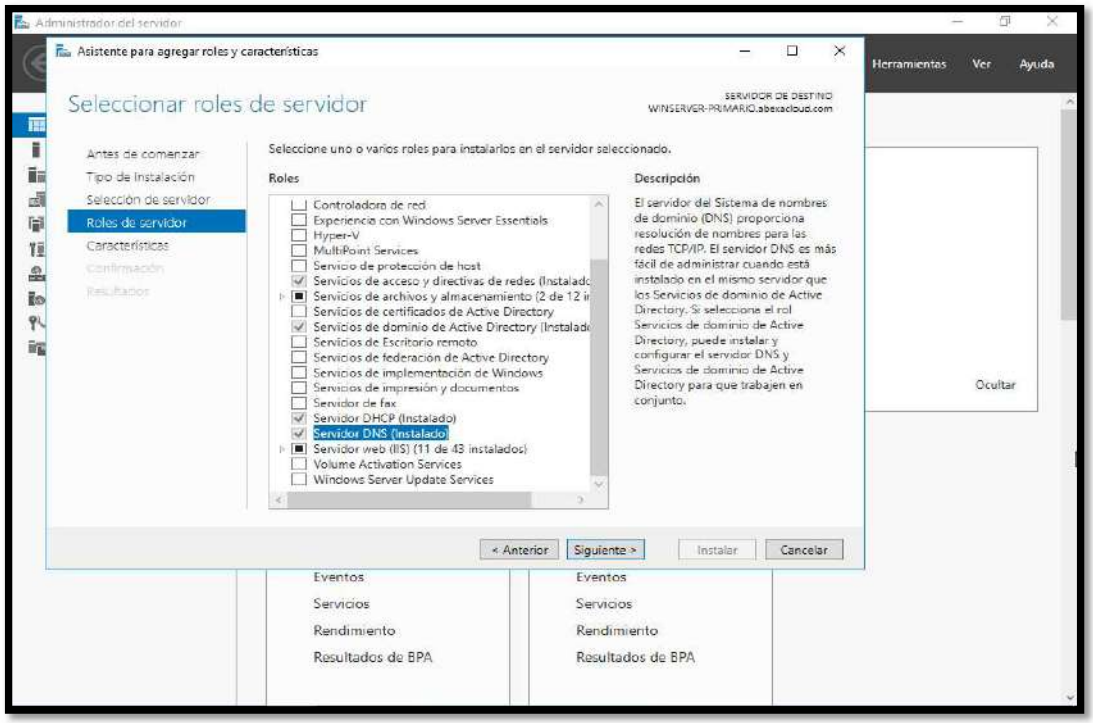
- Clic en siguiente
- La opción WinServer Primario ya está selecionado, clic en siguiente



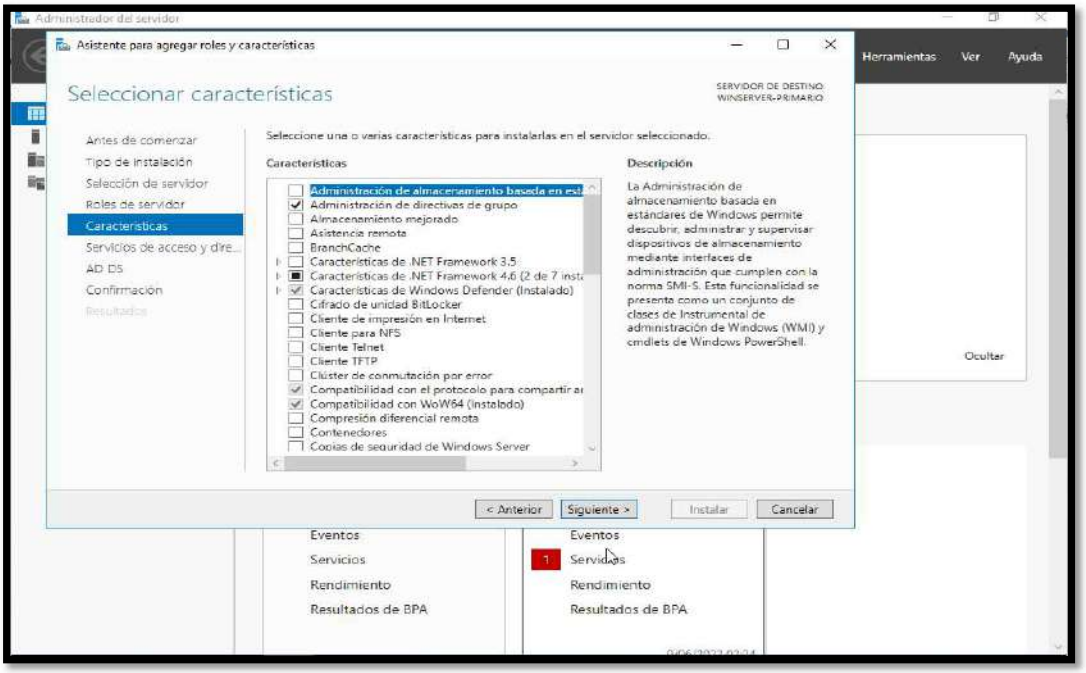
- Clic en agregar características



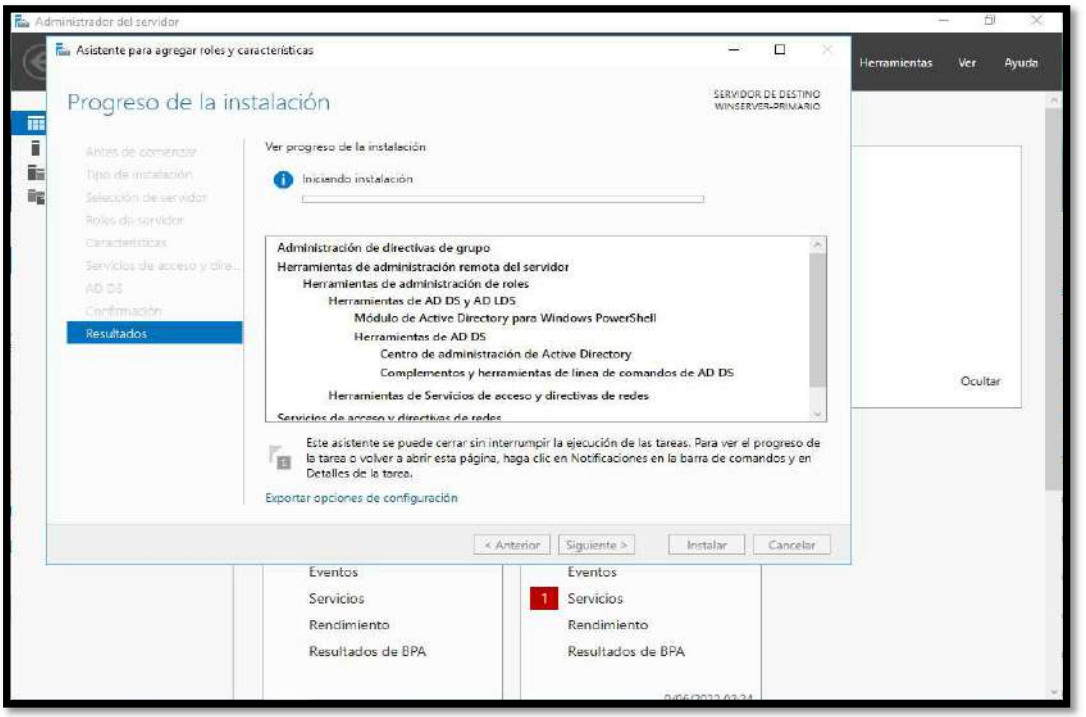
- Elegir Servidor DHCP, DNS, Servicios de dominio de AD, clic en siguiente



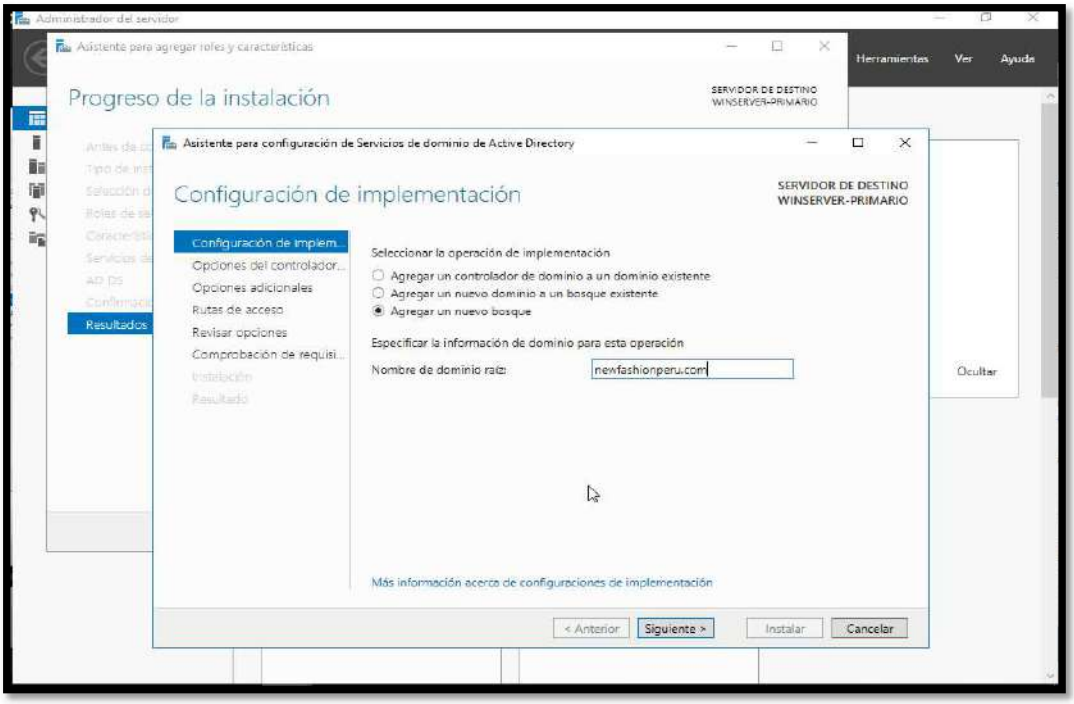
- Clic en siguiente



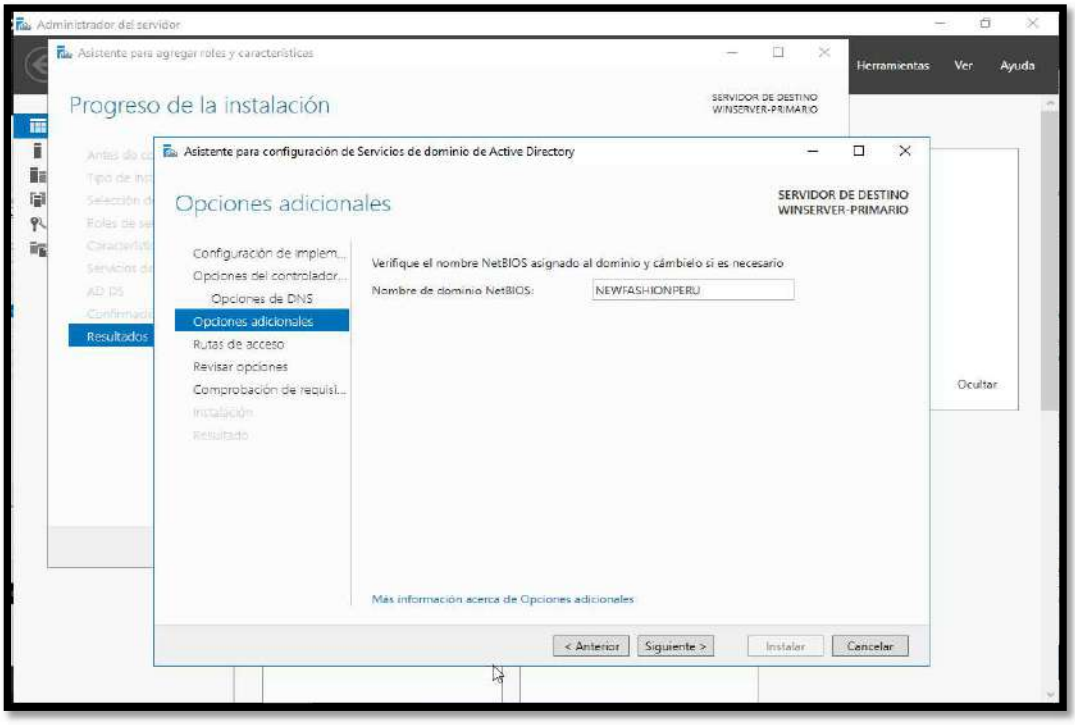
- Aquí ya inició la instalación, al finalizar clic en siguiente



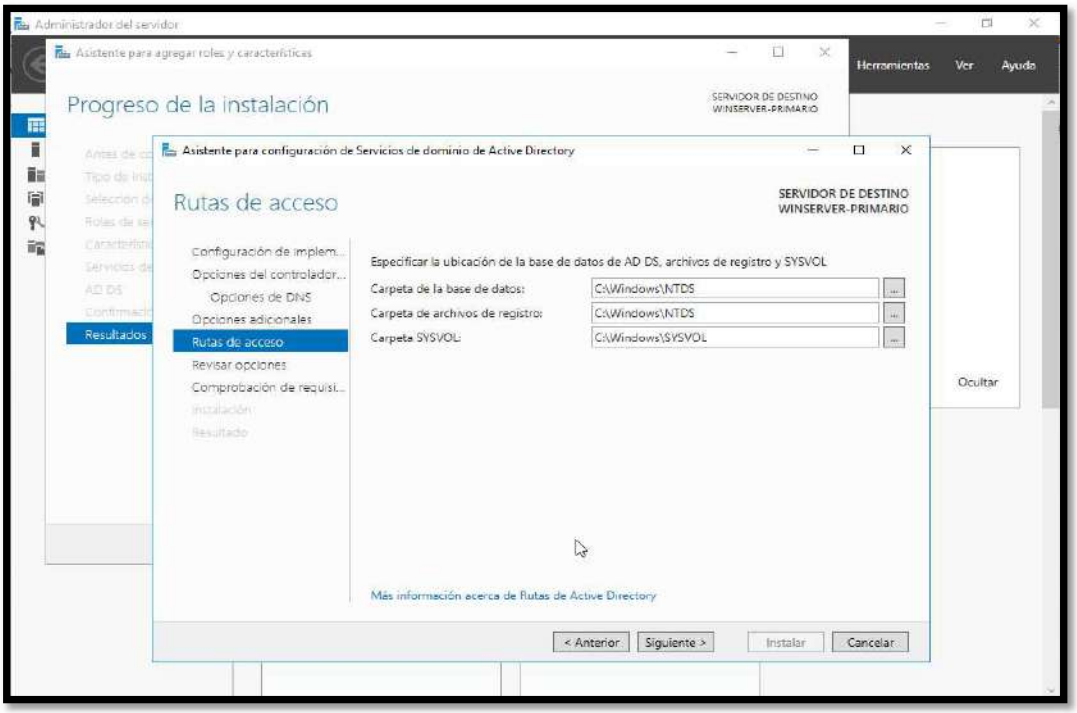
- Elegir agregar un nuevo bosque y colocar el nombre de la Pyme seguido de .com, clic en siguiente



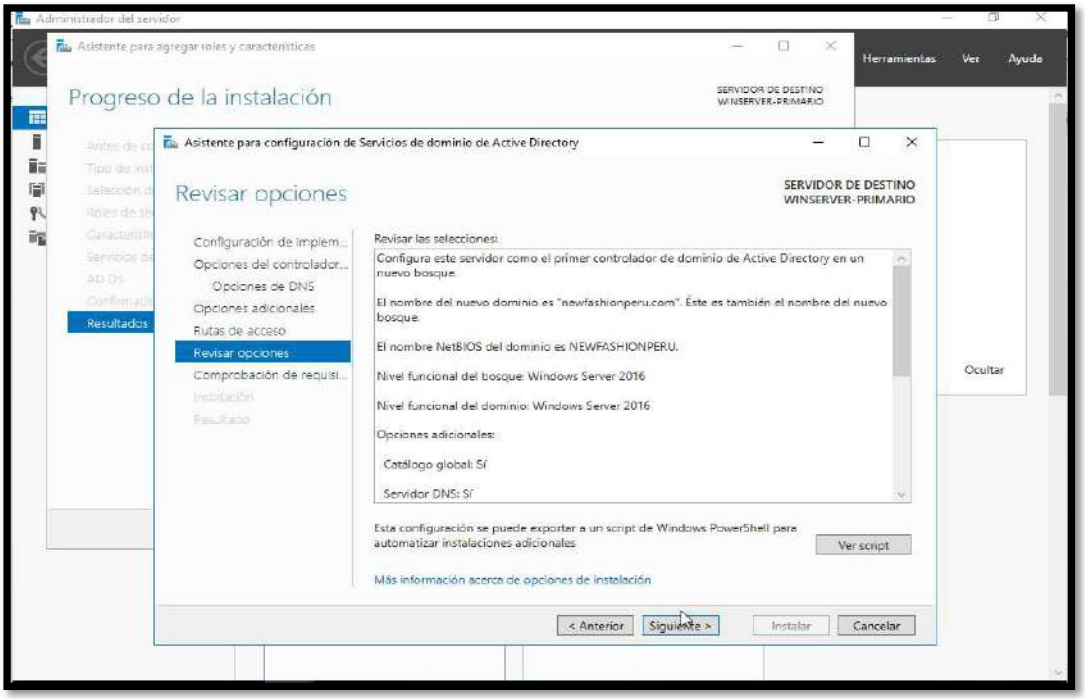
- Clic en siguiente



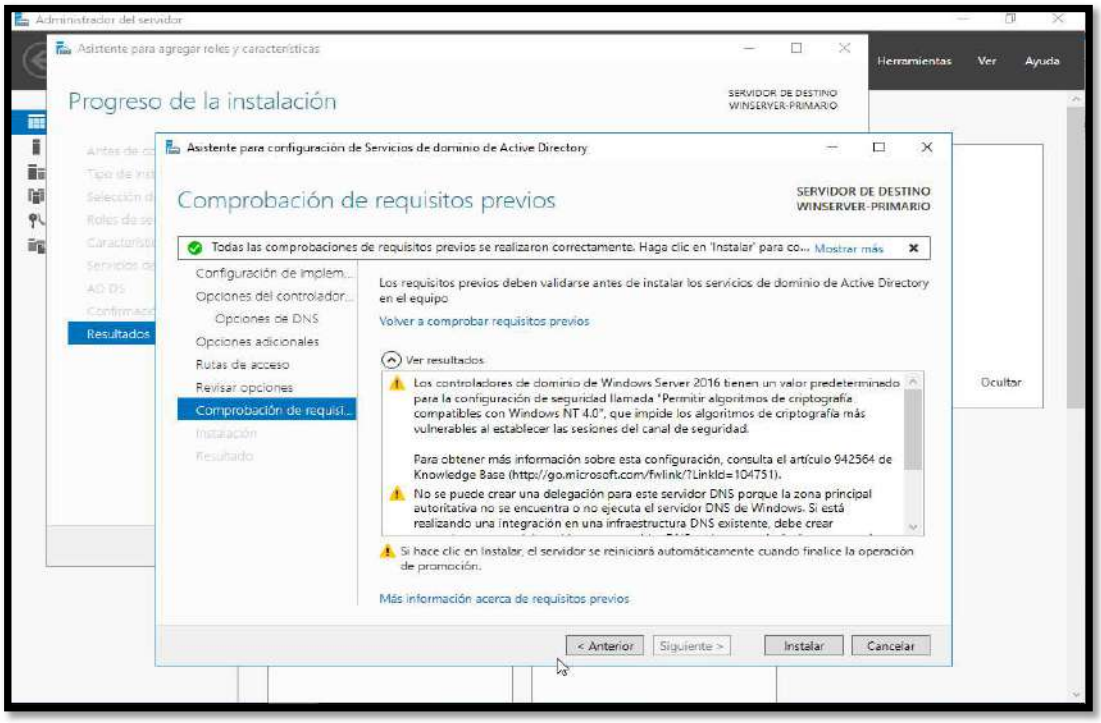
- Clic en siguiente



- Clic en siguiente

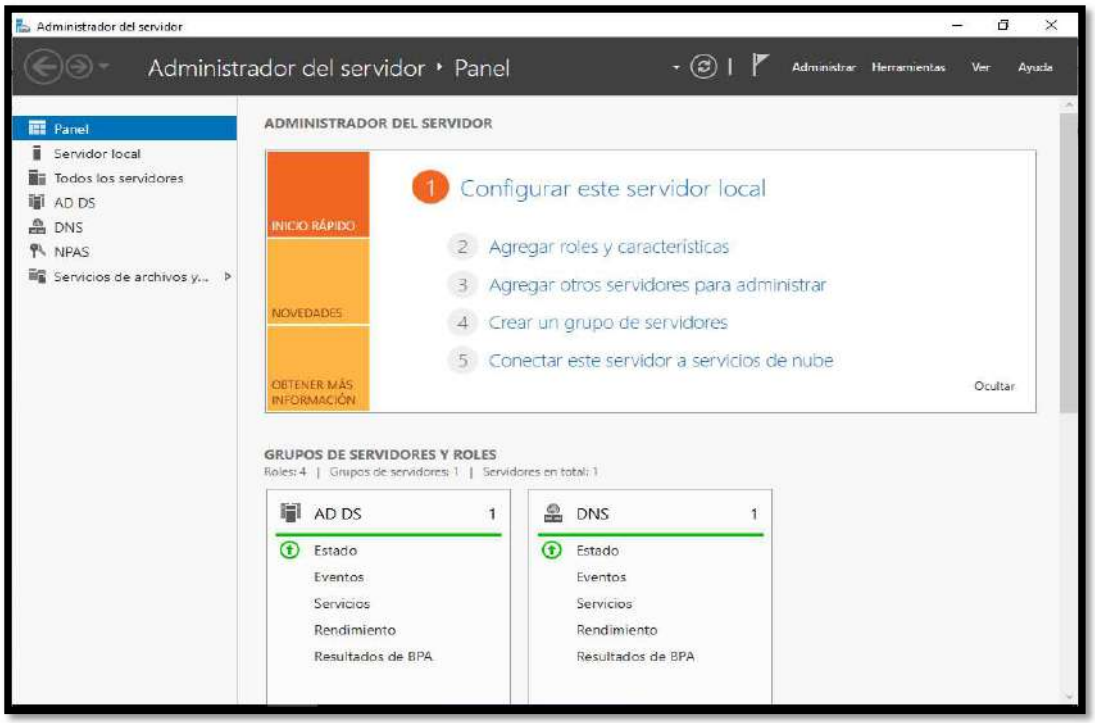


- Clic en Instalar

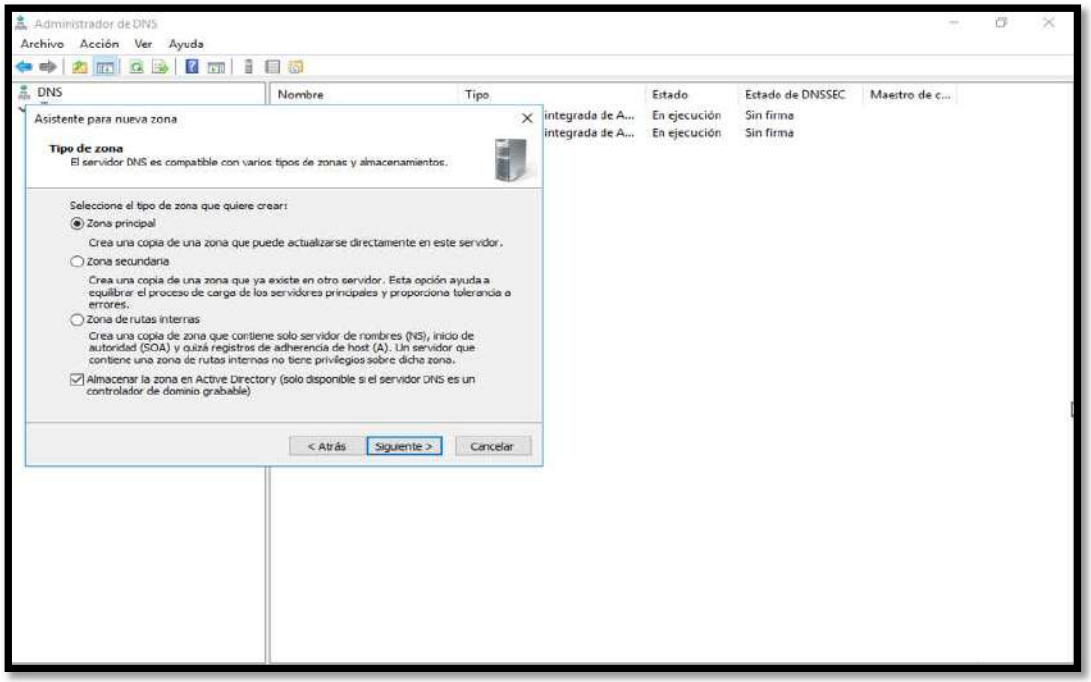


- Proceso de Instalación

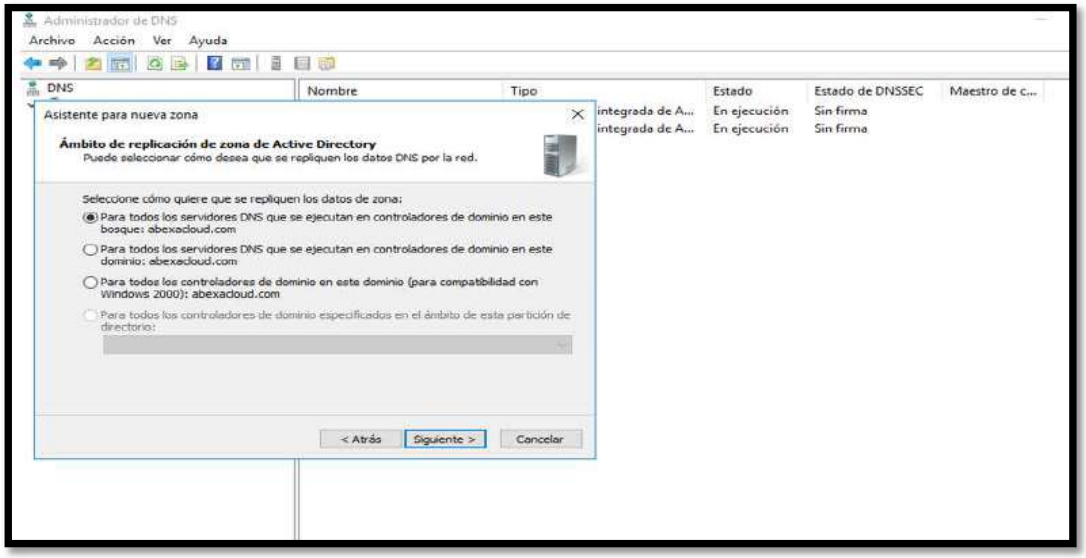
- Aquí se ve el AD DS y el DNS en verde, significa que la instalación fue correcta



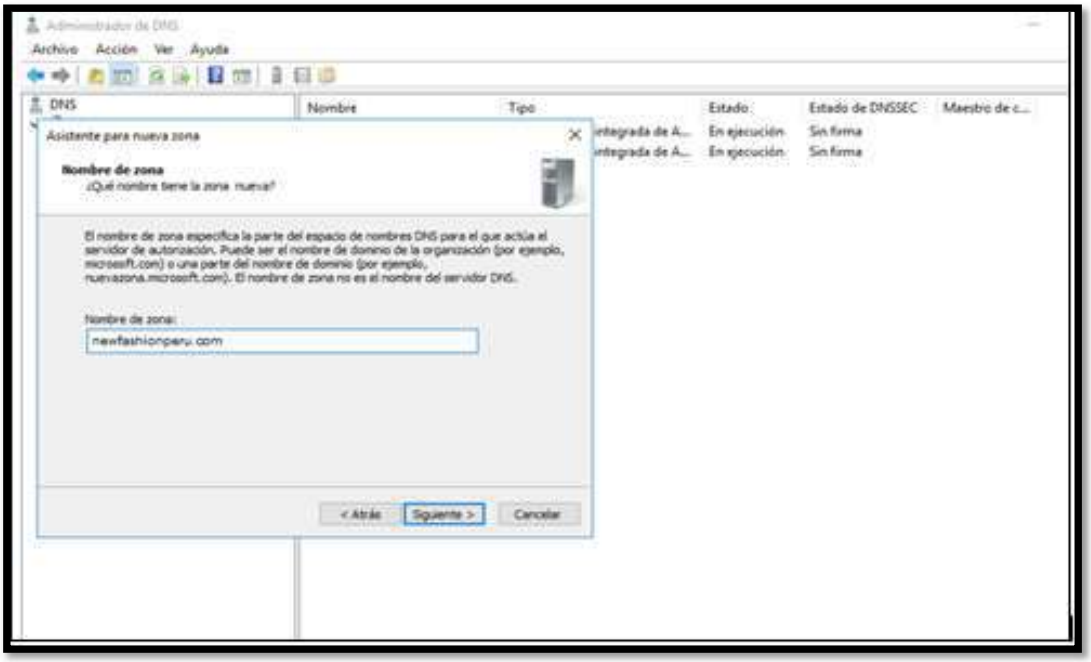
- Clic en siguiente para instalar la zona Directa del AD



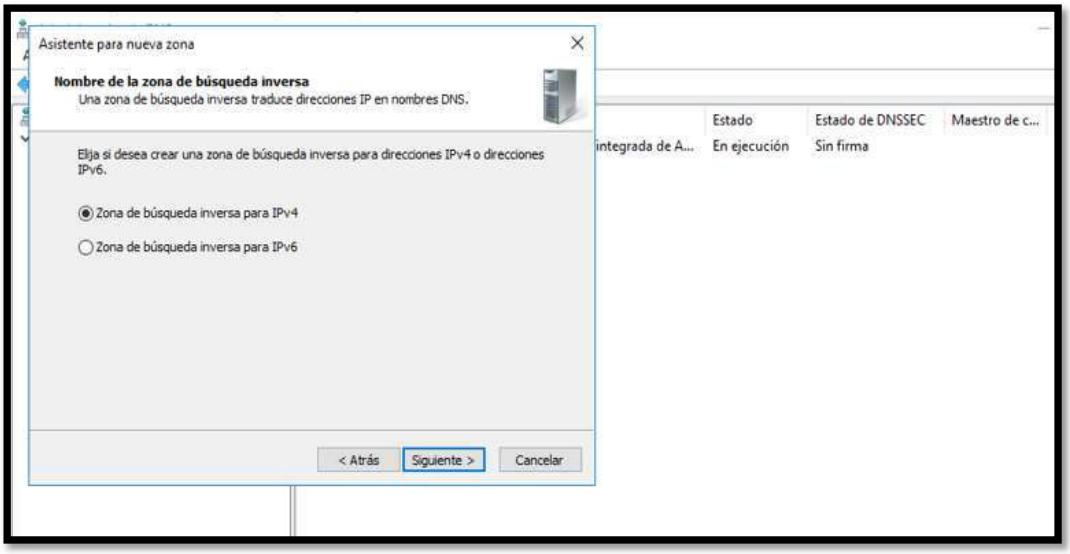
- Clic en siguiente



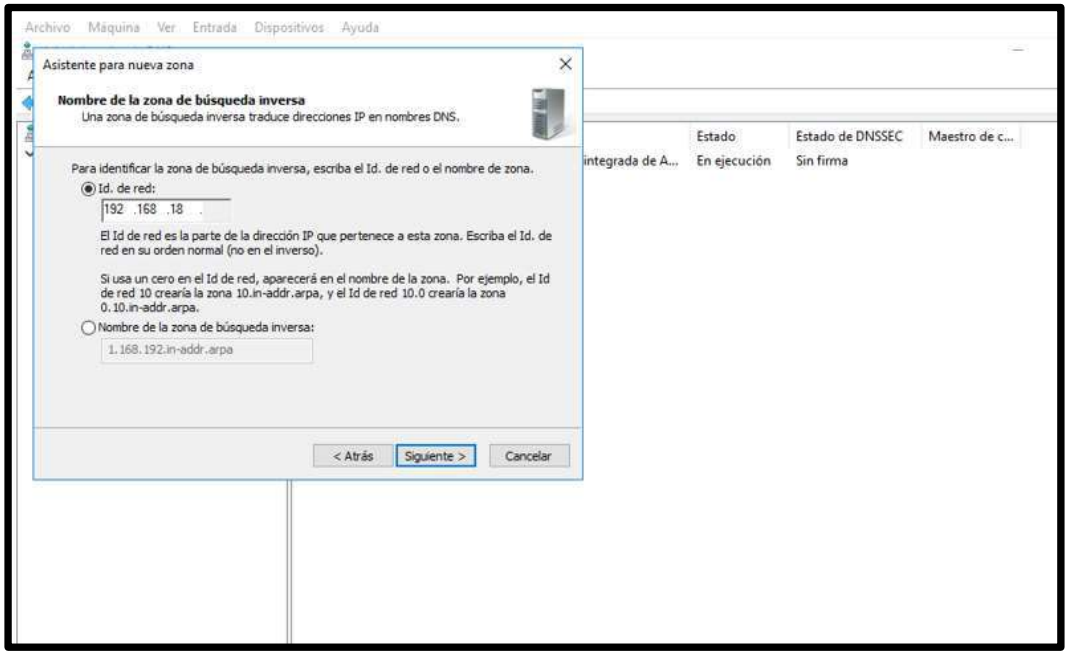
- Colocar el nombre del Dominio de la Pyme y clic en siguiente



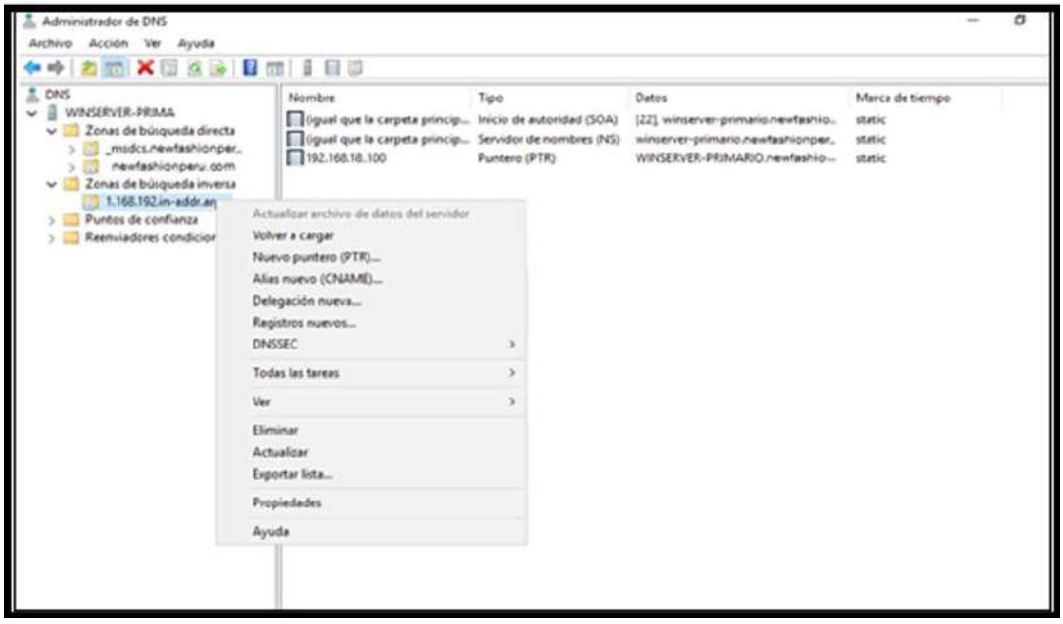
- Clic en siguiente para instalar la zona inversa



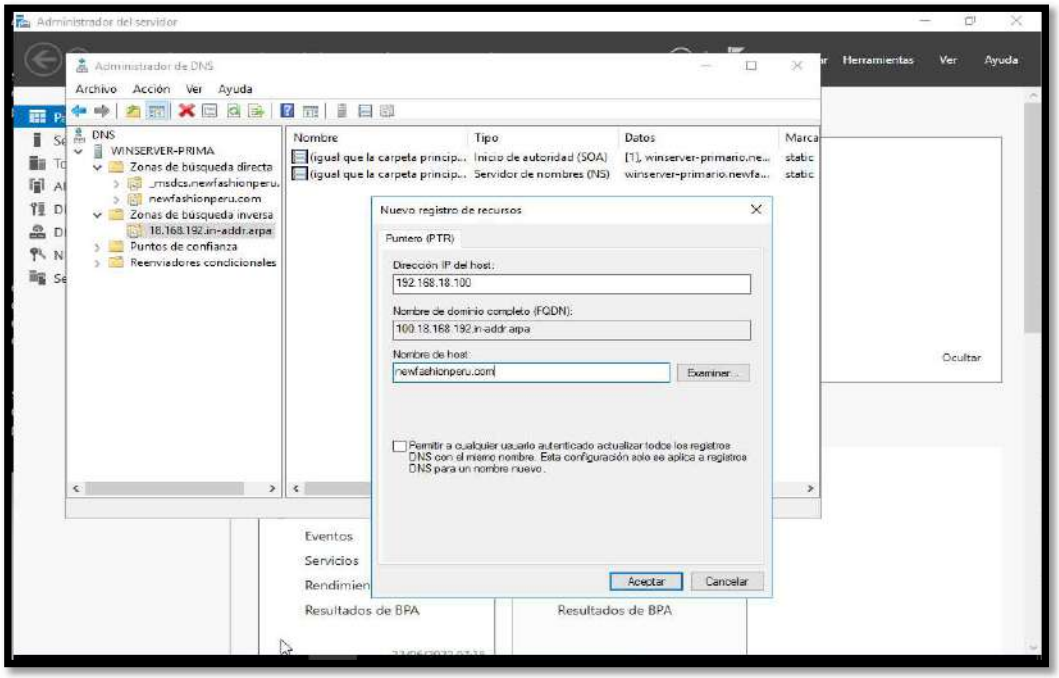
- Colocar el segmento de la red LAN y clic en siguiente



- Clic derecho en la zona de búsqueda inversa y elegir Nuevo Puntero (PTR)

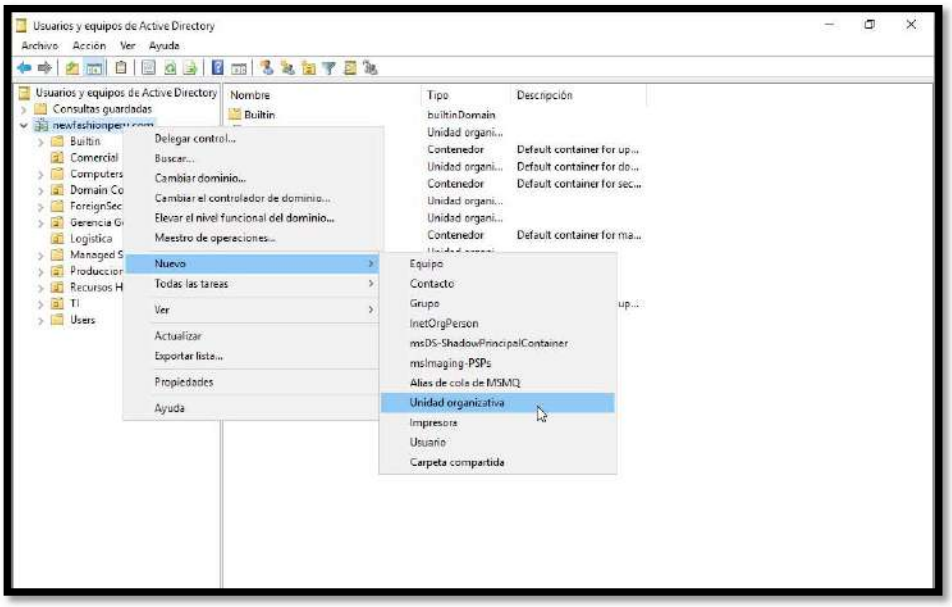


- Colocar el nombre del dominio y clic en Aceptar

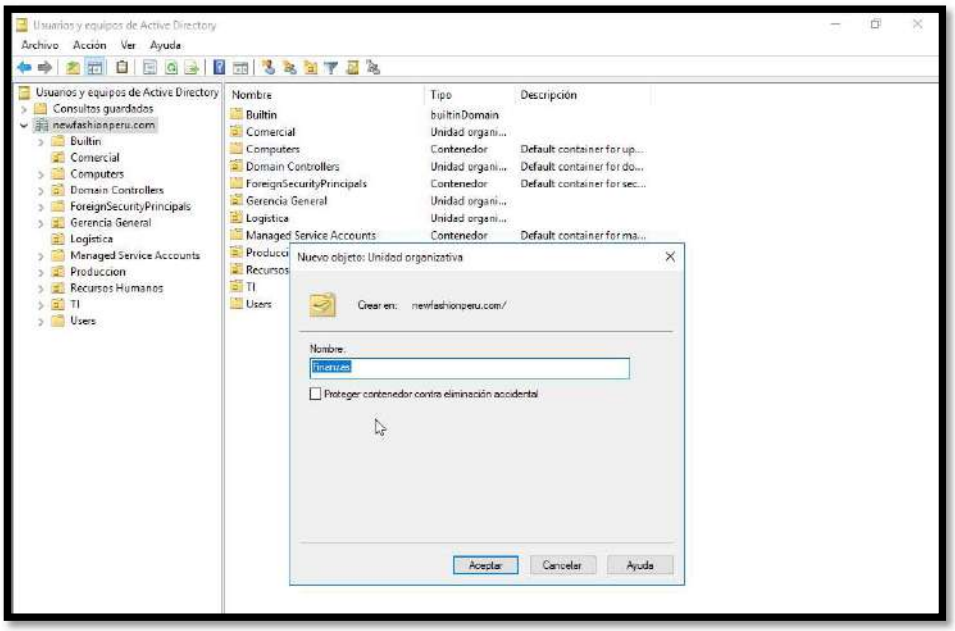


PASO 2: Configuración del Active Directory, Creación de UO y Usuarios

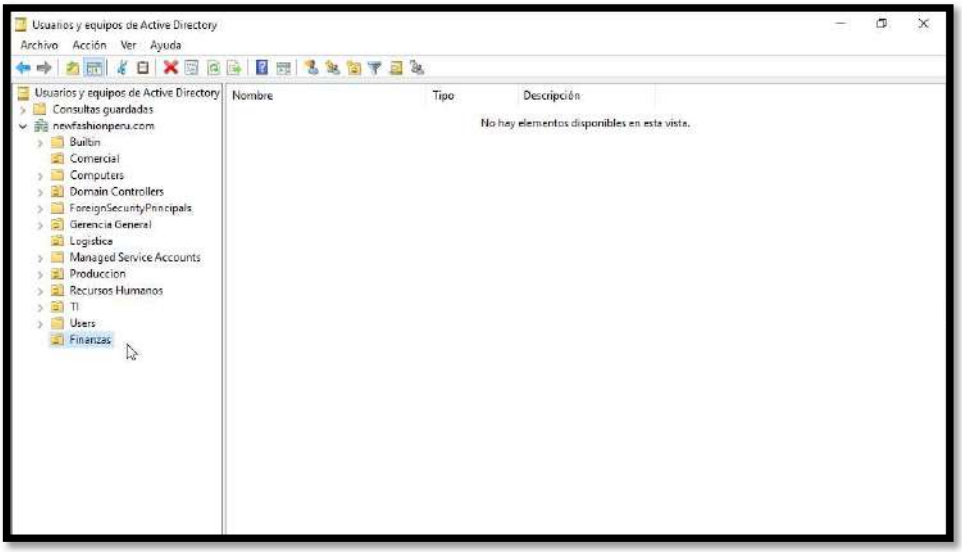
- En el AD dar clic derecho al dominio y elegir Nuevo, luego Unidad organizativa para crear las áreas de la Pyme



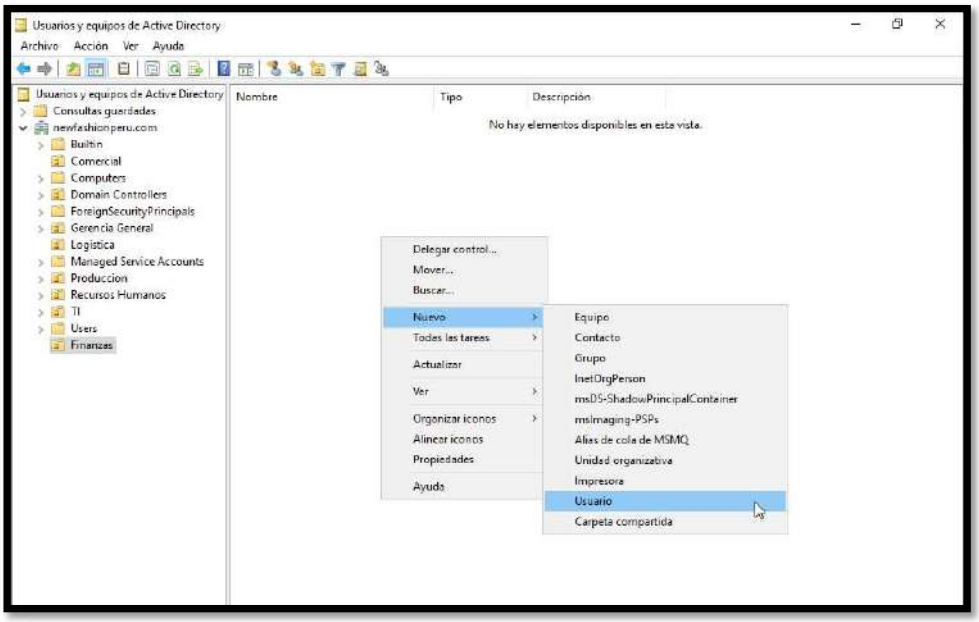
- Luego colocar el nombre del área, por ejemplo, Finanzas y clic en Aceptar.



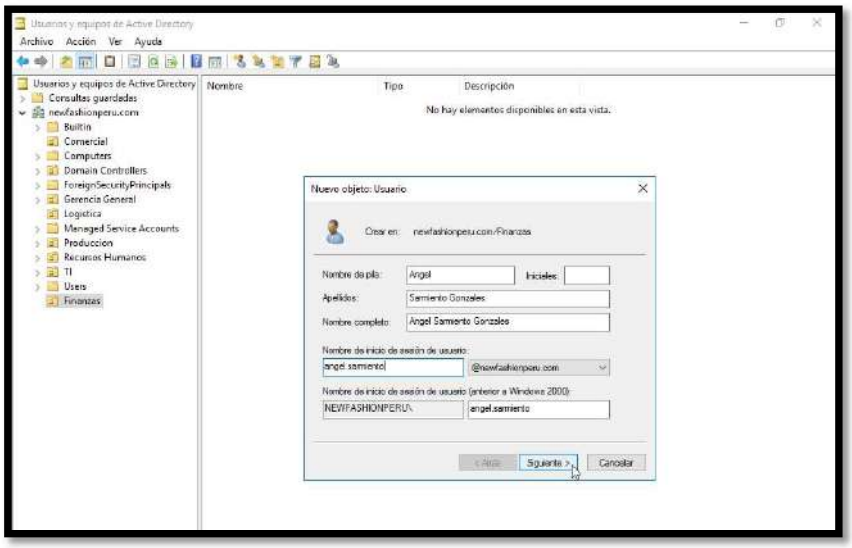
- Aquí vemos el área Finanzas creada.



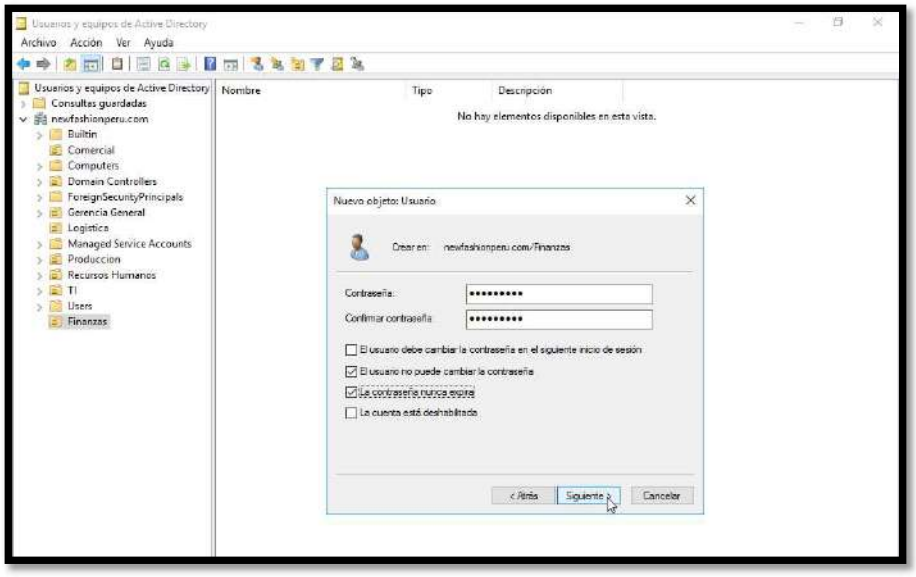
- Luego en la parte derecha dar clic derecho, elegir Nuevo y Usuario



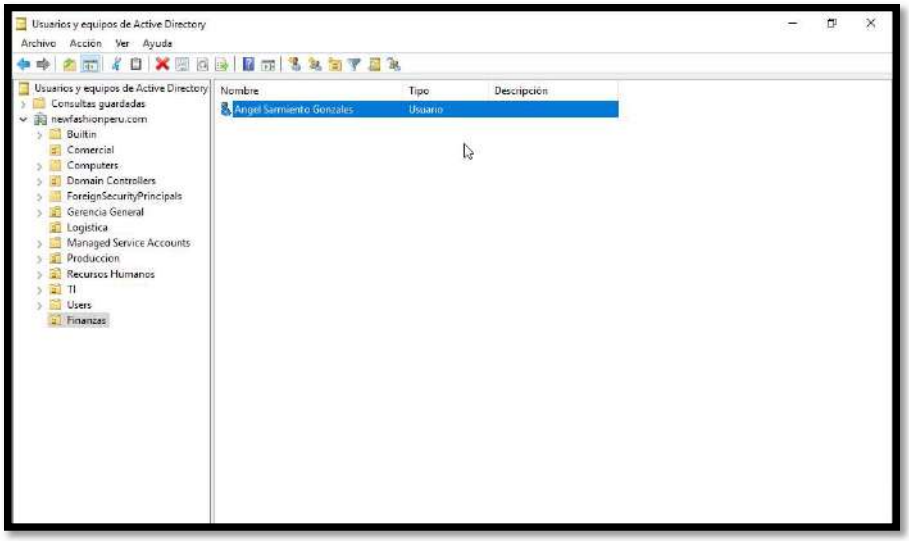
- Aparecerá la ventana para colocar los nombres y apellidos del usuario, así como el inicio de sesión por ejemplo ángel. sarmiento clic en Siguiente



- Luego colocar una contraseña de 8 caracteres como mínimo, que sea alfanumérico, tenga una mayúscula y un carácter. Marcar con check las opciones indicadas, luego Siguiente y Finalizar

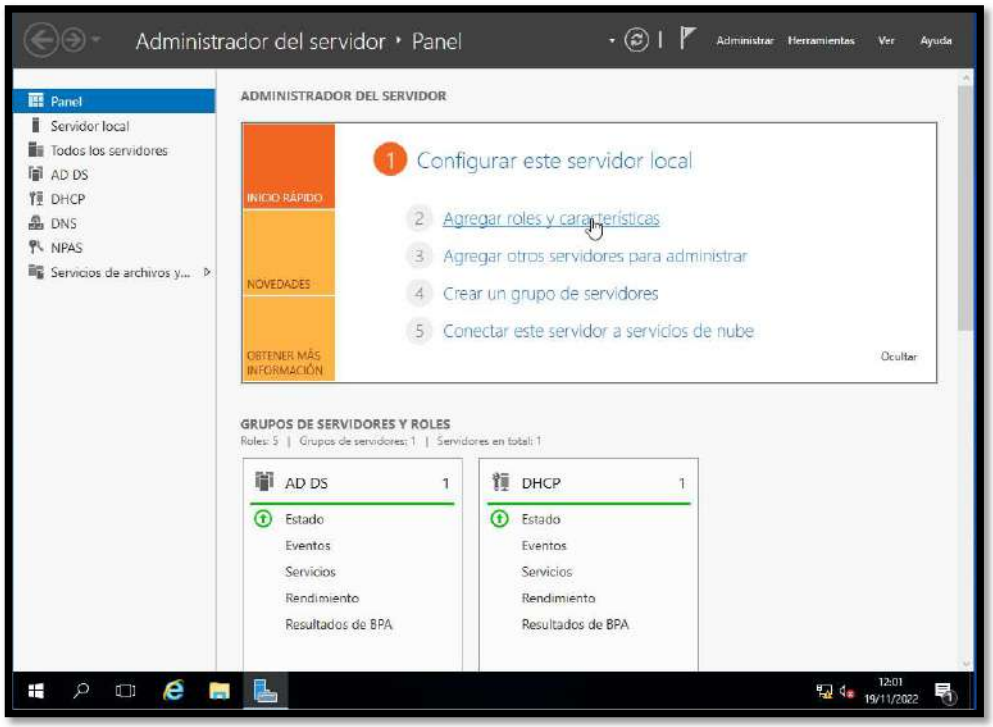


- Se observa que el usuario fue creado correctamente, así también como la Unidad organizativa.

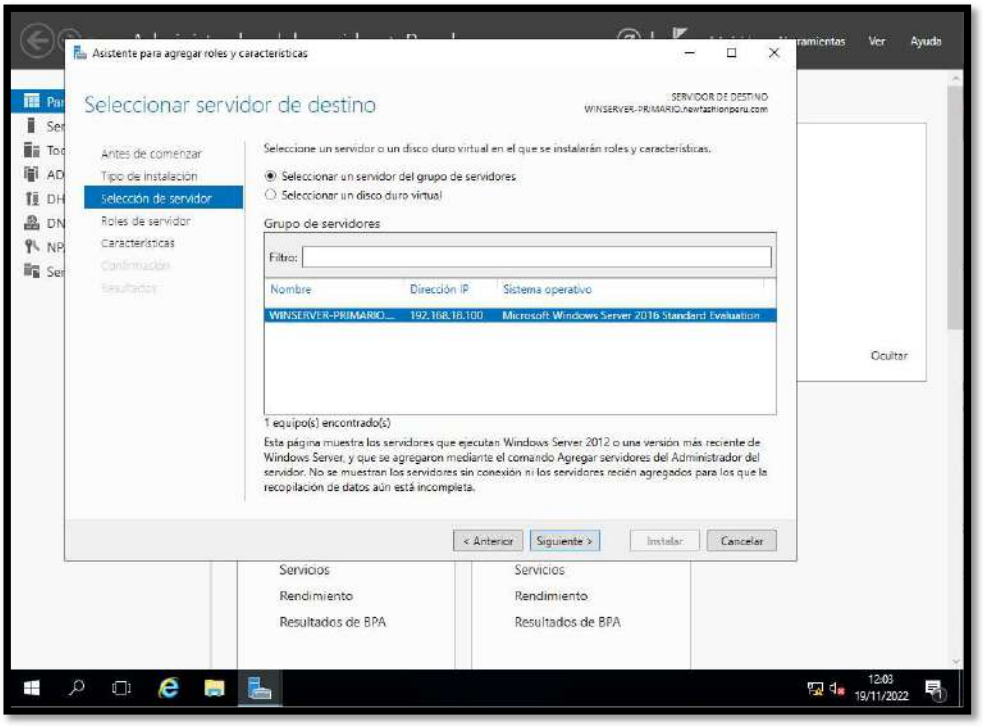


Paso 3: Configuración del File server

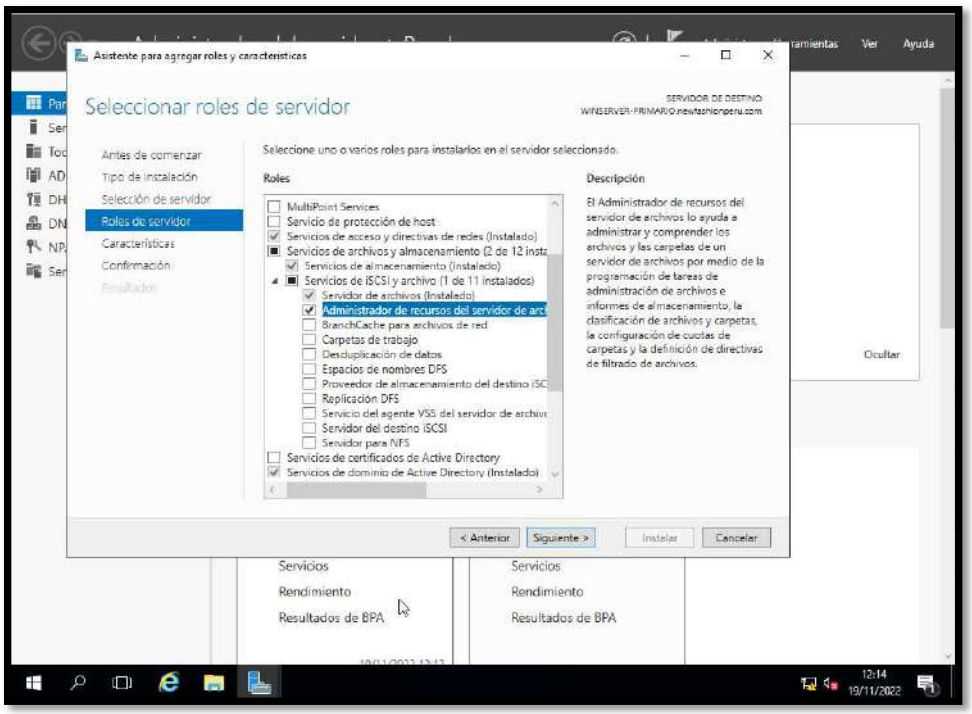
- Clic en Agregar roles y características



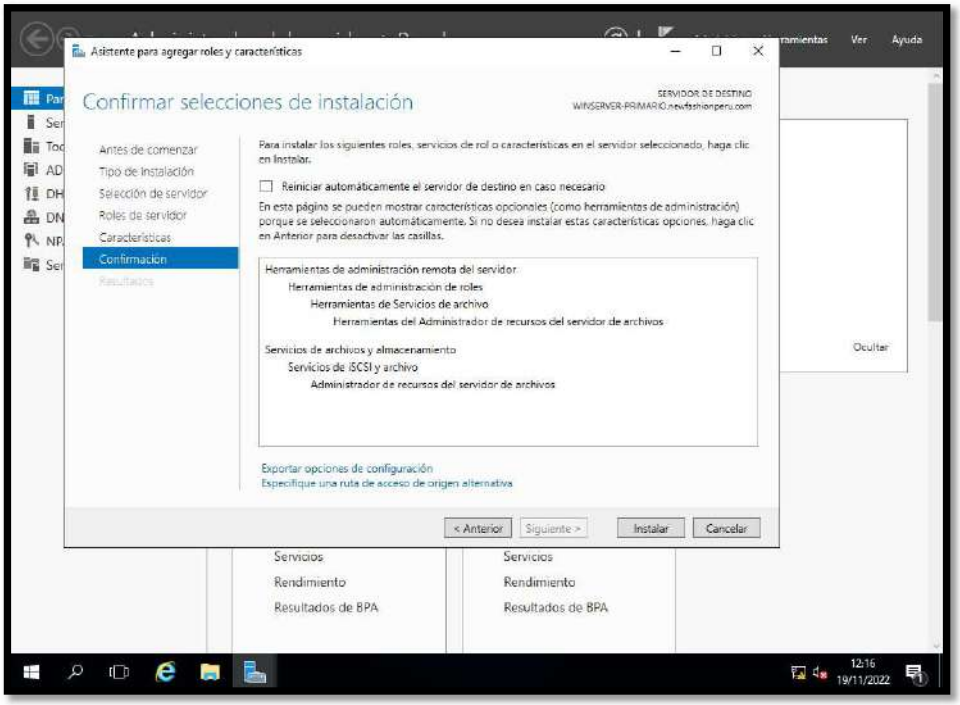
- Clic en Siguiente



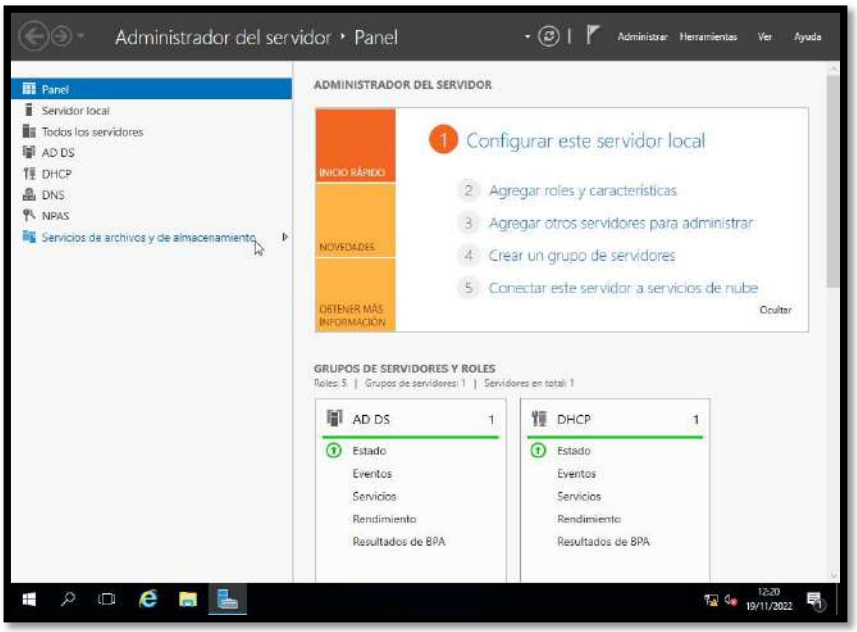
- Marcar las opciones indicadas. Clic en Siguiente.



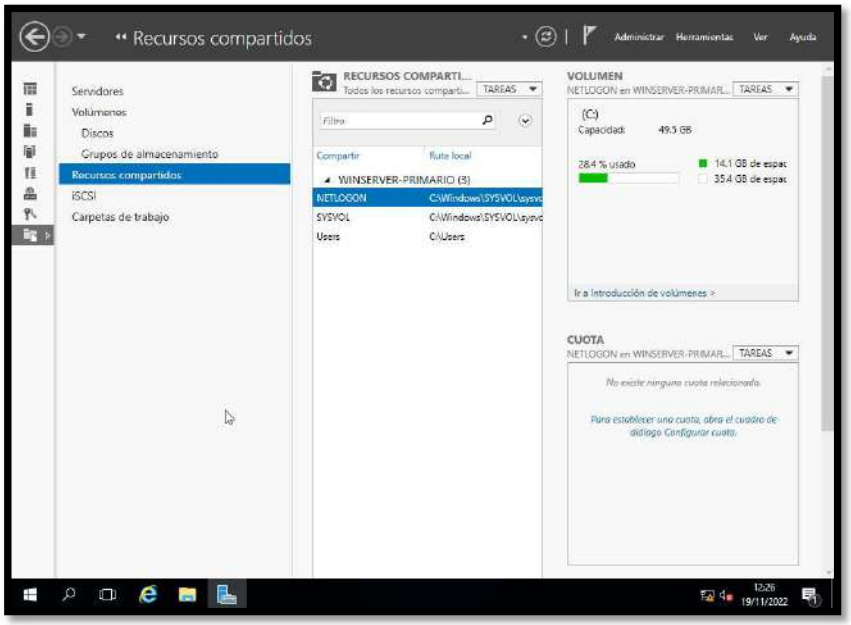
- Clic en Instalar



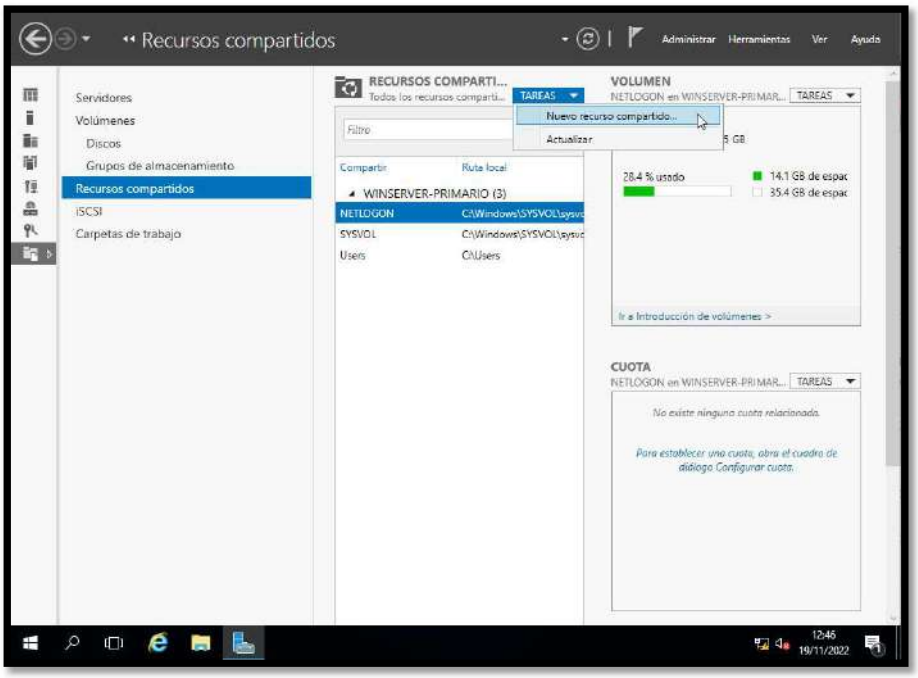
- Clic en Servicios de archivos y almacenamiento



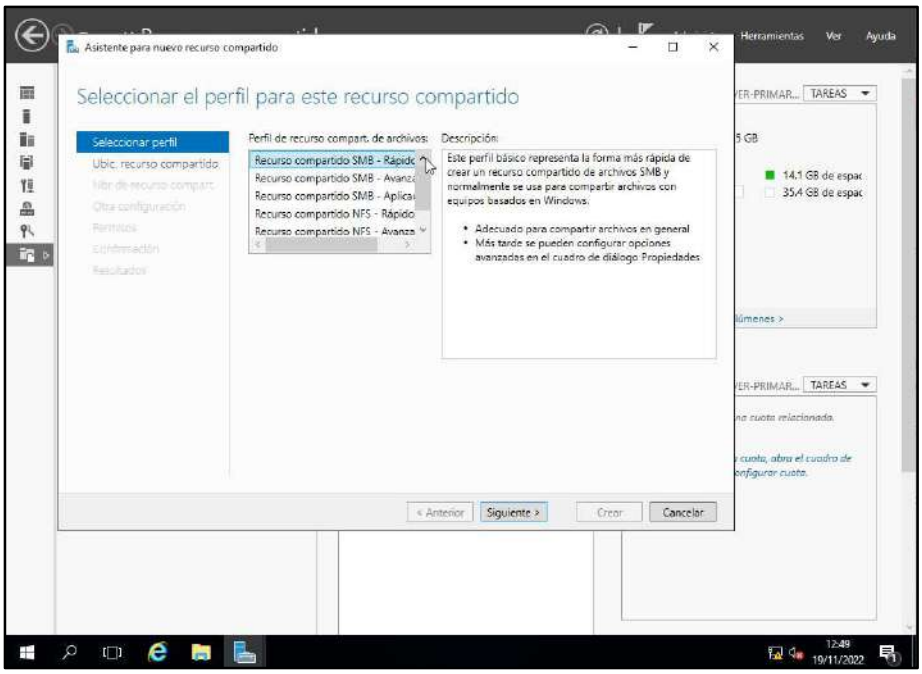
- Clic en Recursos compartidos



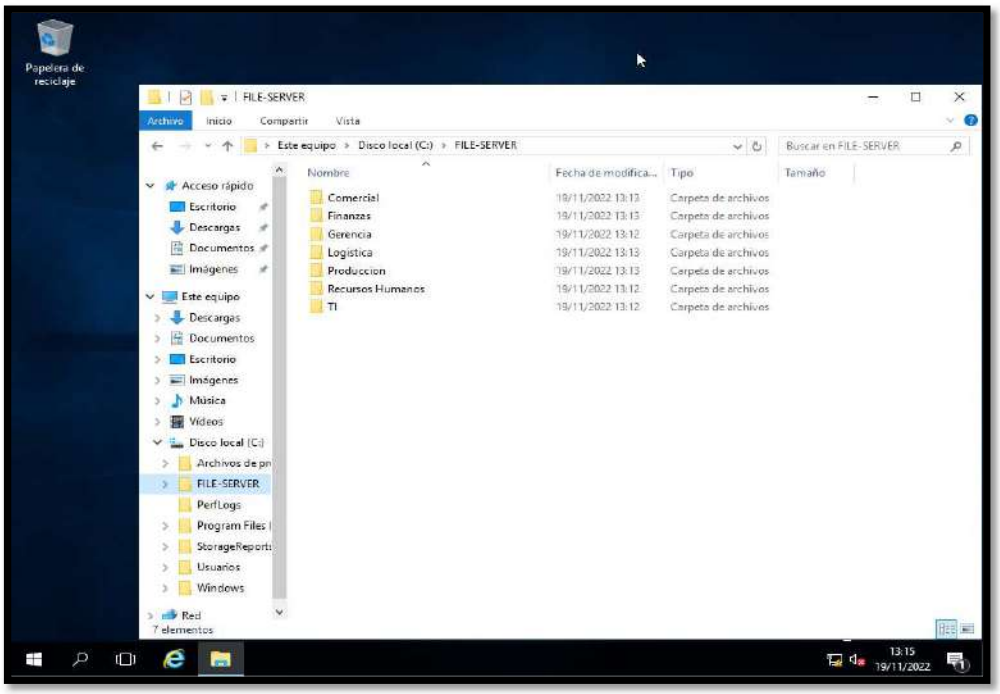
- Clic a Tareas y Nuevo Recurso compartido



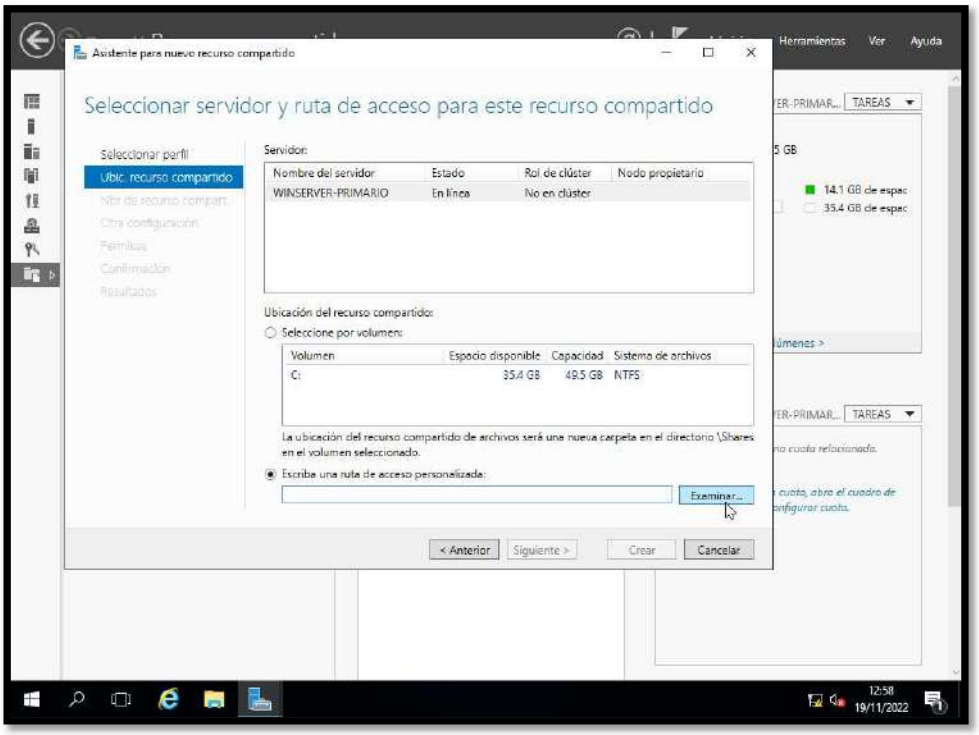
- Elegir para comenzar, Recurso compartido SMB - Rápido. Clic en Siguiente.



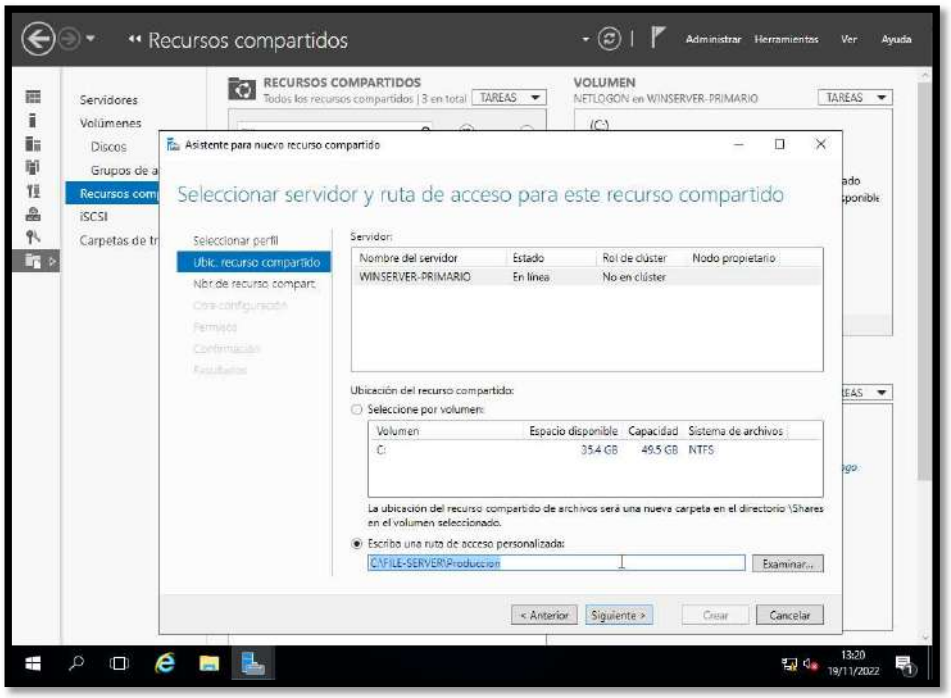
- Crear una carpeta en el Servidor, por Ej. File-Server que con tendrá las carpetas de todas las áreas y servirá para compartir los archivos con completa seguridad a los usuarios de la red.



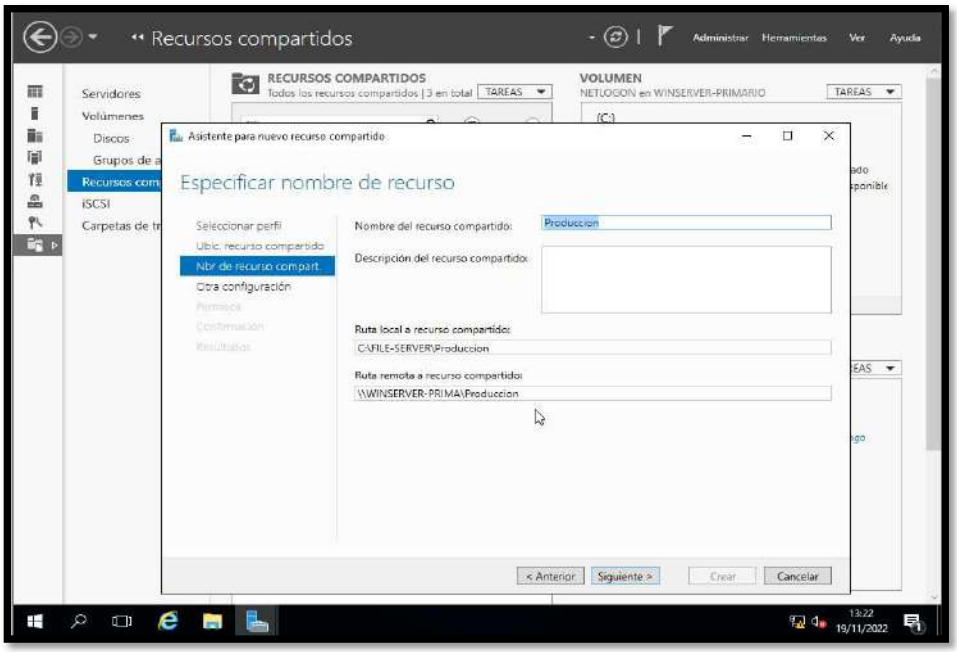
- Clic en Examinar y buscar la carpeta FILE-SERVER creado. Clic en Siguiente.



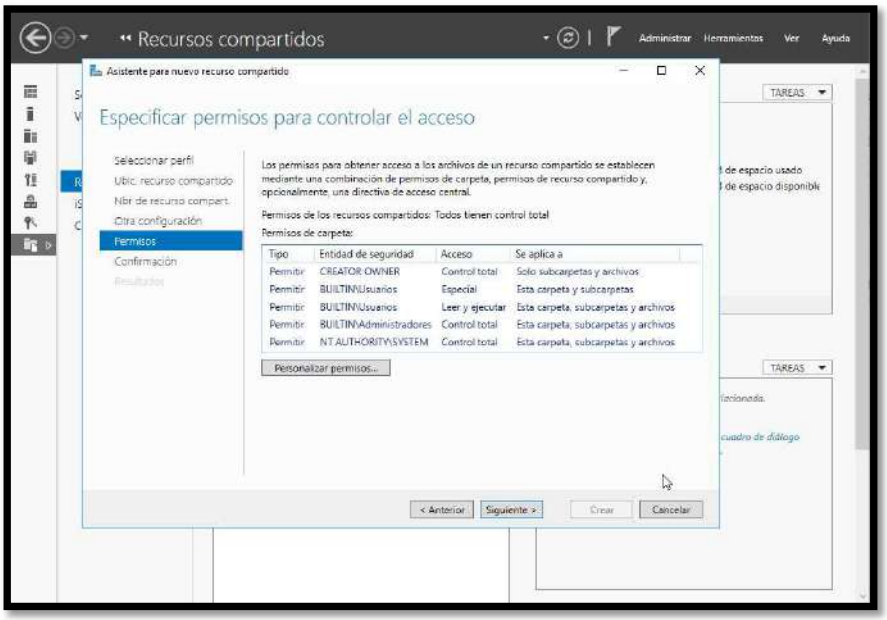
- Aquí elegimos por ejemplo la carpeta del área de Producción



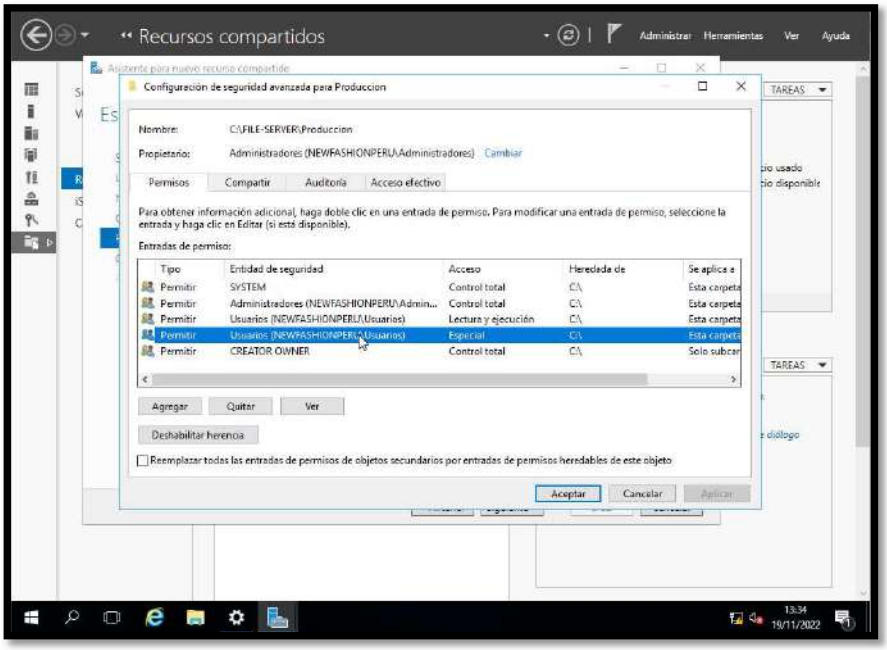
- Aquí si se desea se puede cambiar el nombre de la carpeta compartida o puede quedar igual, se observa también la Ruta remota de las carpetas compartidas que será visible para los usuarios de la red que tengan permiso. Clic en siguiente.



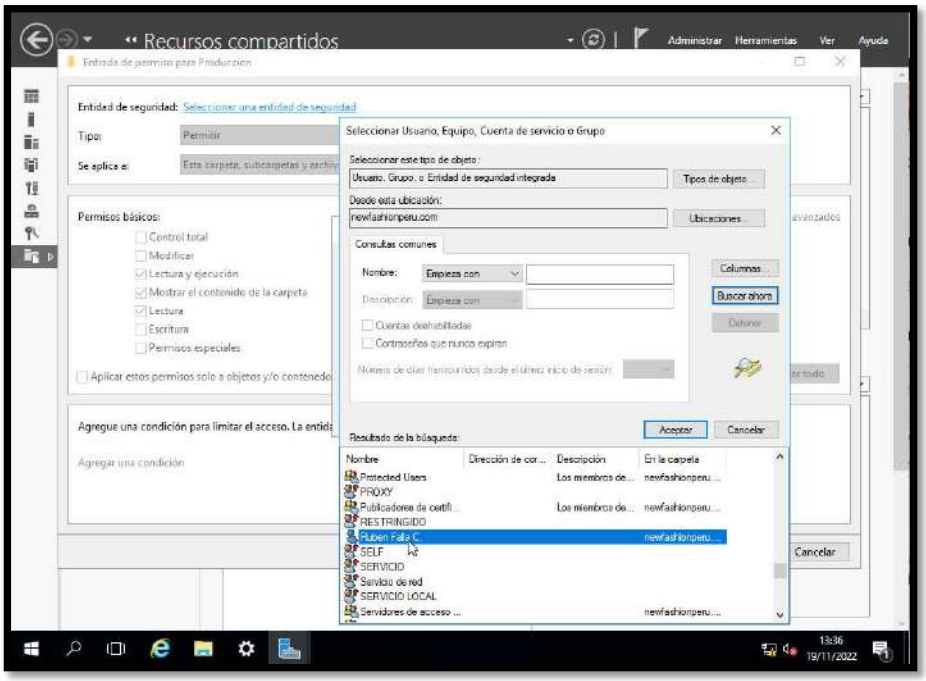
- Aquí se ven las carpetas que por default tienen permisos heredados, quitar las que no se necesite y dar acceso al usuario de la carpeta de Producción. Clic en Personalizar permisos.



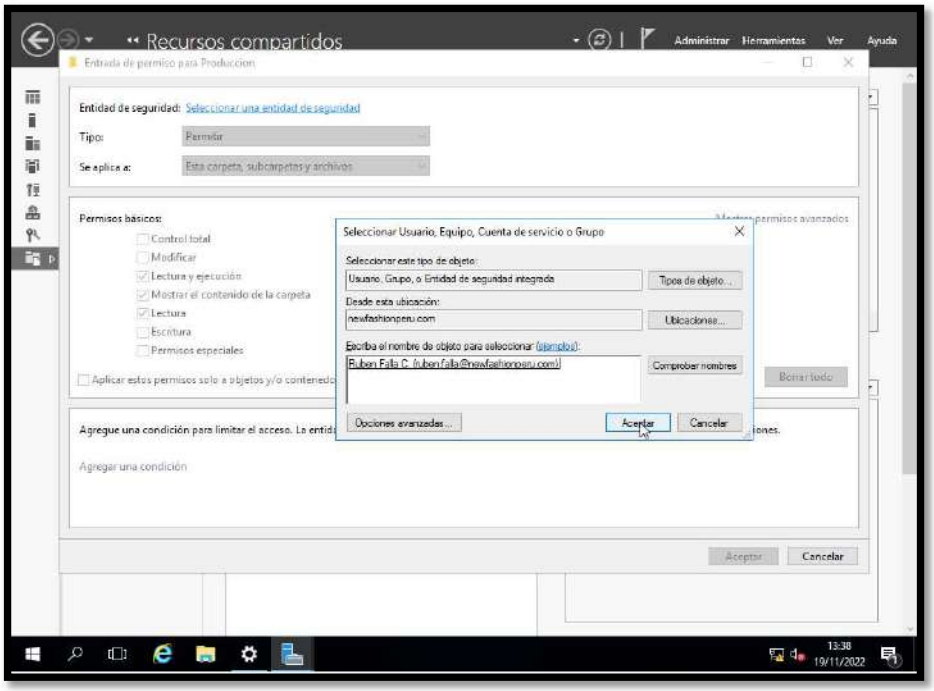
- Aquí eliminar y agregar permisos a los usuarios que son del área de Producción.



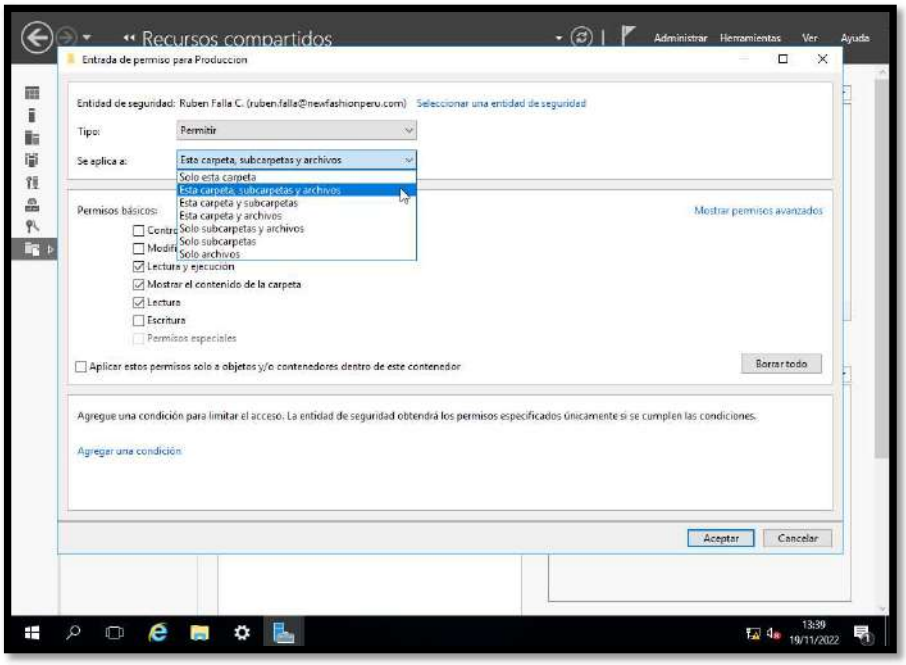
- Después de quitar a los usuarios que no corresponden, clic en Seleccionar una entidad de seguridad y elegir a los usuarios que se desea agregar.



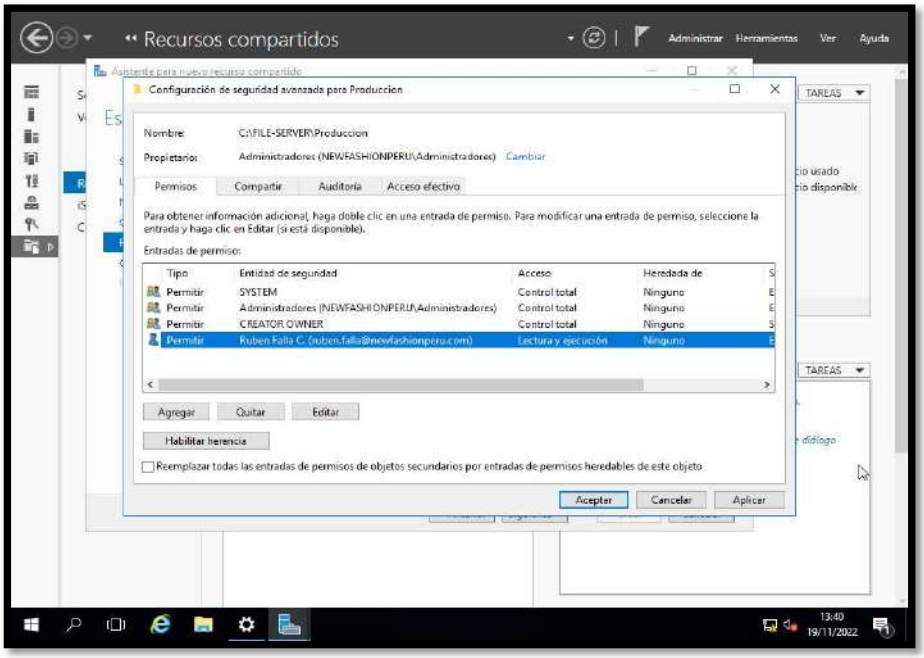
- Se elige al usuario y Aceptar.



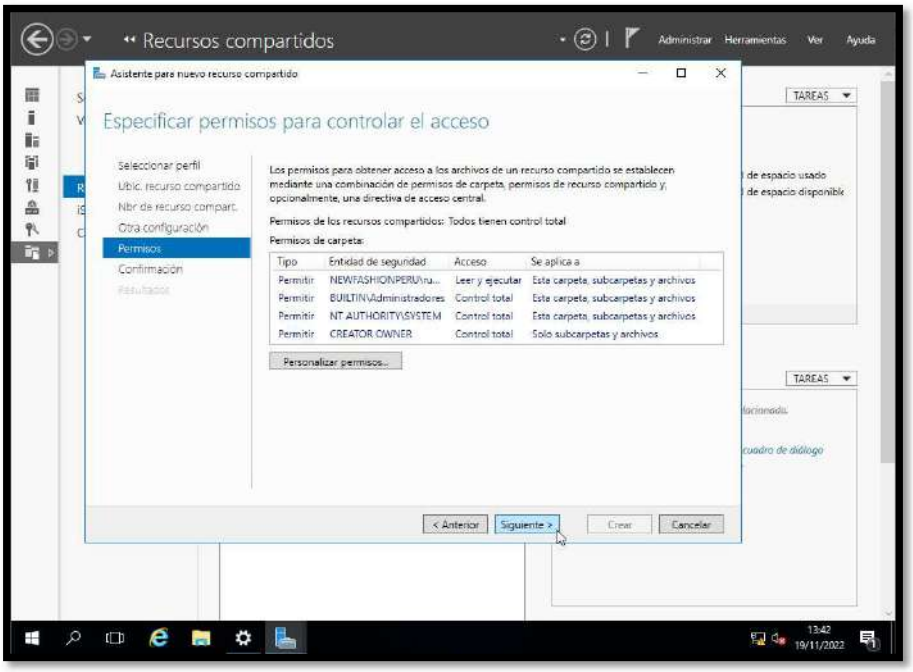
- Elegir que opciones de compartir se desea aplicar, Control Total, Lectura y ejecución, etc. Clic en Aceptar.



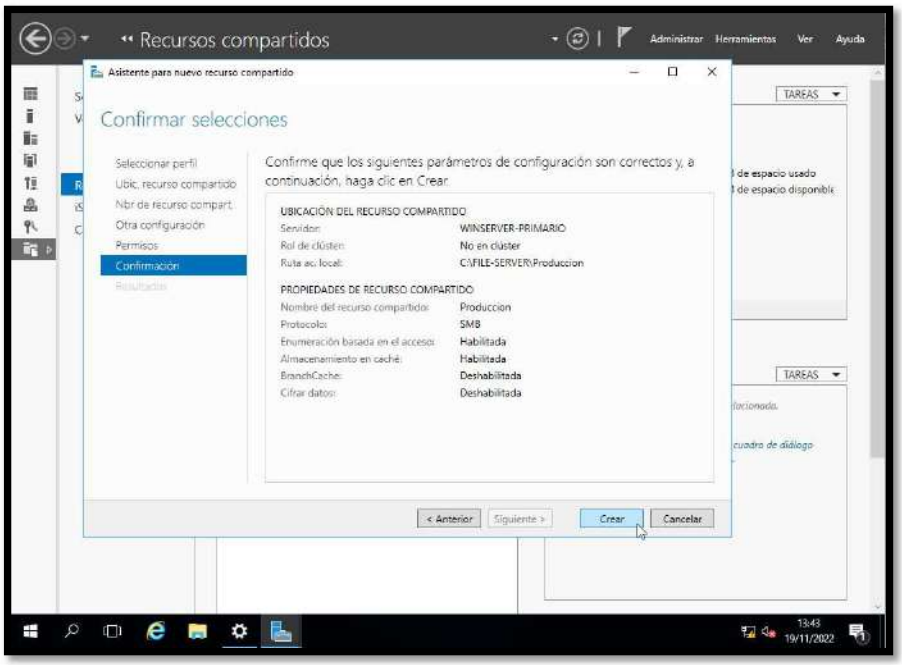
- Aquí se observa al usuario agregado, con la opción solo de Lectura y ejecución. Clic en Aceptar.



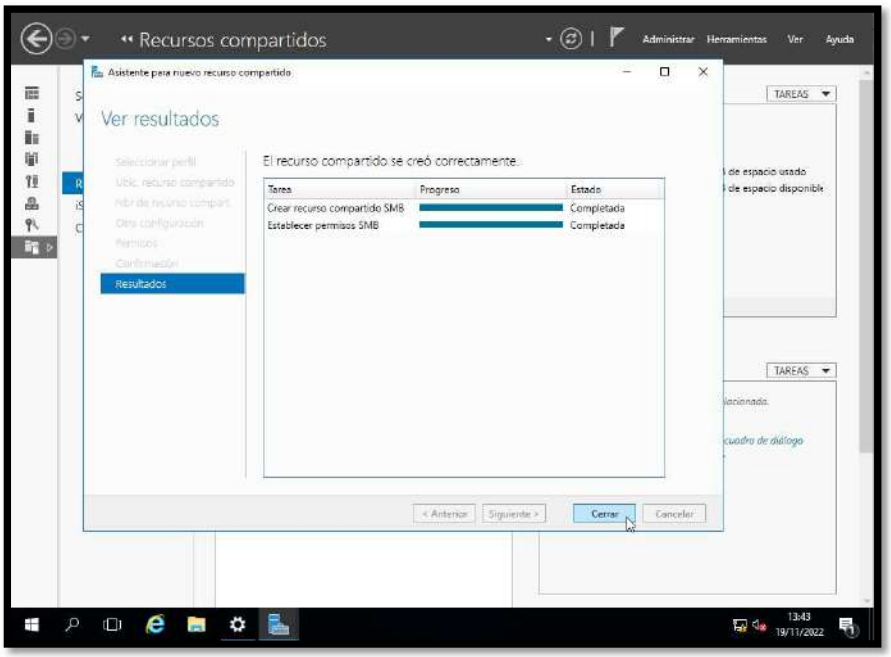
- Clic en Siguiente.



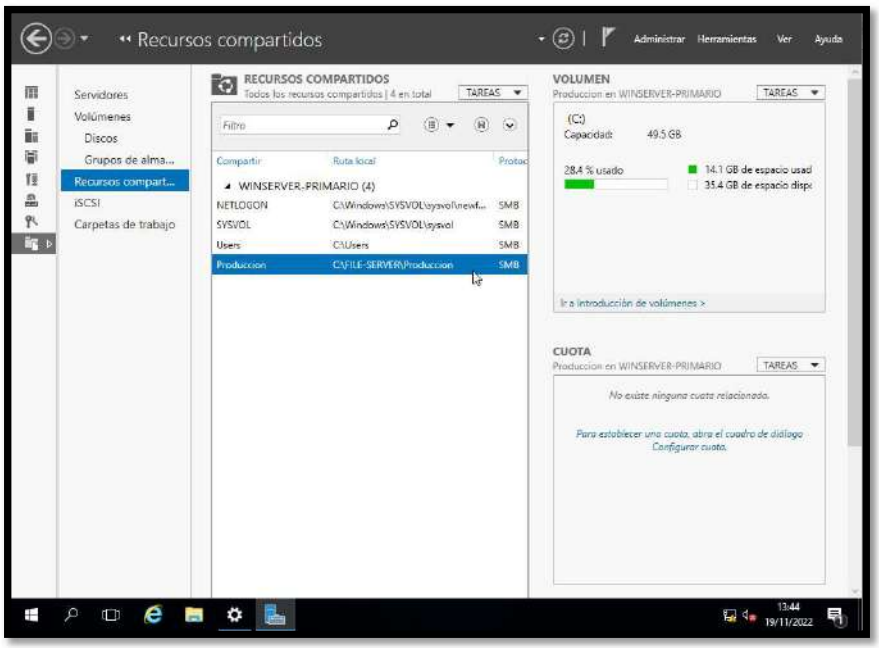
- Para finalizar, clic en Crear.



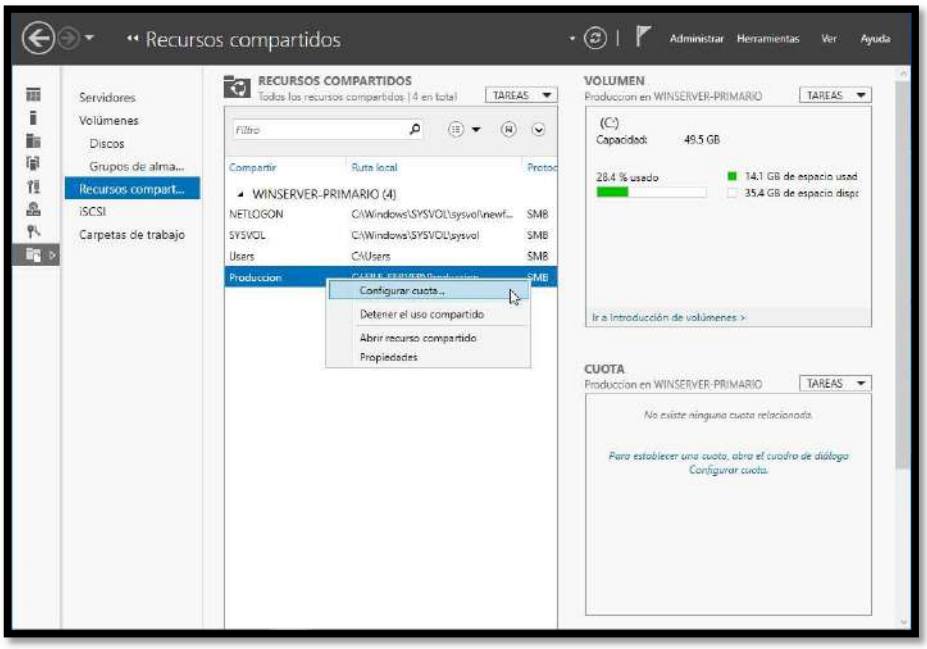
- Nuevamente clic en Crear.



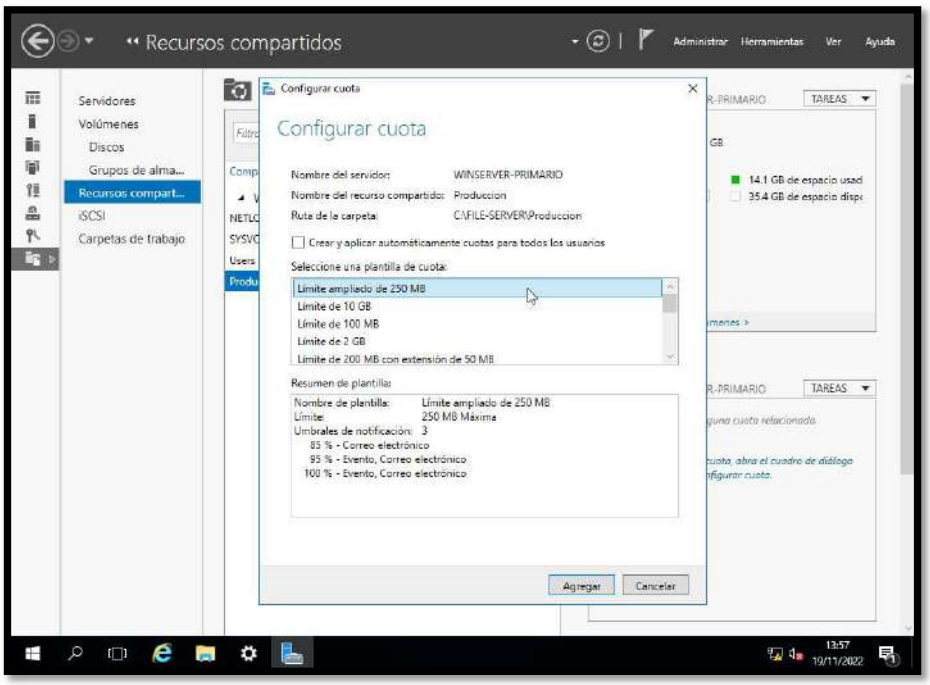
- Se observa que la carpeta Producción fue agregada con los permisos a los usuarios asignados.



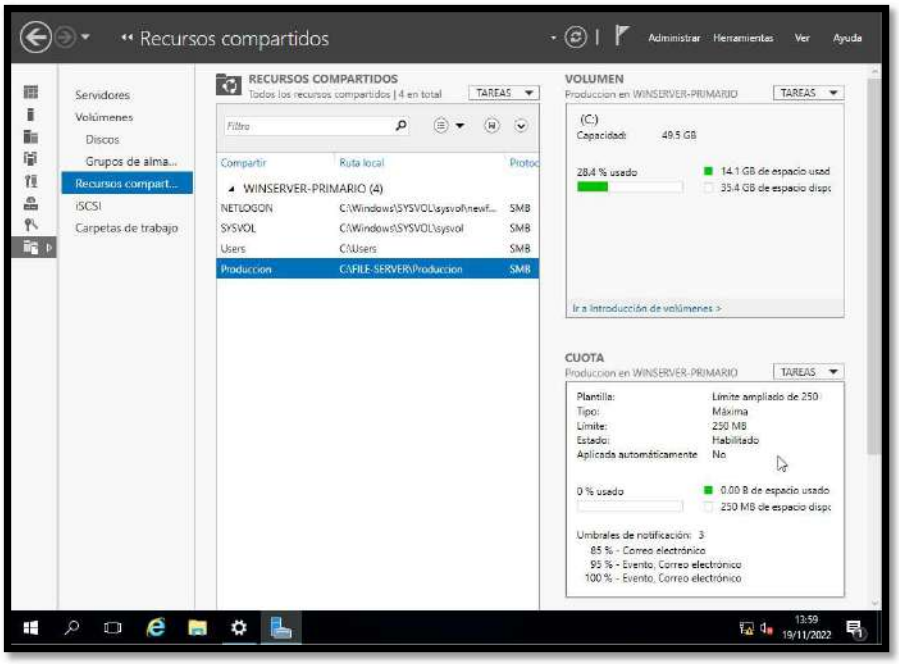
- También se puede configurar la cuota



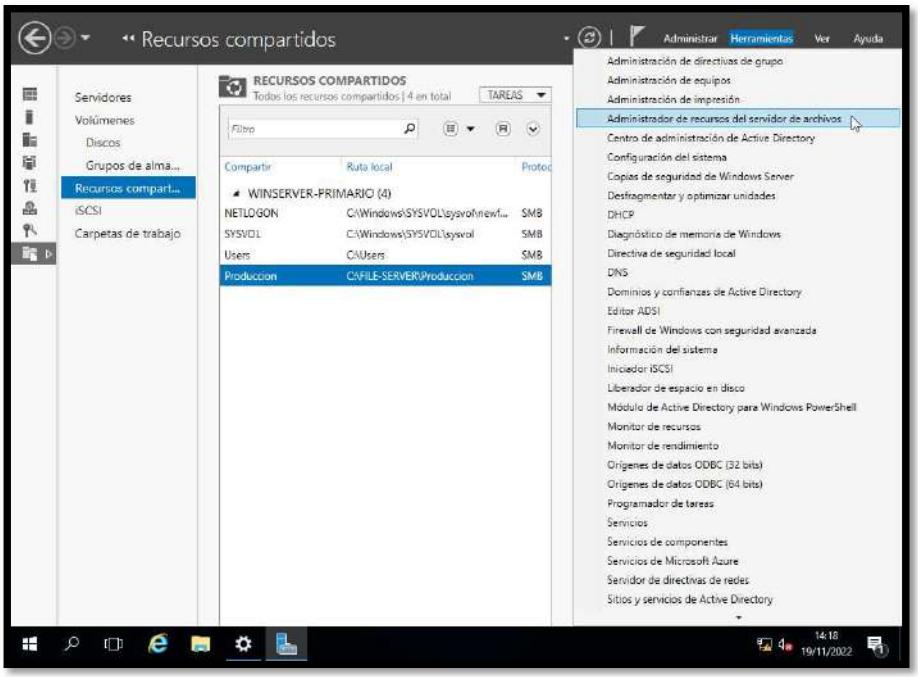
- Y elegir un tamaño de capacidad para la carpeta. Al llegar al 85% al usuario le saldrá un mensaje de aviso de que su carpeta ya se está llenando, por lo que tendrá que avisar a TI y explicar los motivos por los cuales solicita ampliación de capacidad.



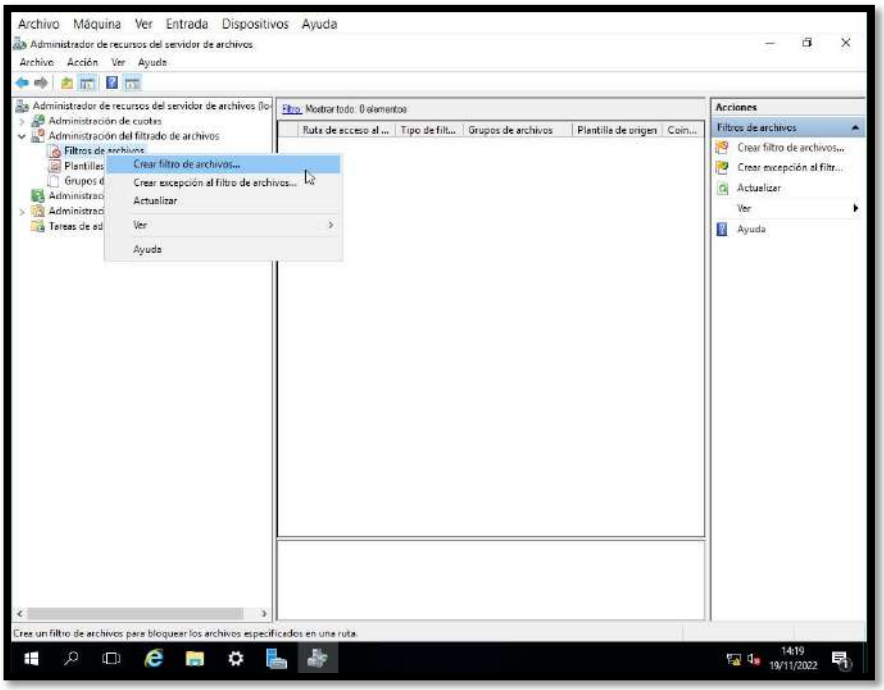
- En la parte inferior derecha se observa la cuota configurada.



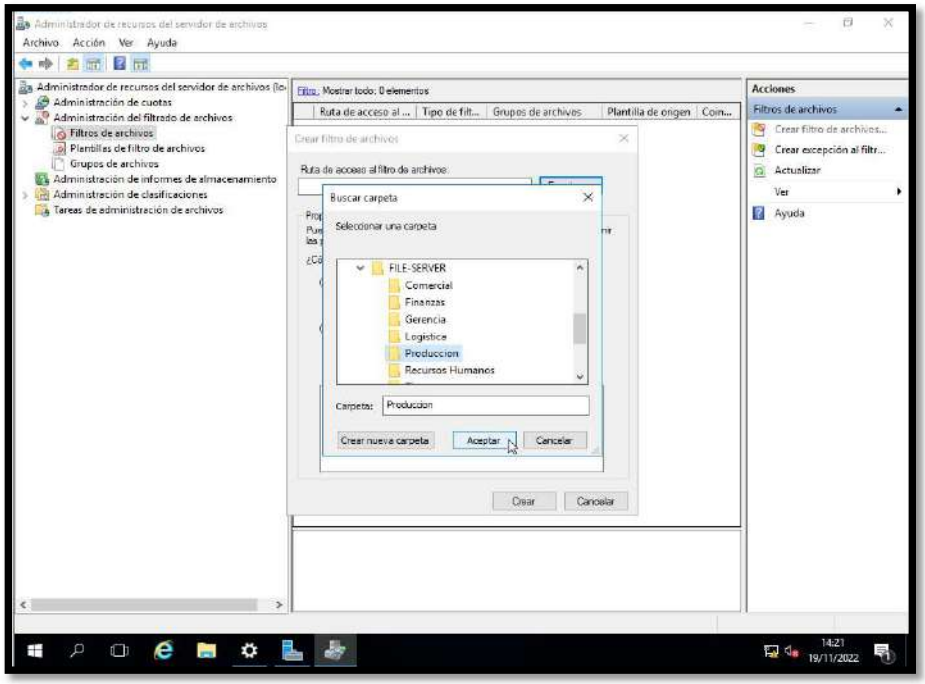
- Luego clic en herramientas y Administrador de recursos del servidor de archivos.



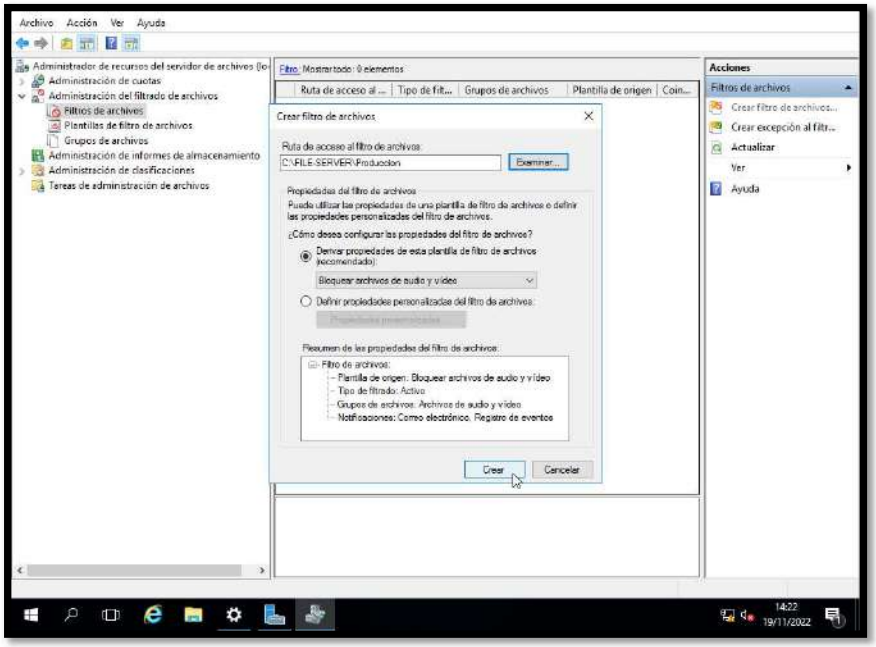
- Clic derecho en Filtros de archivos y Crear filtro de archivos.



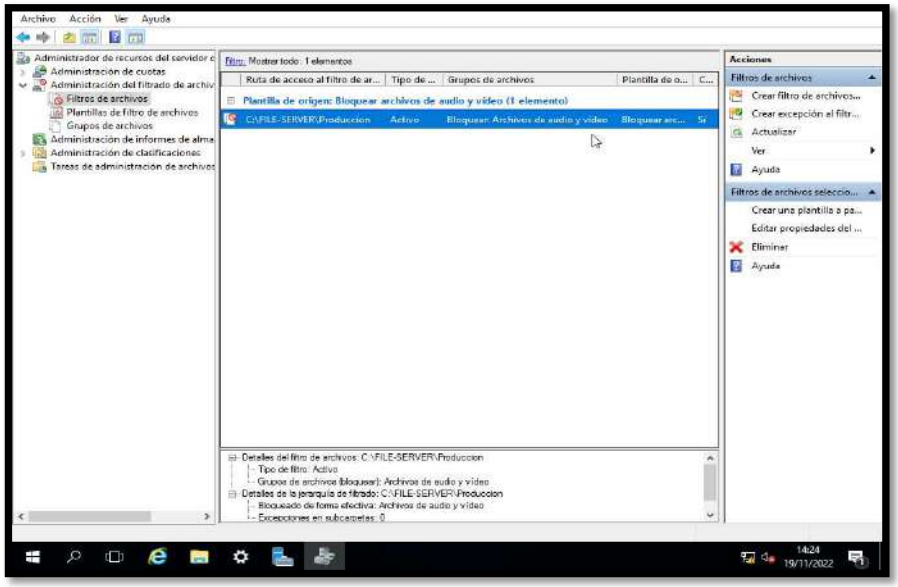
- Elegir la carpeta donde se desea filtrar los archivos. Clic en Aceptar.



- Se observa que la carpeta Producción ya cuenta con el filtro de archivos de audio y video, es decir, ya no podrá guardar en esa carpeta archivos con extensión .mp3, .mp4, .avi, etc.

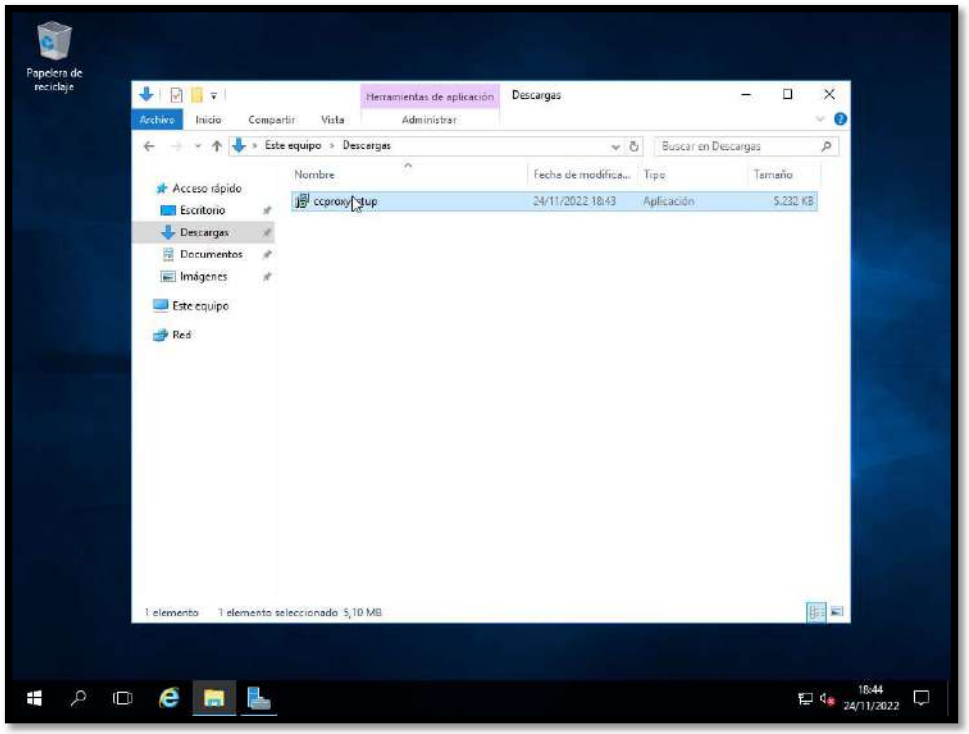


- Aquí se observa el resultado final de la carpeta Producción con las restricciones configuradas.

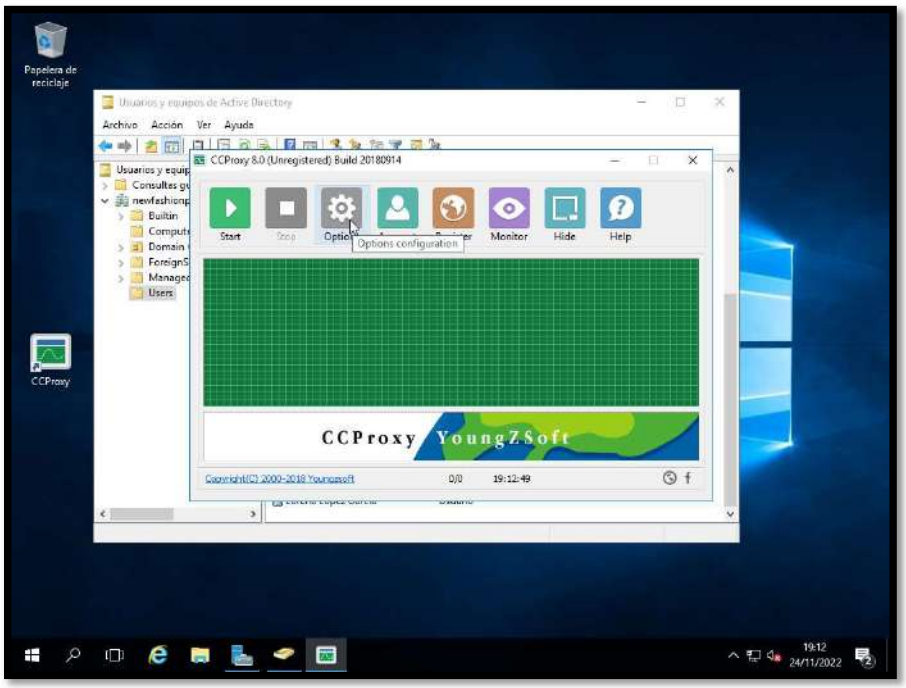


Paso 4: CONFIGURACIÓN DE PROXY EN WINDOWS SERVER

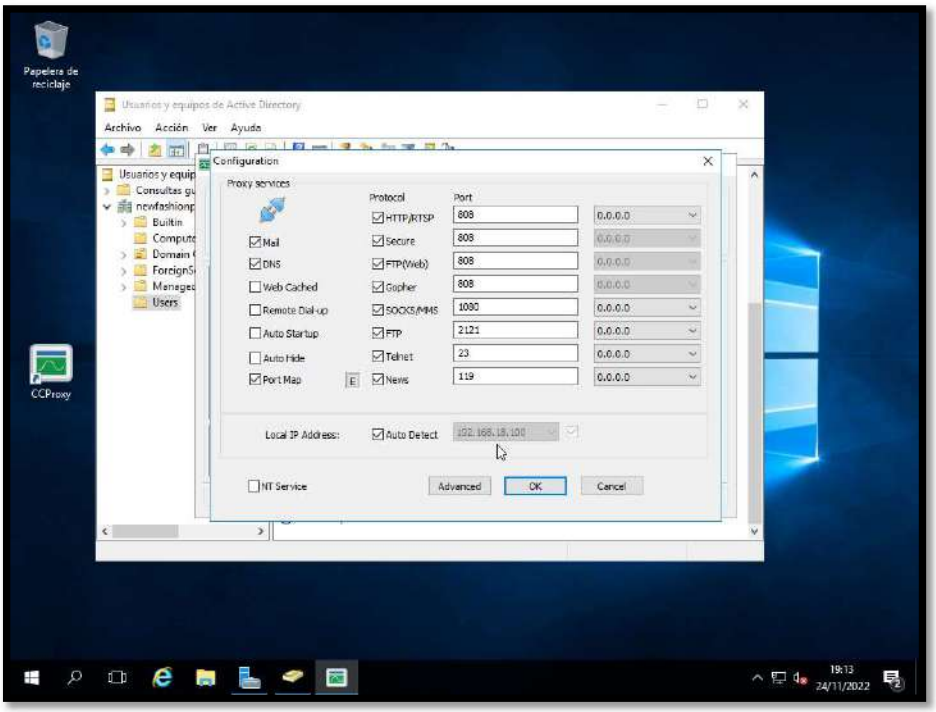
- Descargar el ejecutable ccproxysetup.exe



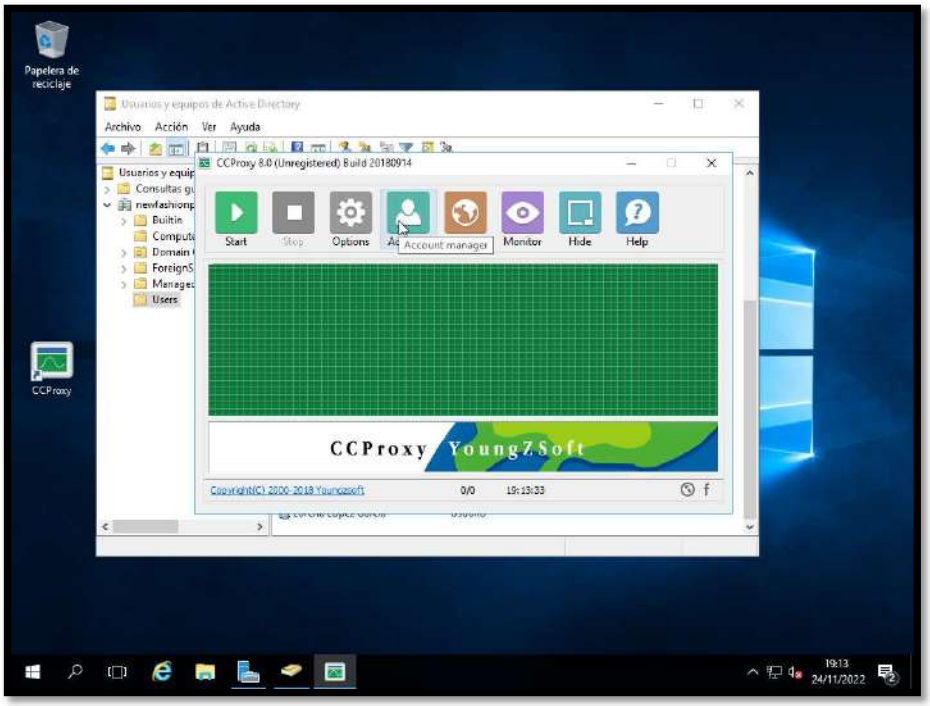
- Luego de instalarlo, dar clic en el ícono Options



- Aquí habilitar la opción Auto Detect y debe visualizarse el IP del servidor.

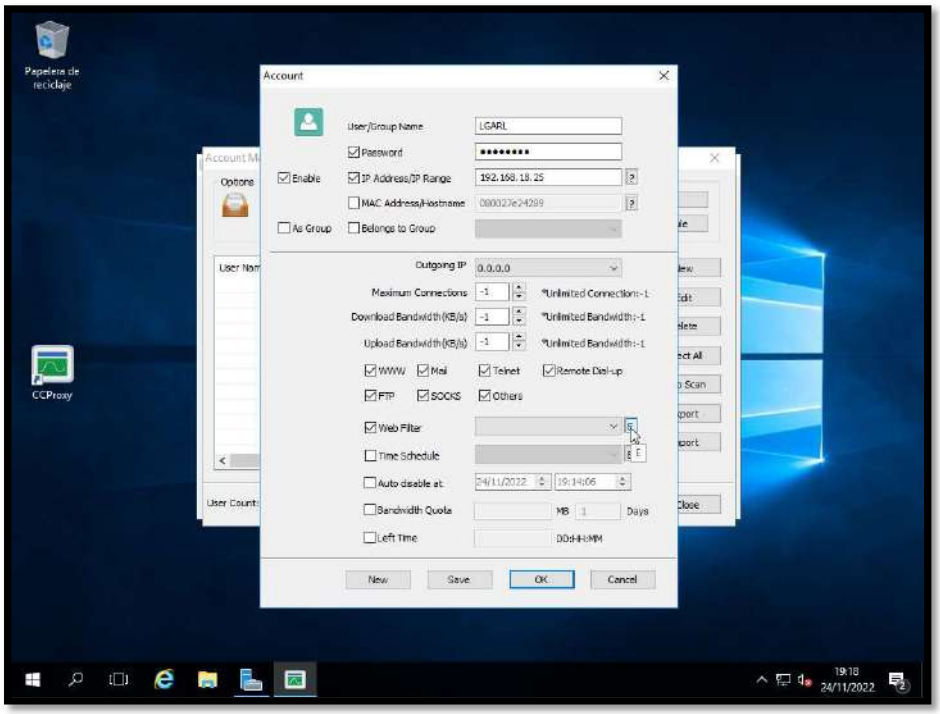


- Clic en Account Manager

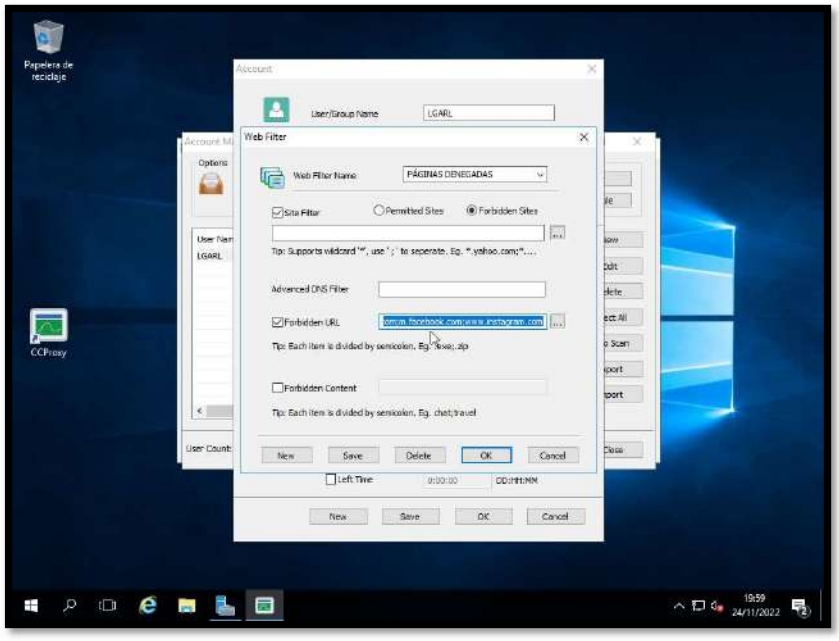


- Elegimos New para configurar las políticas para un usuario

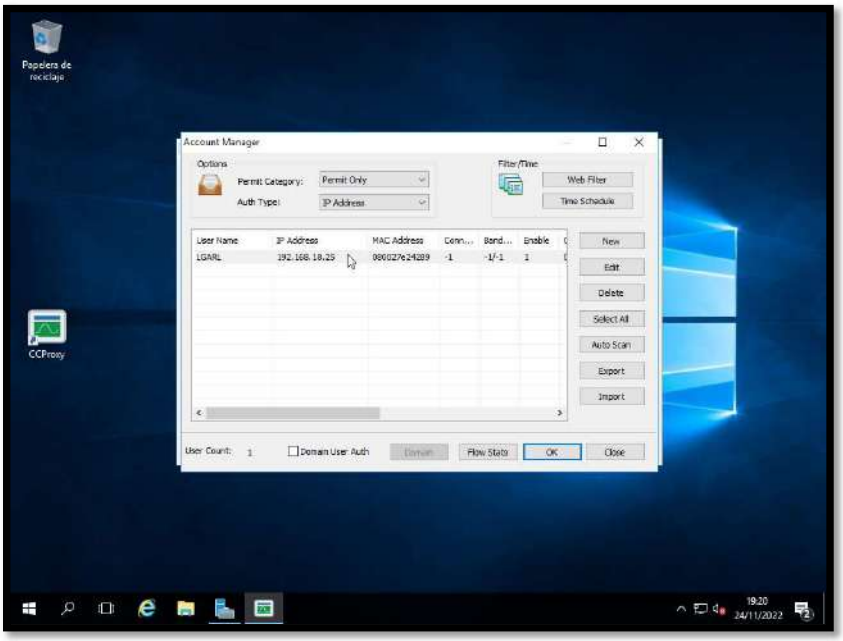
- Colocar las iniciales del usuario creado en el AD o el usuario completo, luego habilitar el check Web Filter y dar clic en E.



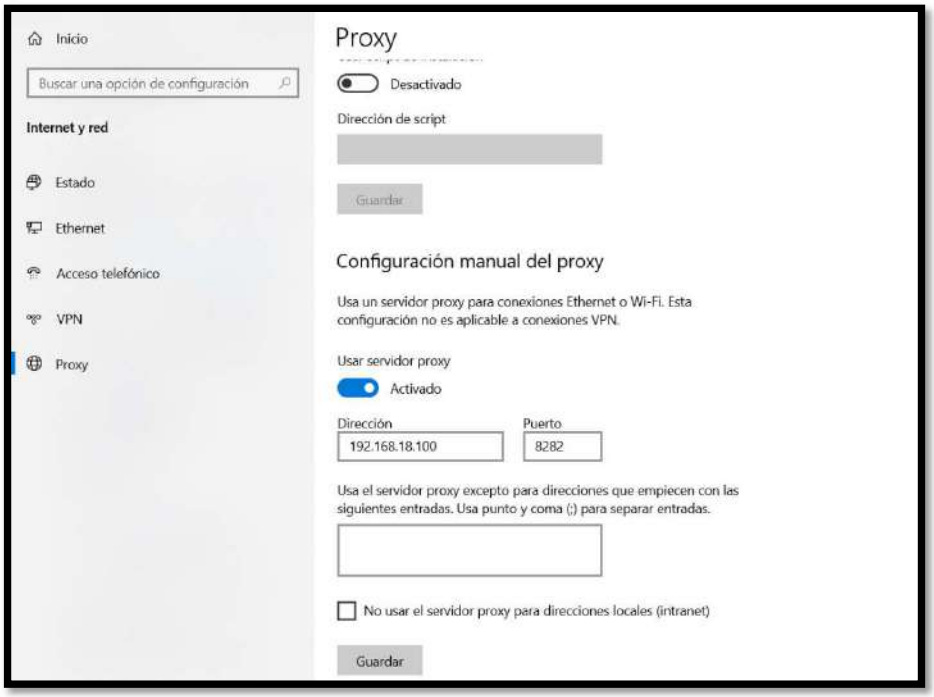
- Colocar un nombre en Web Filter Name, por ejemplo PAGINAS DENEGADAS, habilitar el check Forbbiden URL y colocar las páginas web que serán bloqueadas, por ejemplo
- . www.youtube.com
- www. Facebook.com



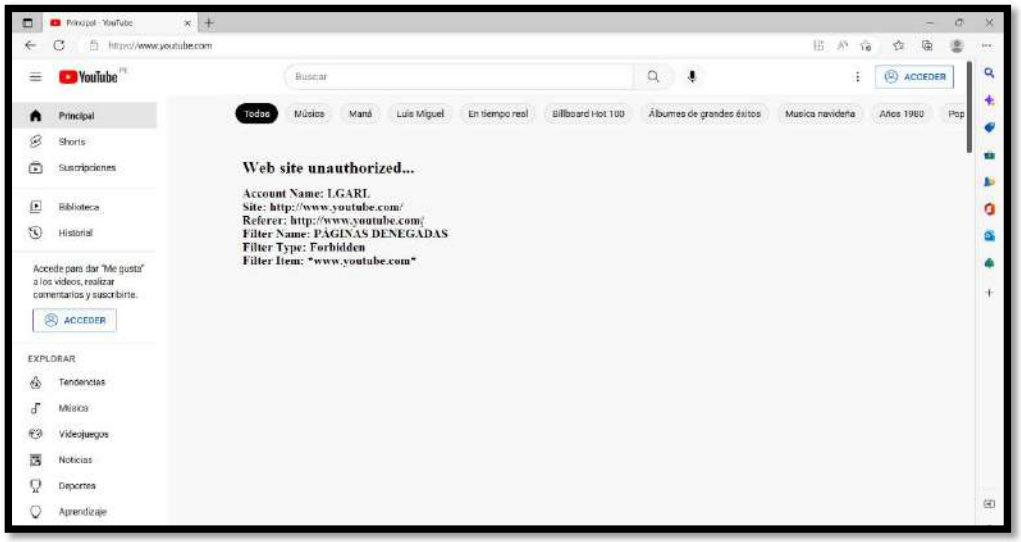
- Aquí vemos que se agregó correctamente el usuario.



- Luego en el cliente Windows 10, buscar Proxy en configuración y colocar el IP del servidor y de preferencia el puerto TCP 8282.



- Observamos en la barra de búsquedas que la página www.youtube.com no está autorizada por lo tanto, no se muestra en el navegador y sale un mensaje de que el usuario configurado no puede ingresar a esa web.
-



Paso 5: Crear cuenta en Azure

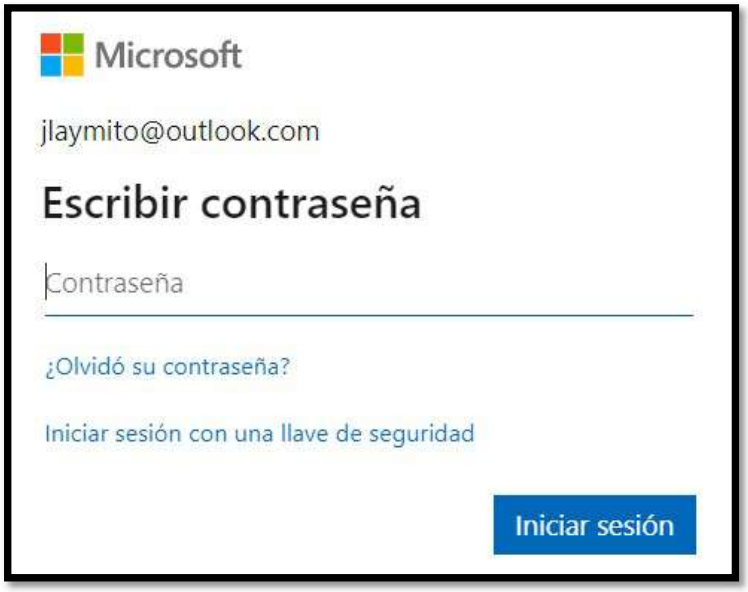
Creación de cuenta de usuario en la nube de Azure

Para crear una cuenta debemos entrar a azure.microsoft.com y dar clic en la opción Cuenta gratuita.

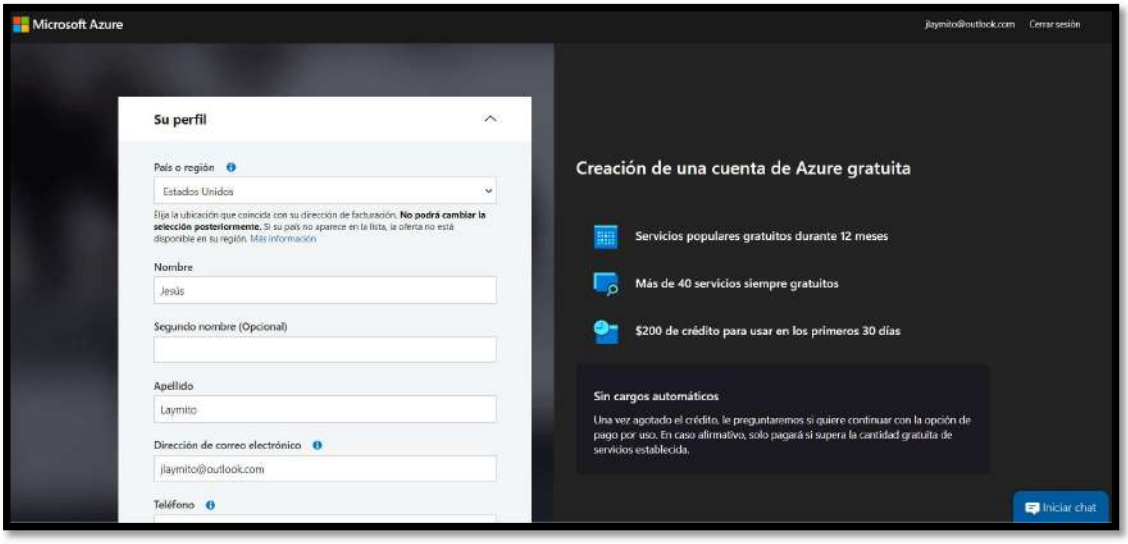
- Luego clic en la opción **Empiece grati**

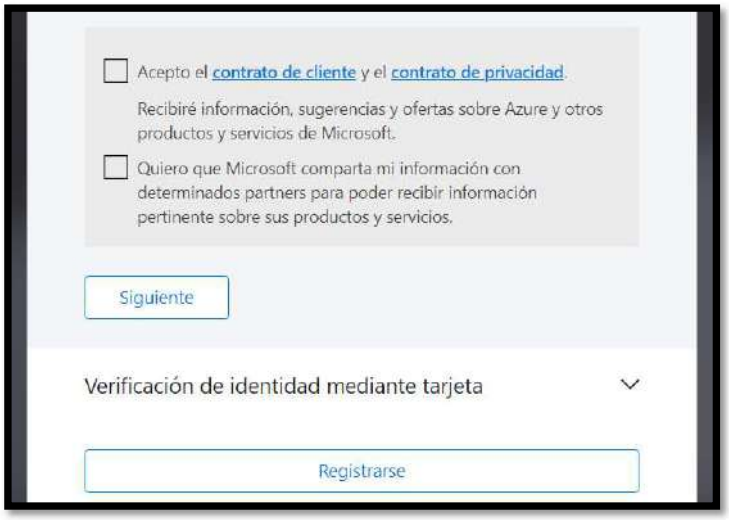
s

- Luego tenemos que ingresar un correo válido @hotmail.com o @outlook.com



- Creación del perfil en Azure

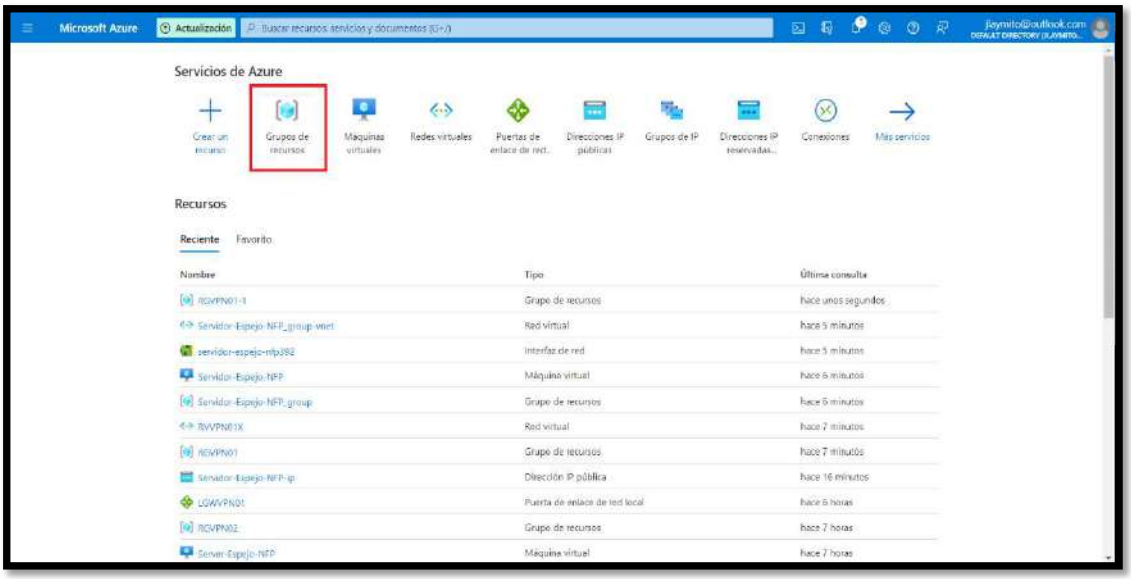




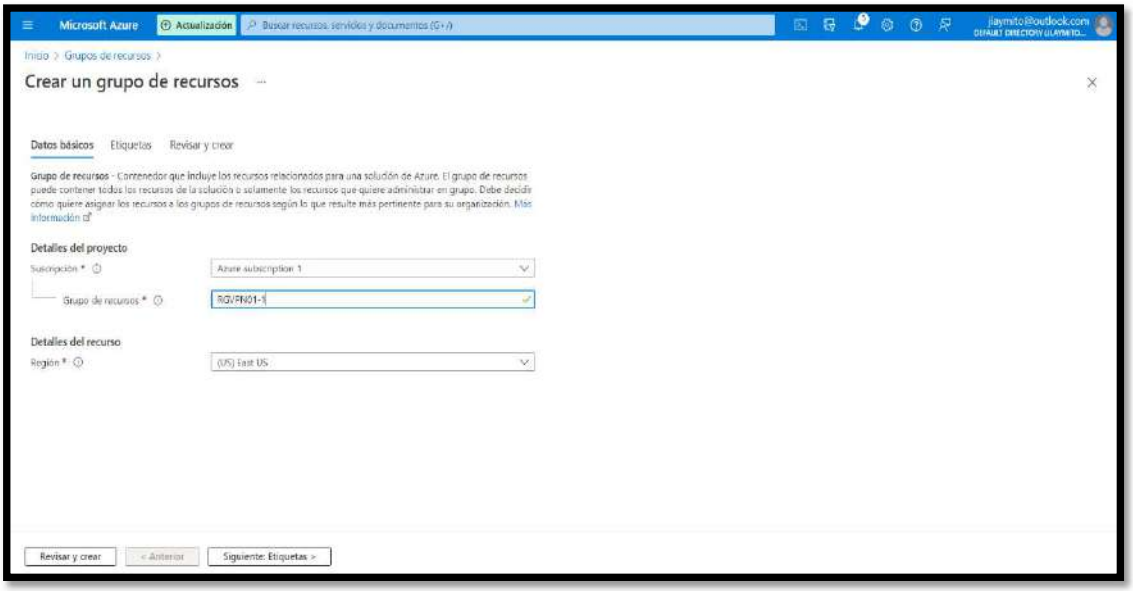
- De esta manera podemos habilitar una máquina virtual para realizar las pruebas y posteriormente el servidor espejo final.

Paso 6: creación de una vpn site to site en Azure

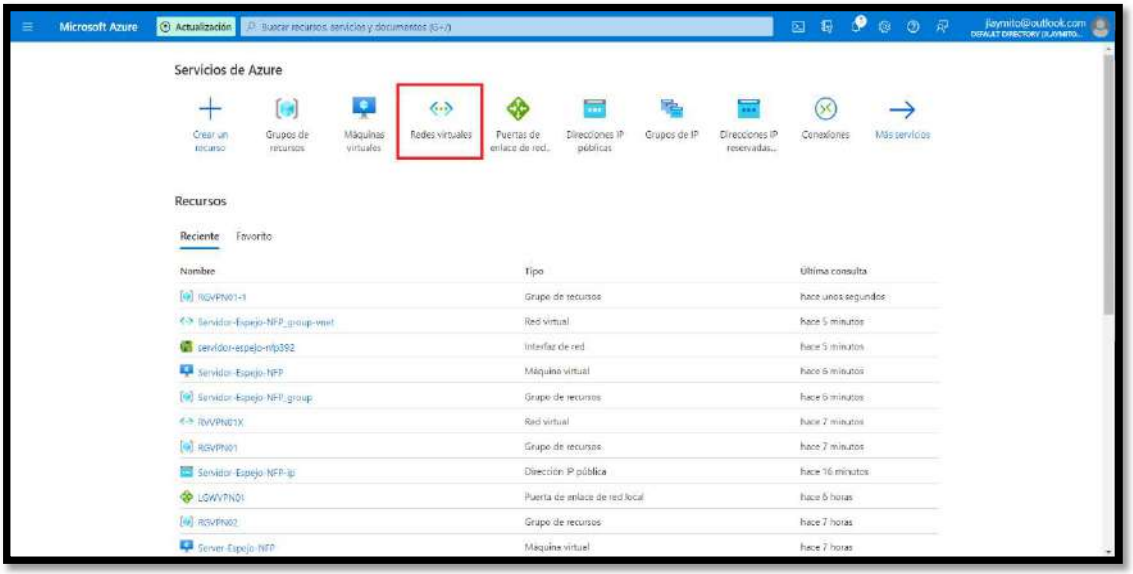
- Crear grupo de recursos, aquí se colocarán los elementos que se utilizarán para la vpn site to site



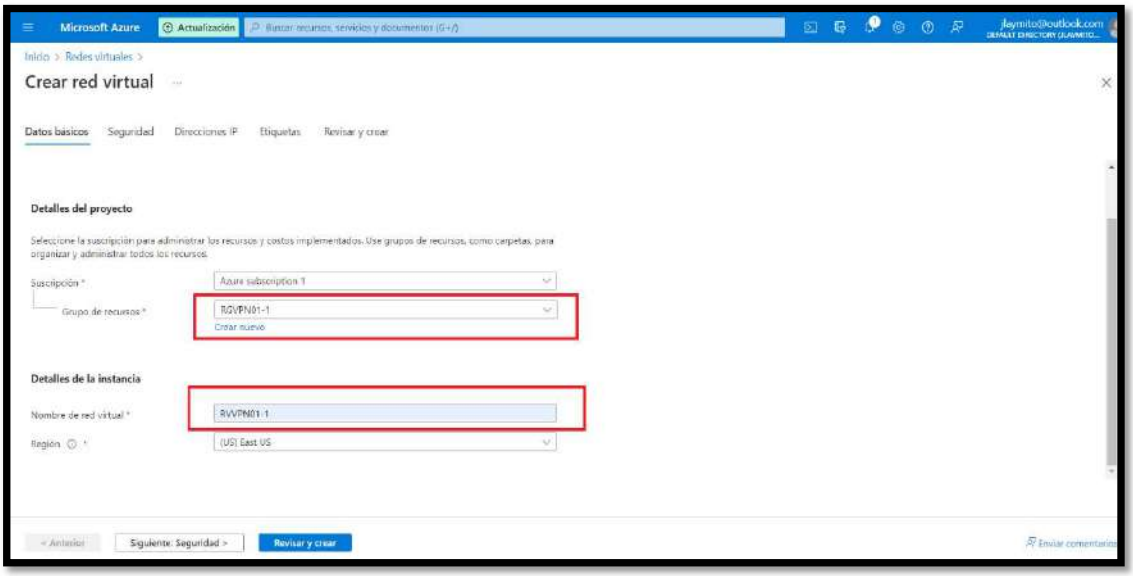
- Seleccionar una suscripción, colocar un nombre para grupo de recursos, la ubicación. Luego revisar y crear.



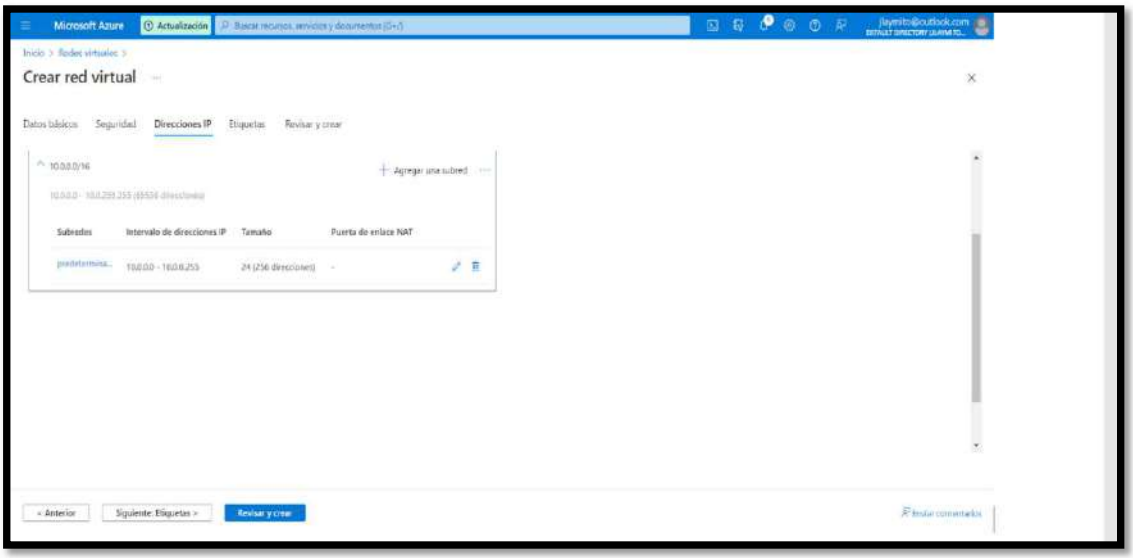
- Luego crear una red virtual o vnet



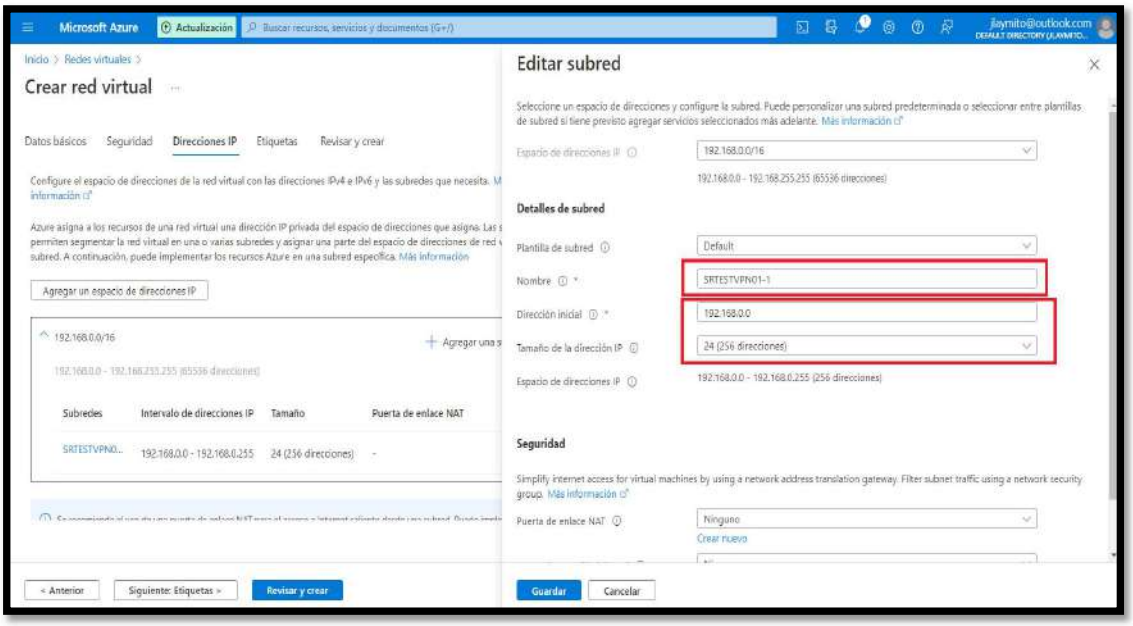
- Colocar el grupo de recursos creados en el paso anterior y un nombre para la red virtual.



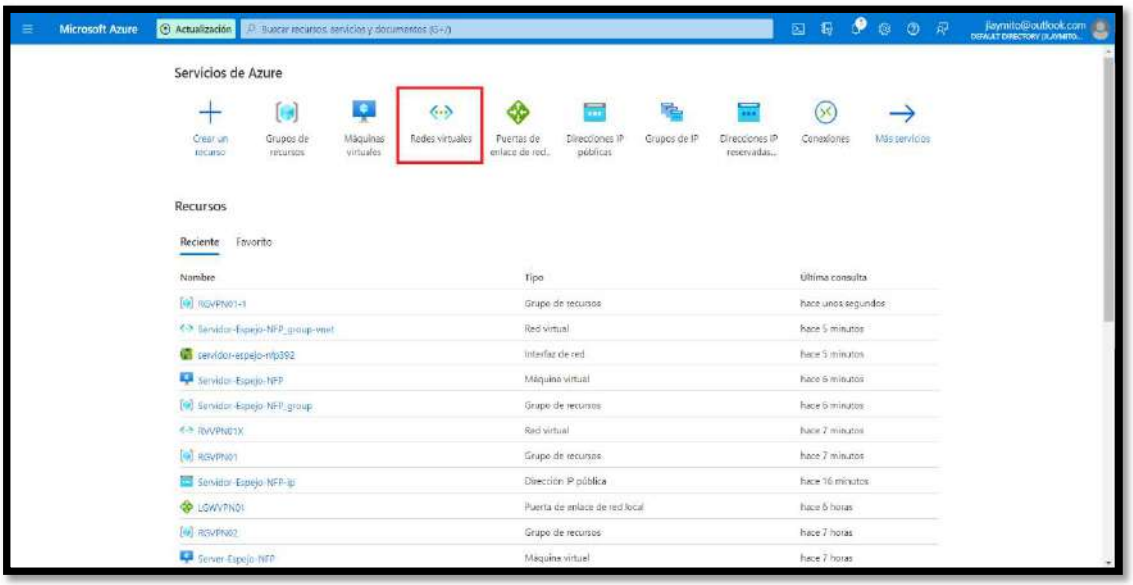
- Aquí se muestra el ip por default 10.0.0.0/16 agregar en subredes un nuevo segmento /24



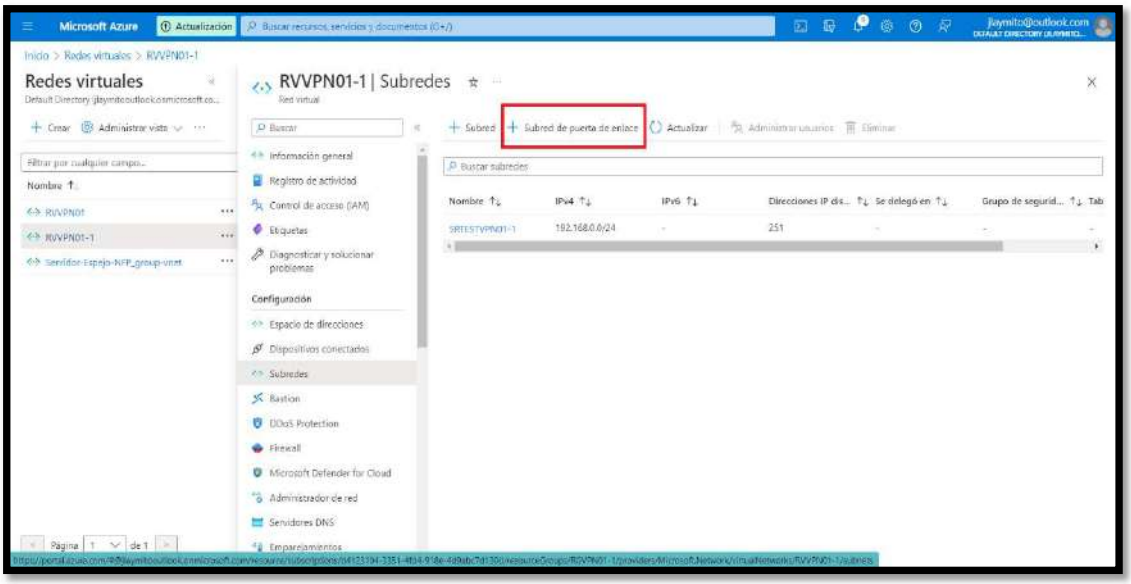
- Aquí se cambia el nombre de la subred por un nombre más representativo.



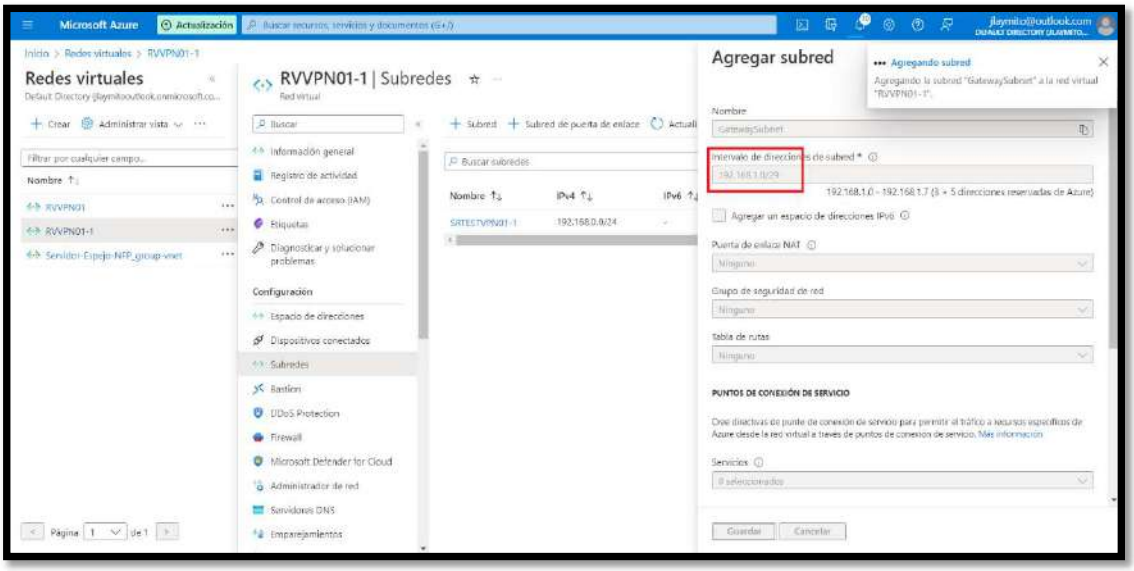
- Ingresamos otra vez a redes virtuales



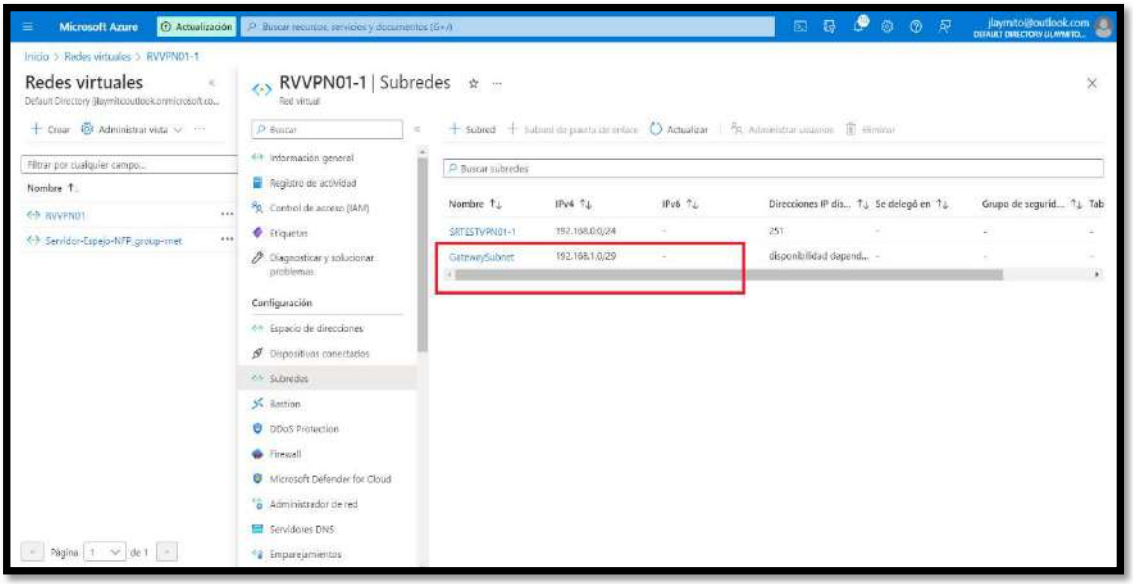
- Dar clic en subredes y en subred de puerta de enlace



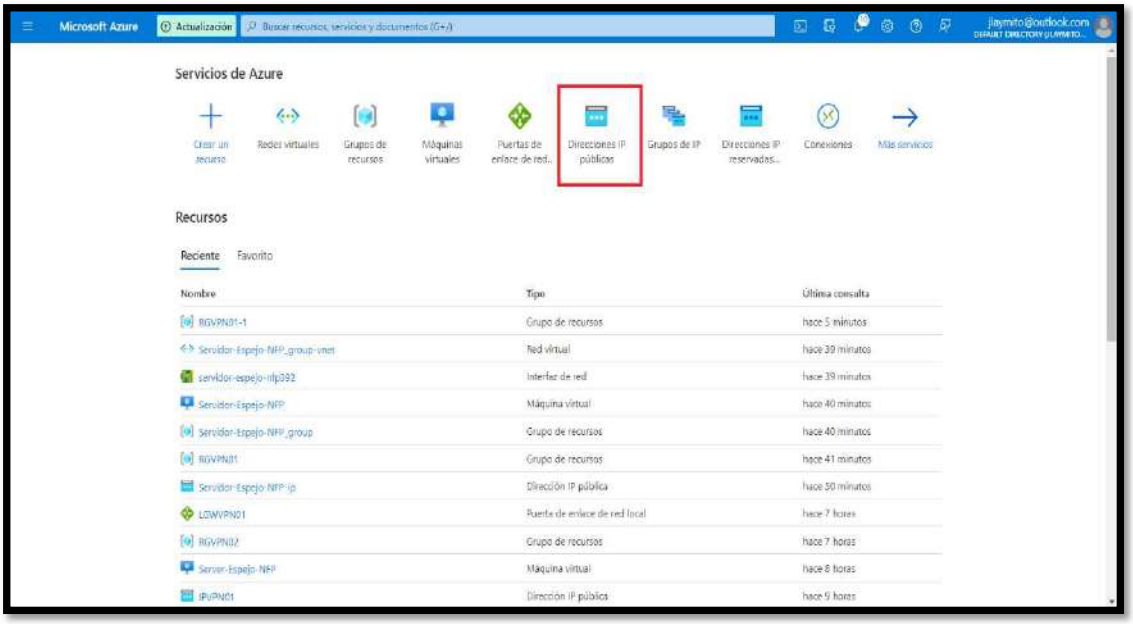
- Clic en subred de puerta de enlace, se muestra un segmento diferente cambiar la máscara por una máscara que permita una red más pequeña. Clic en guardar.



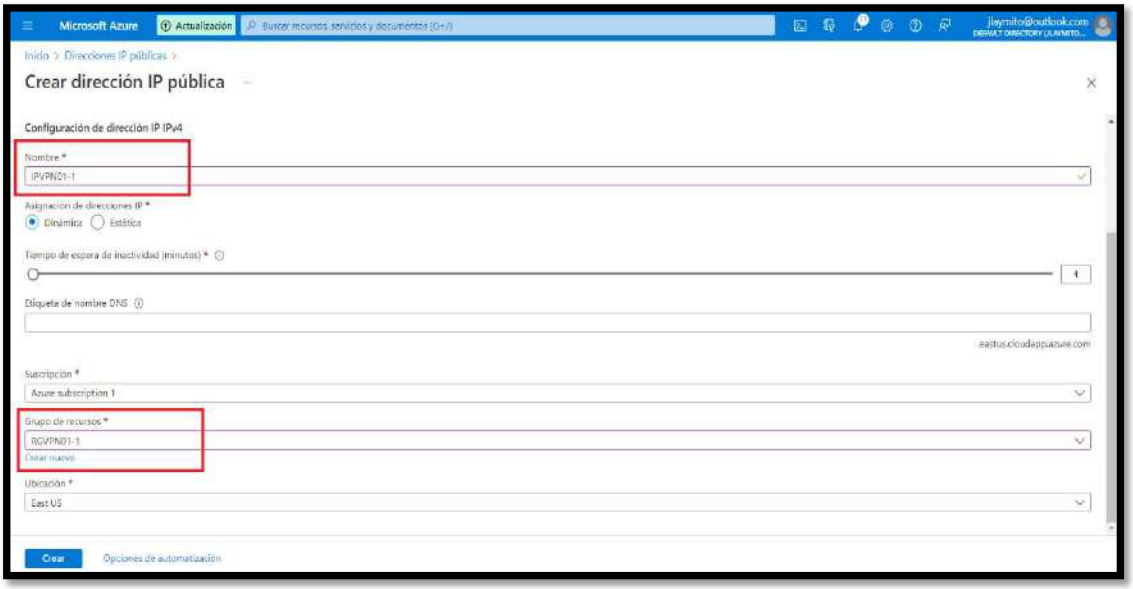
- Ya tenemos la subred para el vpn Gateway



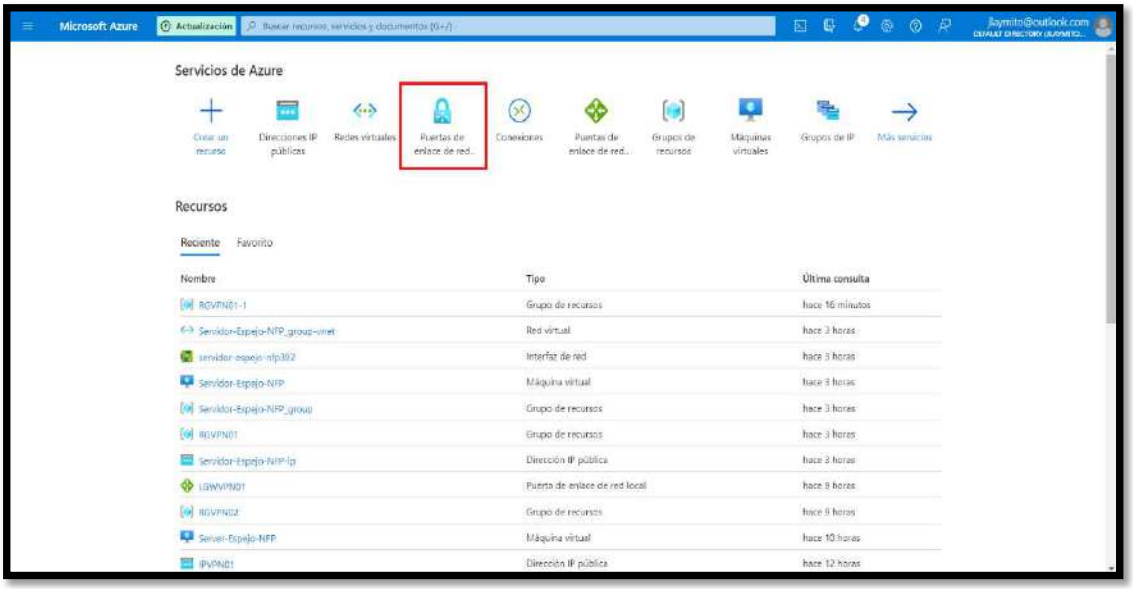
- Crear una ip publica que es la que utilizará el Gateway para establecer la conexión vpn



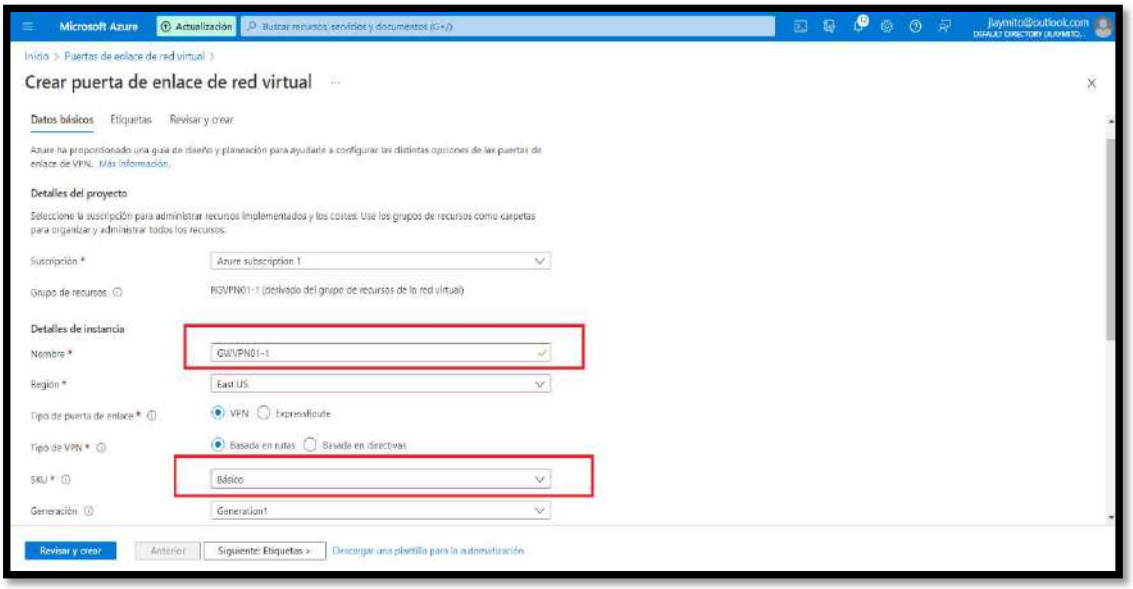
- Colocar un nombre y elegir el grupo de recursos. Luego clic en crear.



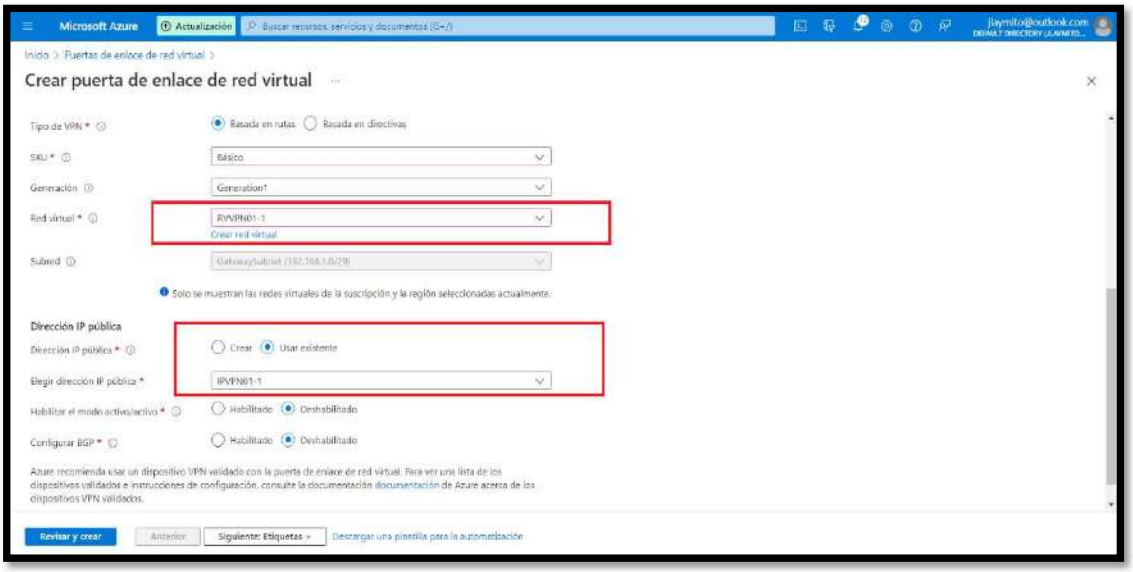
- Crear puerta de enlace de red o Gateway vpn



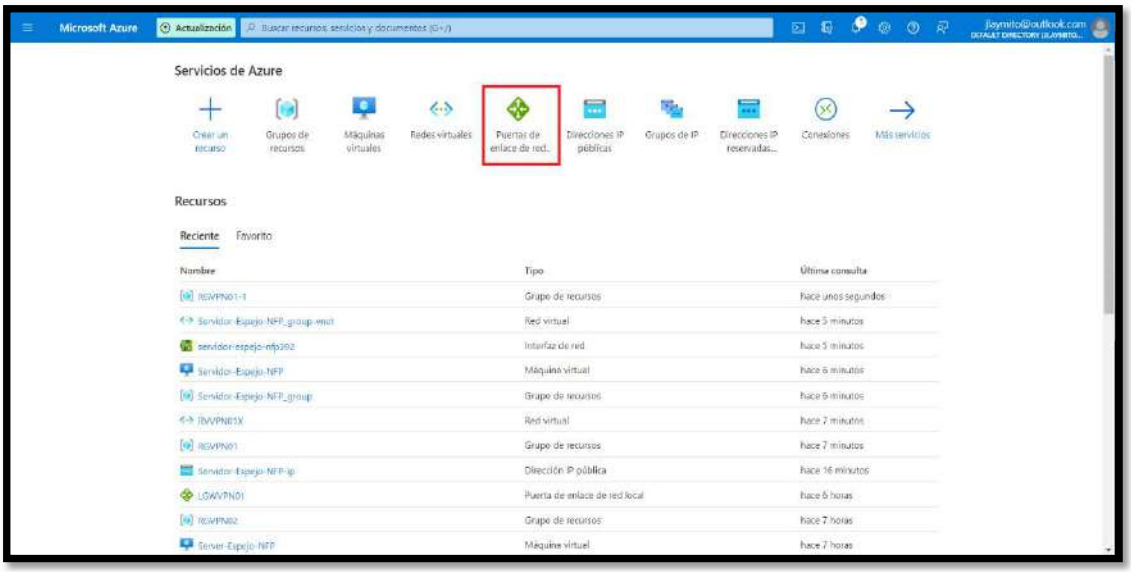
- Colocar un nombre, elegir sku básico.



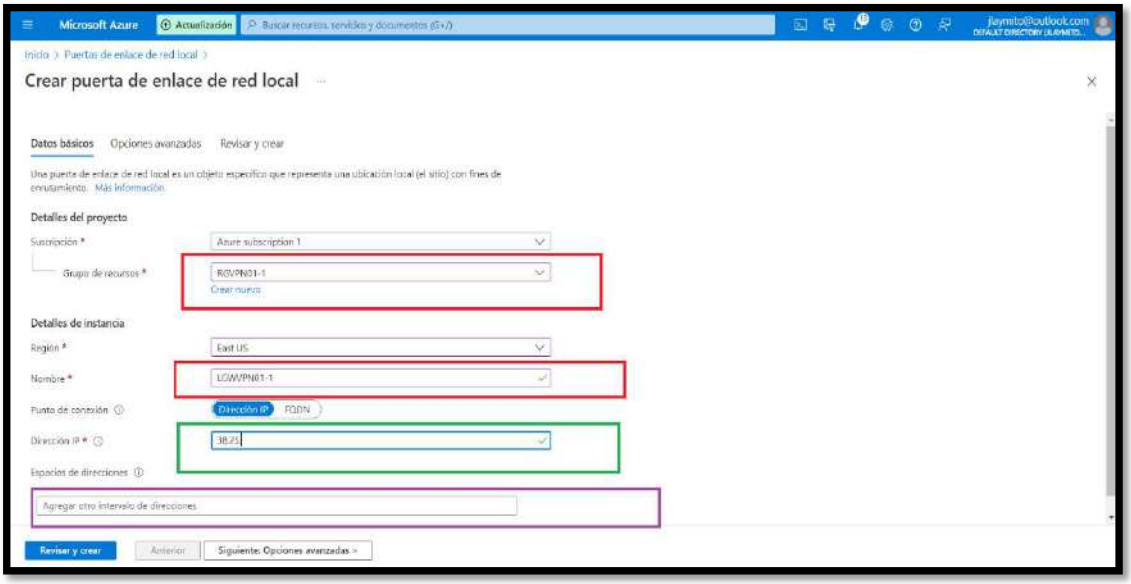
- Elegir la red virtual creada y la ip pública creada. Luego clic en revisar y crear. Este proceso de guardado dura aprox. 30 minutos.



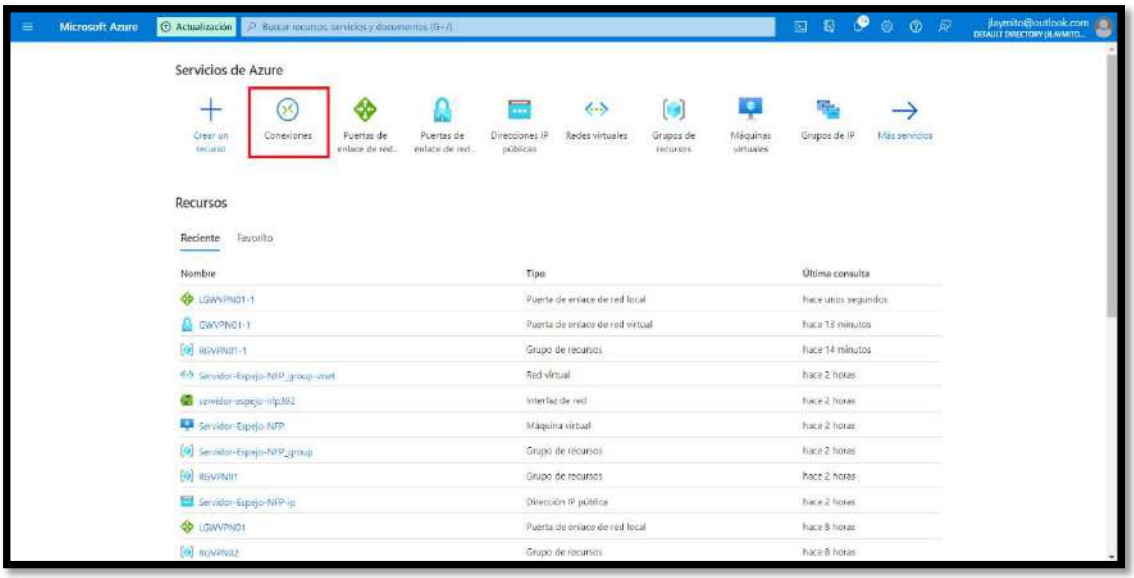
- Crear el Gateway de la red local. Esto es un objeto que identifica el dispositivo que hará de terminador vpn en nuestra casa



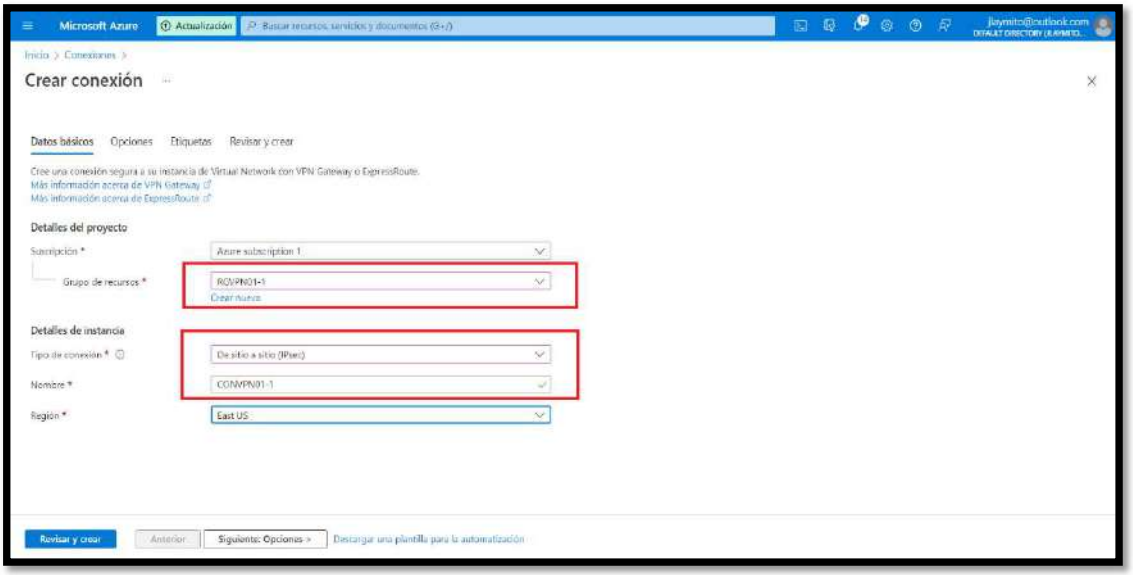
- Colocar las configuraciones, en el cuadro verde colocar la ip pública del router (este dato se obtiene buscando en la web “cuál es mi ip pública”). En el cuadro morado colocar la ip local de la casa. Luego clic en revisar y crear.



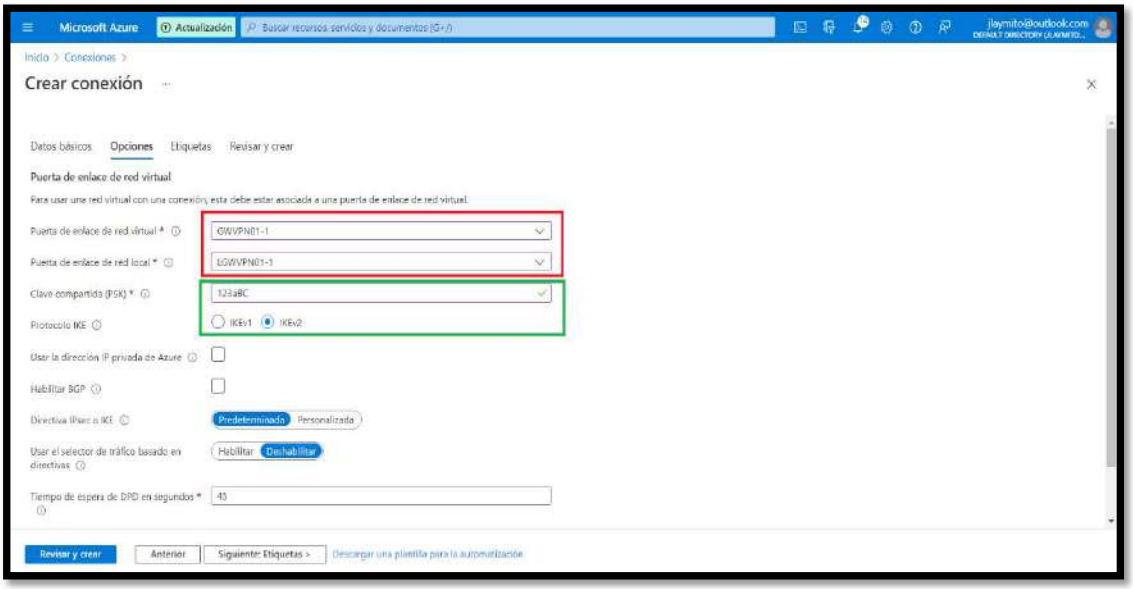
- Ahora se agrega la conexión, es un elemento que identifica cual es el origen cual es el destino y que tipo de comunicación existirá entre esos dos extremos.



- Colocar la siguiente configuración. Luego clic en revisar y crear.

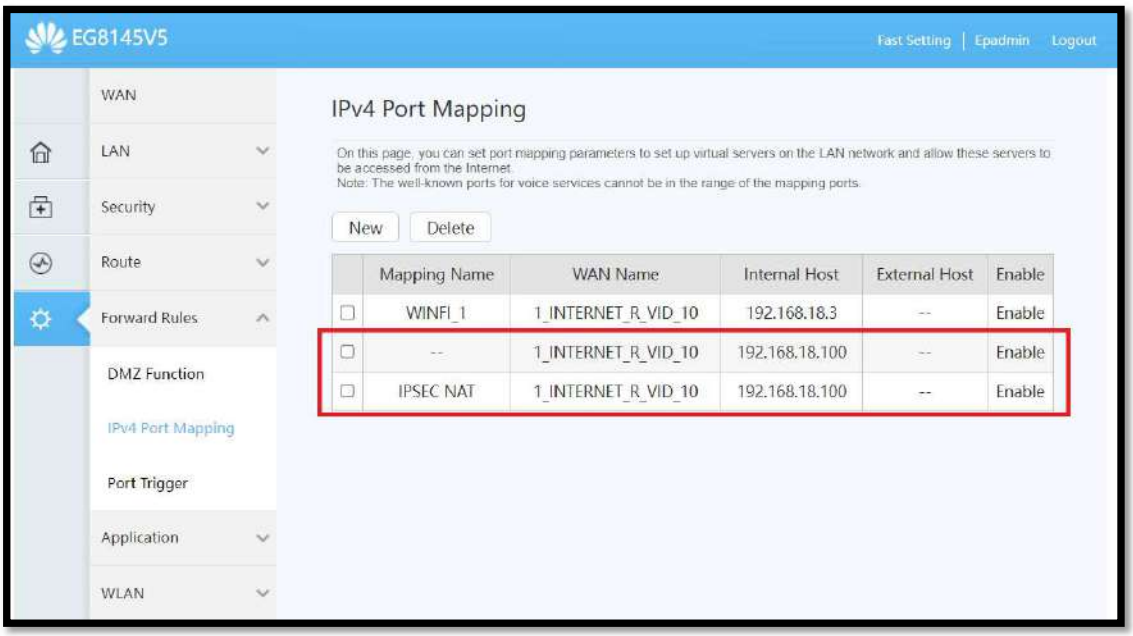


- Colocar las configuraciones indicadas. En el cuadro verde colocar una contraseña que se usa en el extremo local para que se pueda crear el túnel vpn. Luego clic en revisar y crear.

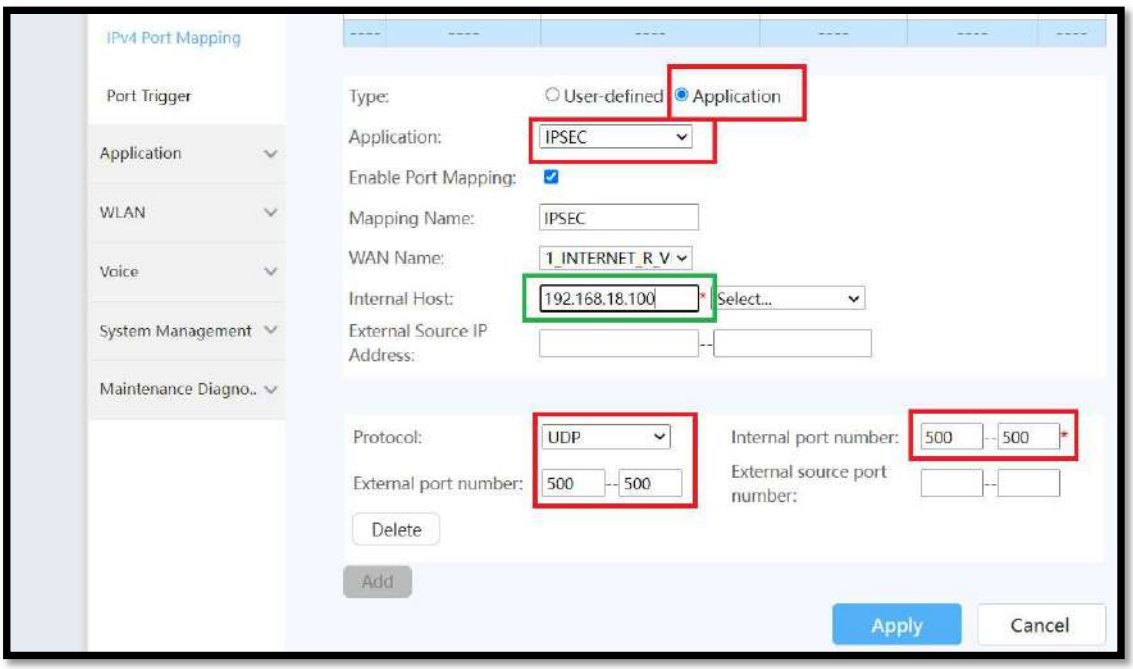


Paso 7: configuración del router de new fashion (Redirección de puertos)

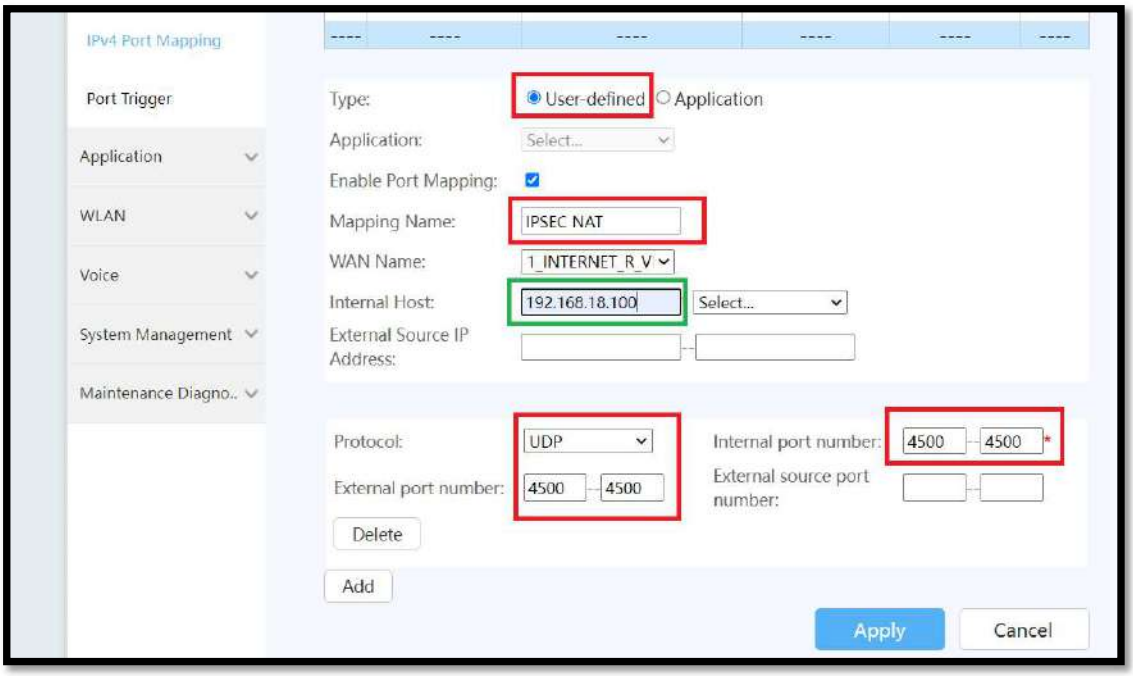
- Ingresar al router e ir a la siguiente configuración donde se agregarán dos puertos al router



- Agregar el puerto **ipsec** con number port **500**. Colocar las configuraciones según indica la imagen, en el cuadro verde colocar la dirección ip del servidor principal.

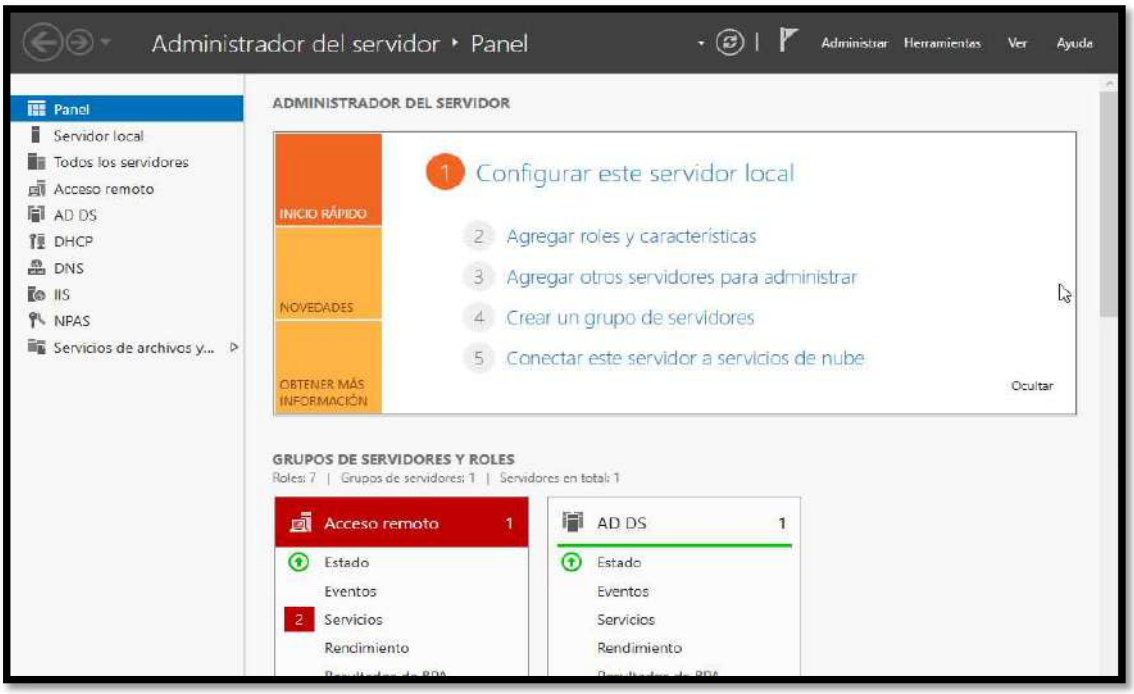


- Agregar el puerto **ipsec nat** con number port **4500**. Colocar las configuraciones según indica la imagen, en el cuadro verde colocar la direccion ip del servidor principal.

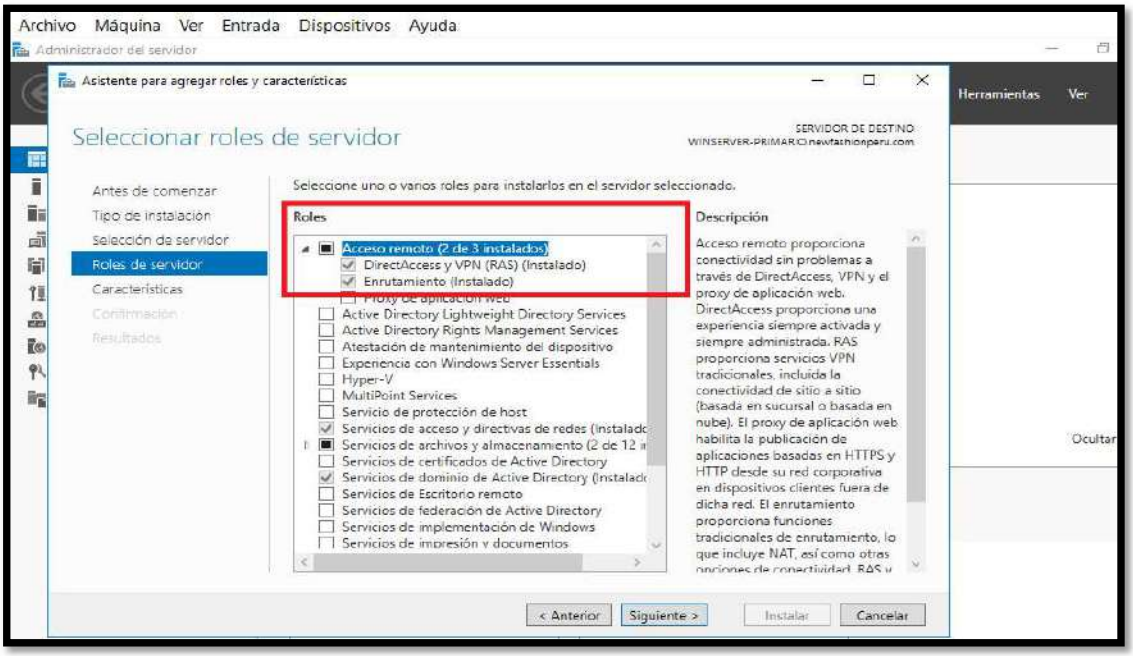


Paso 8: configuración en el servidor principal-Acceso Remoto

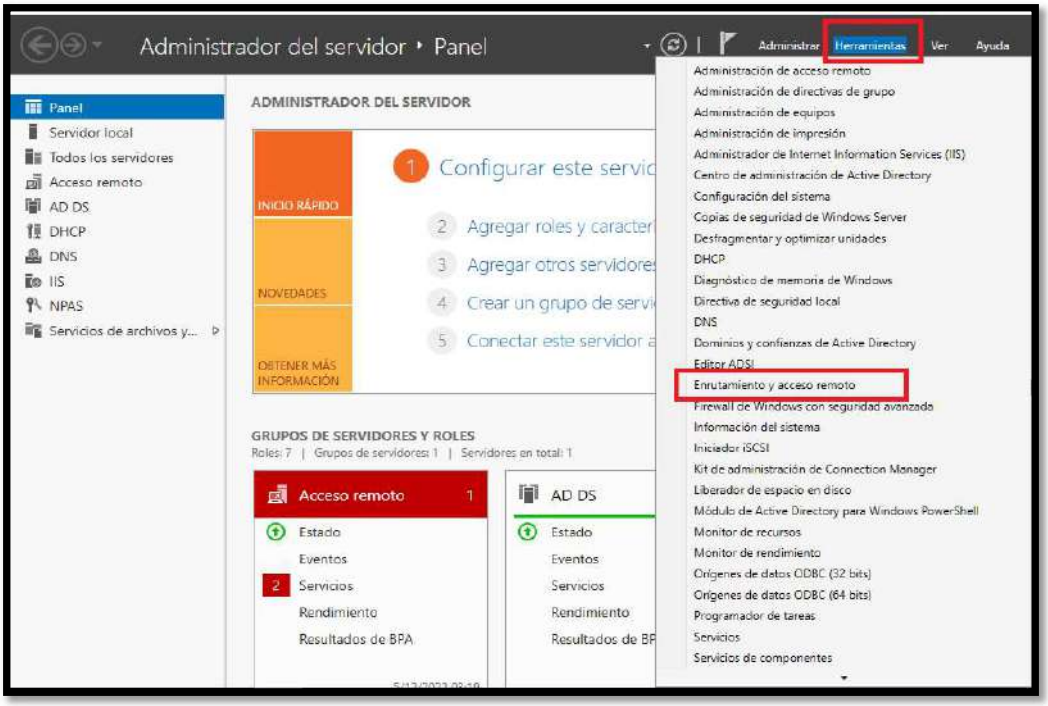
- Creación del rras (routing and remote access service)



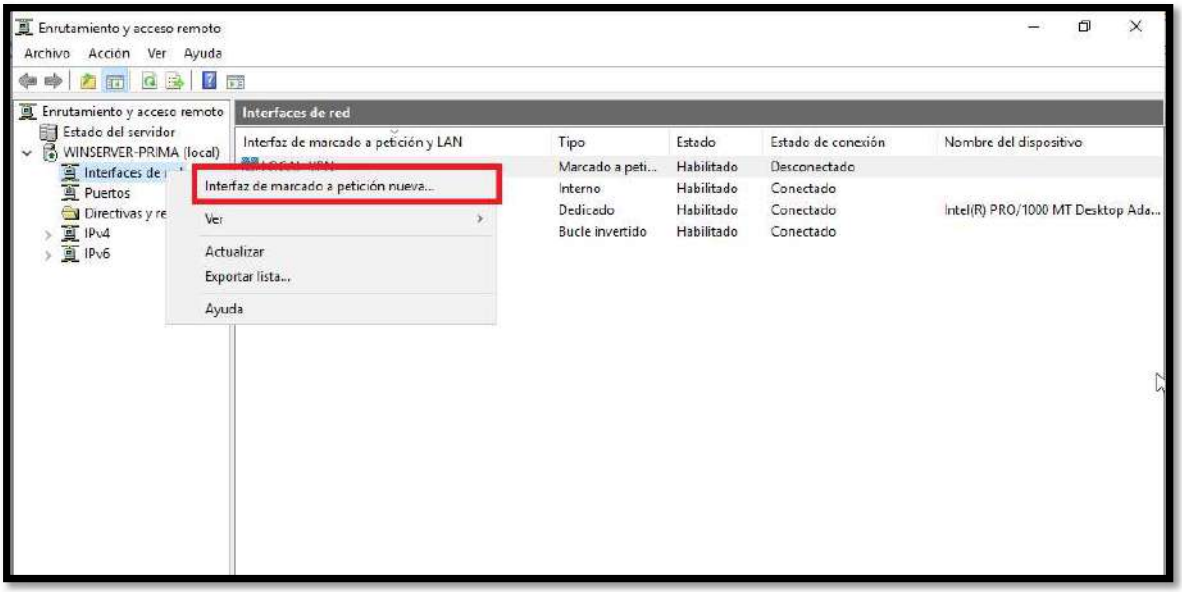
- Clic en agregar roles y características



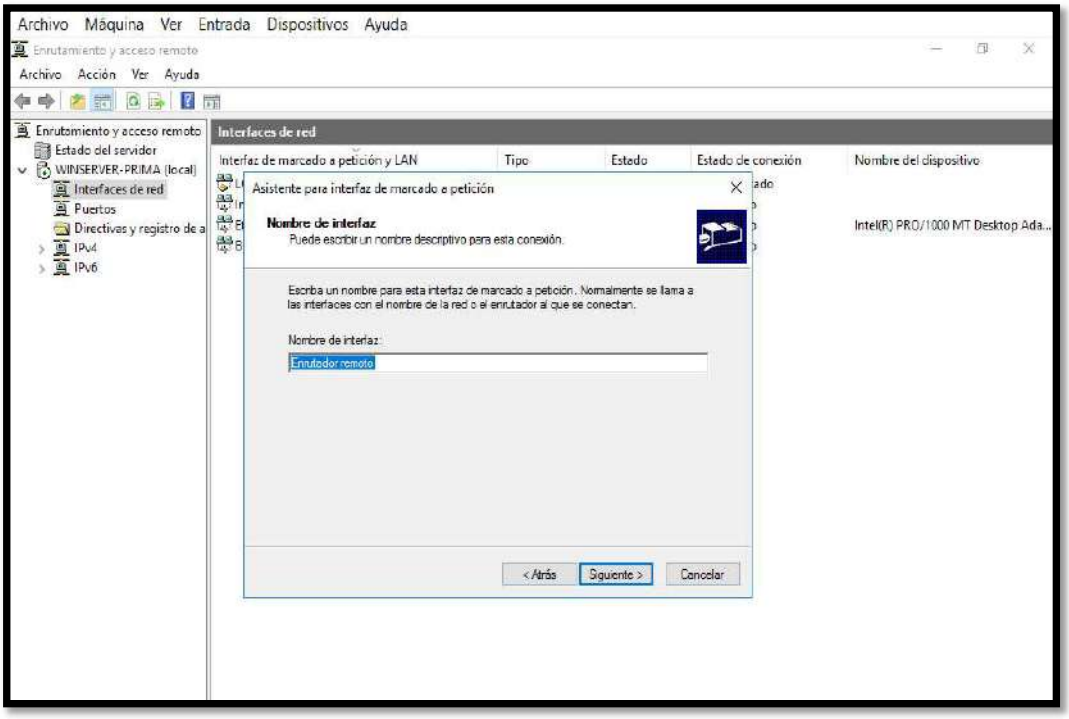
- Dar clic en roles y seleccionar lo marcado, siguiente para instalar.



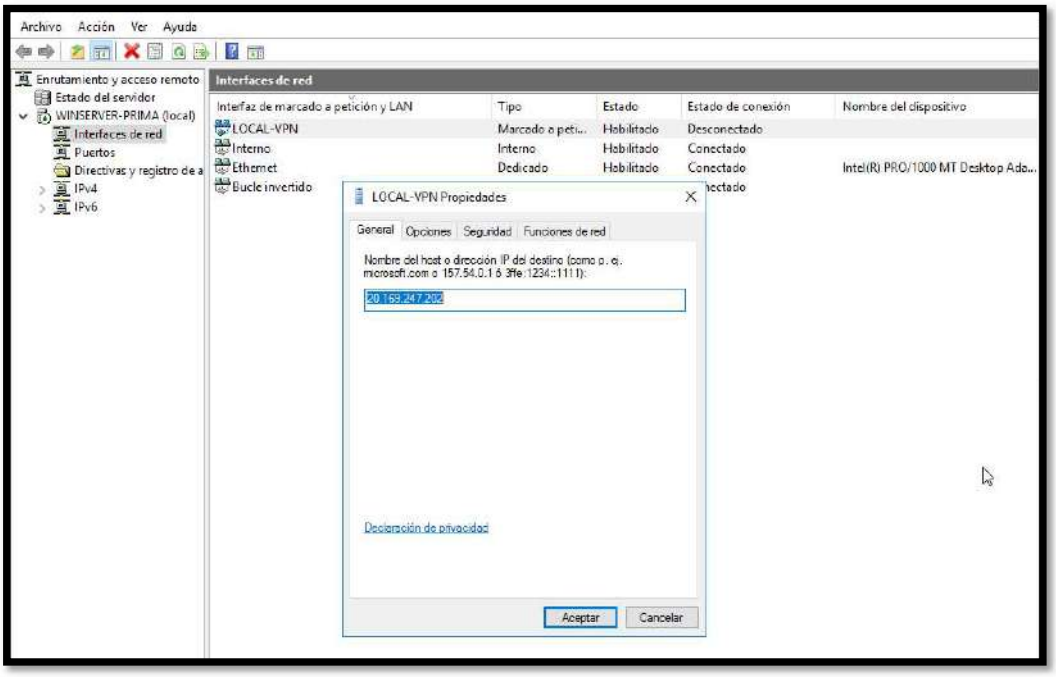
- Ingresar a lo resaltado en rojo para la configuración.



- Botón derecho en interfaces de red y clic en interfaz de marcado
- Clic en siguiente, luego pedirá un nombre colocar por ej. Local vpn



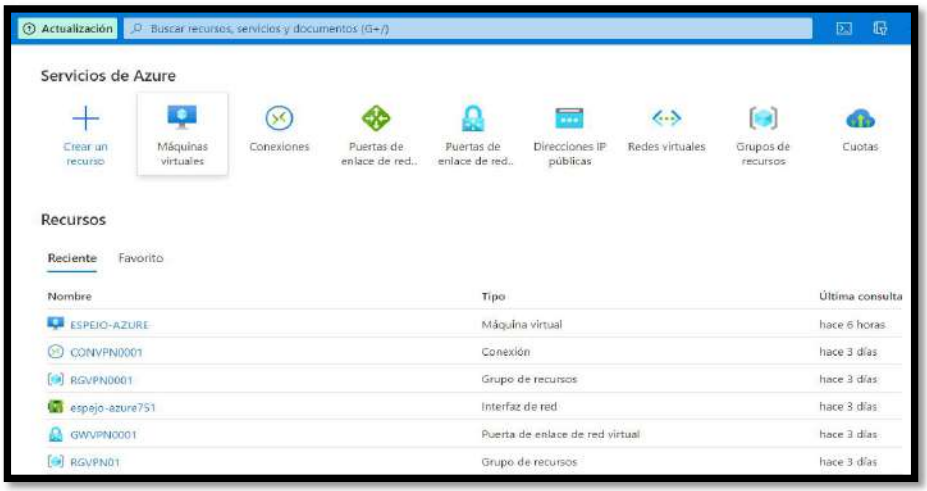
- En general colocar el ip público de la mv de azure y en la pestaña seguridad colocar el ikev2 con la clave que se configuró en el azure



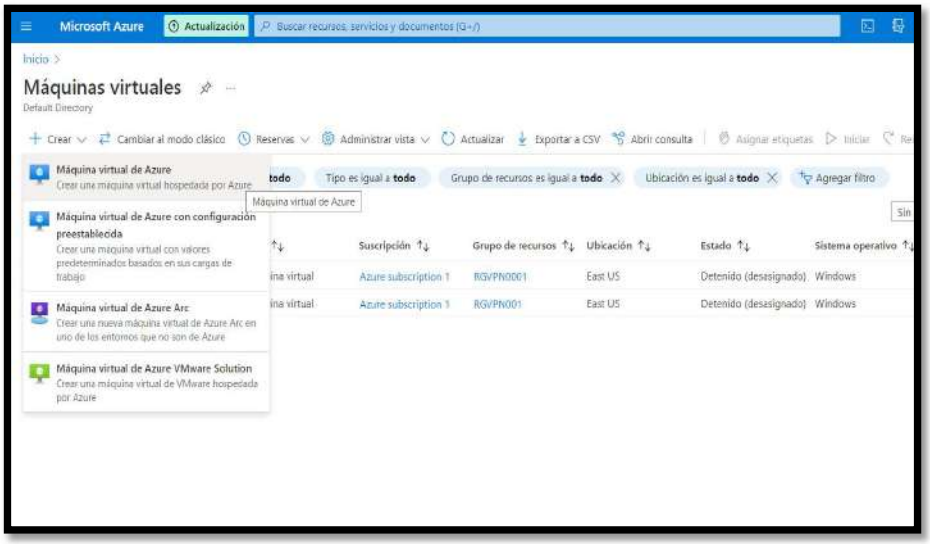
.

PASO 9: CONFIGURACIÒN DE LA MAQUINA VIRTUAL EN LA NUBE

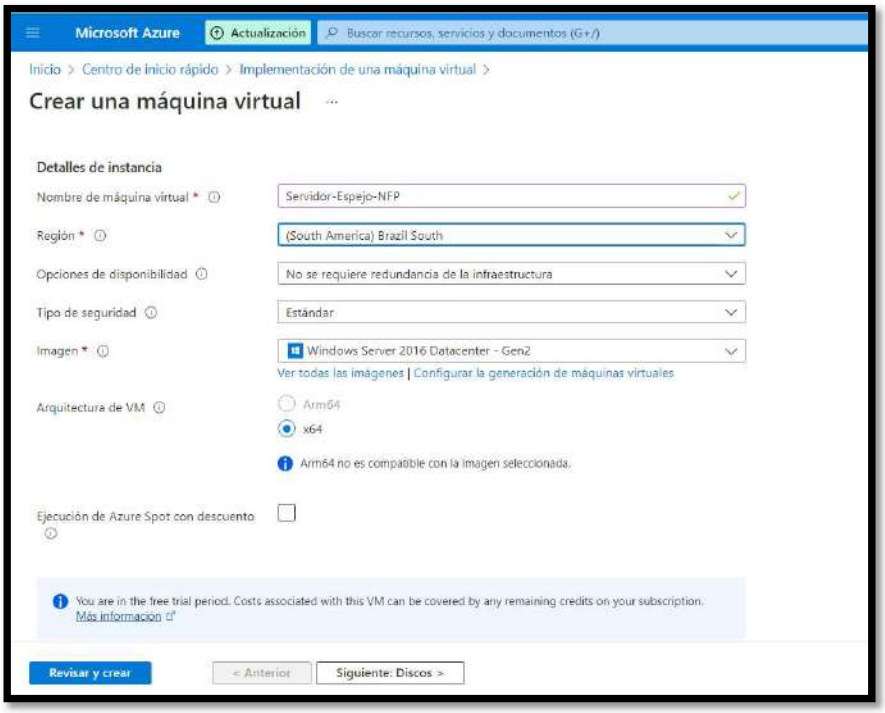
- Clic en Máquinas Virtuales



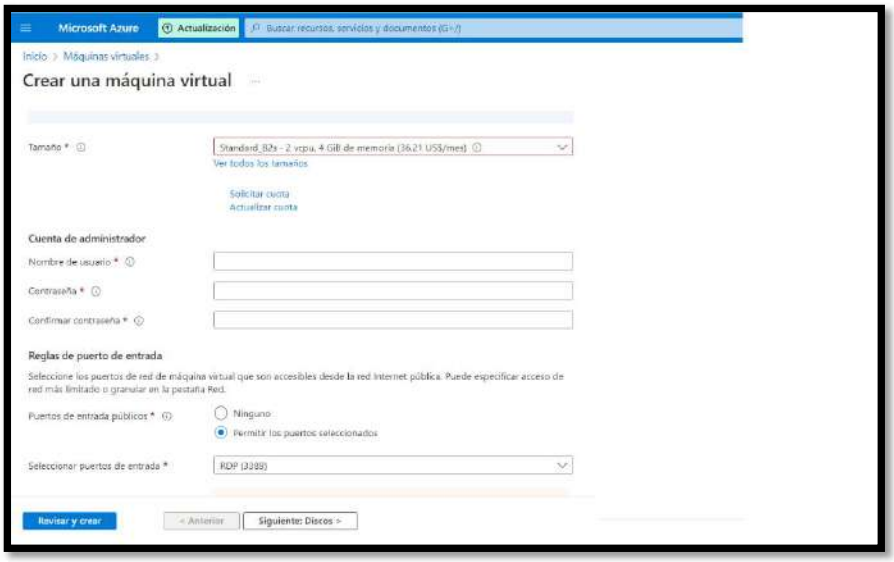
- Clic en Máquina Virtual de Azure



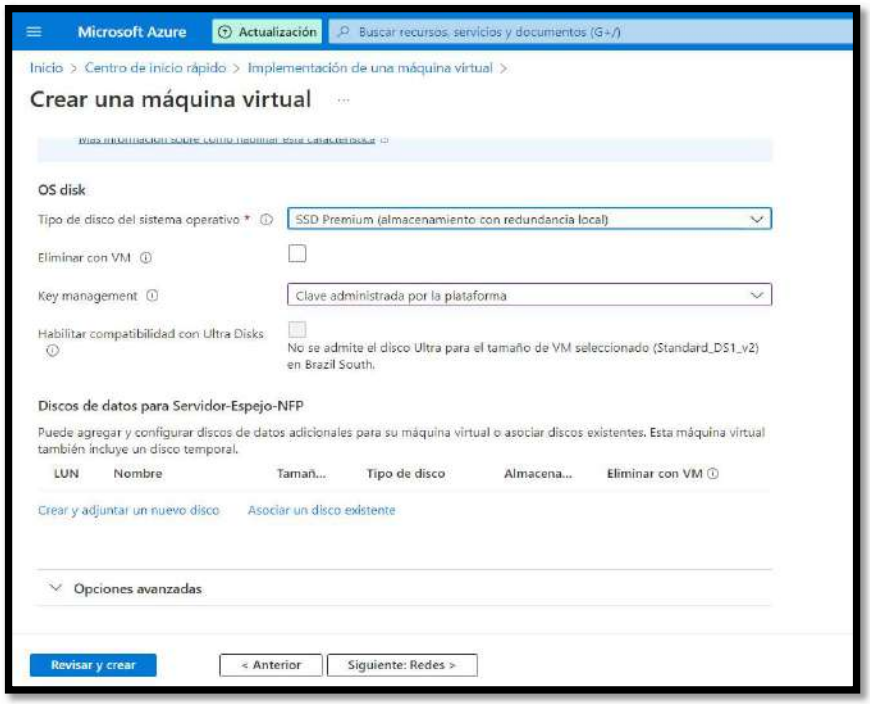
- Colocar un nombre a la MV, elegir la región y el Sistema Operativo



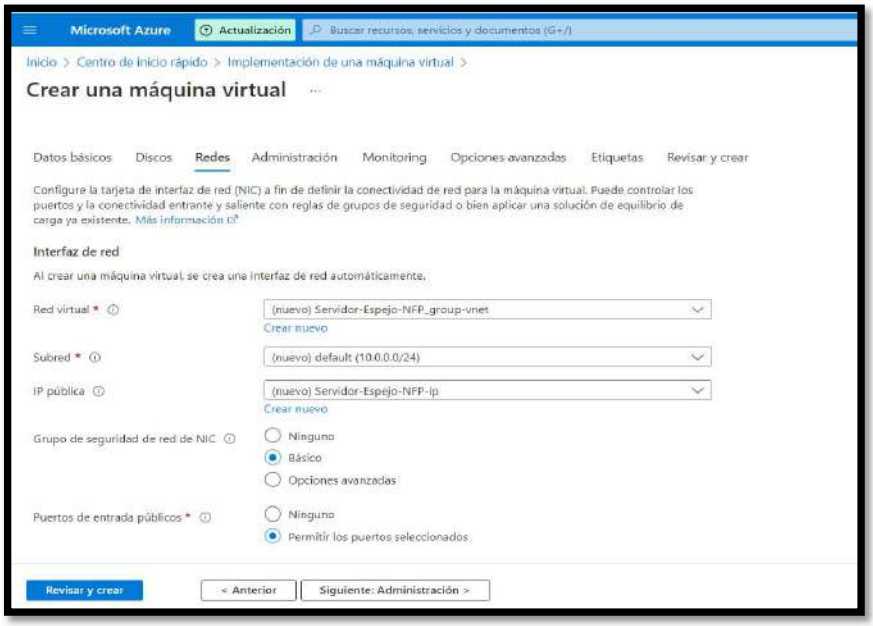
- Desplegar más abajo y elegir la cantidad de disco, memoria y cores, así como también el nombre y clave del Administrador



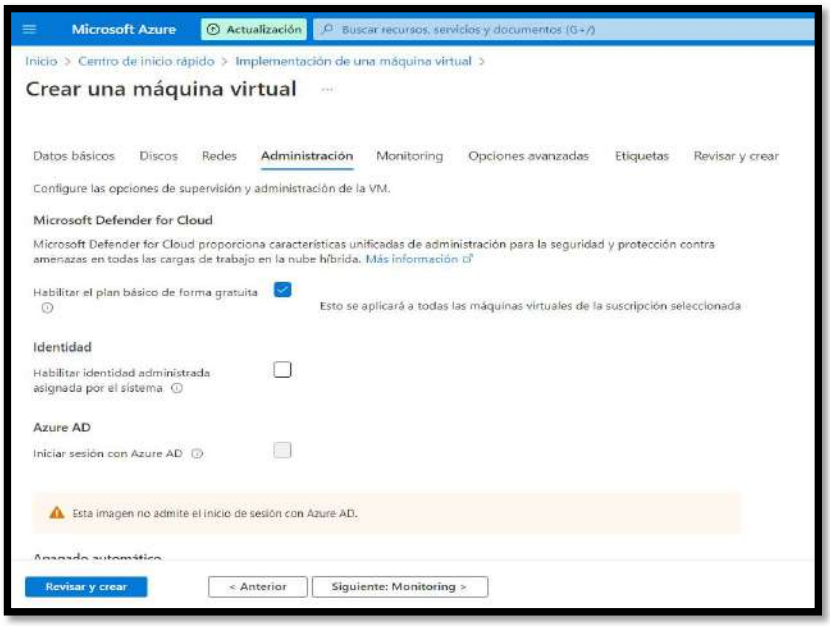
- Luego elegir el tipo de disco duro, clic en Siguiente Discos



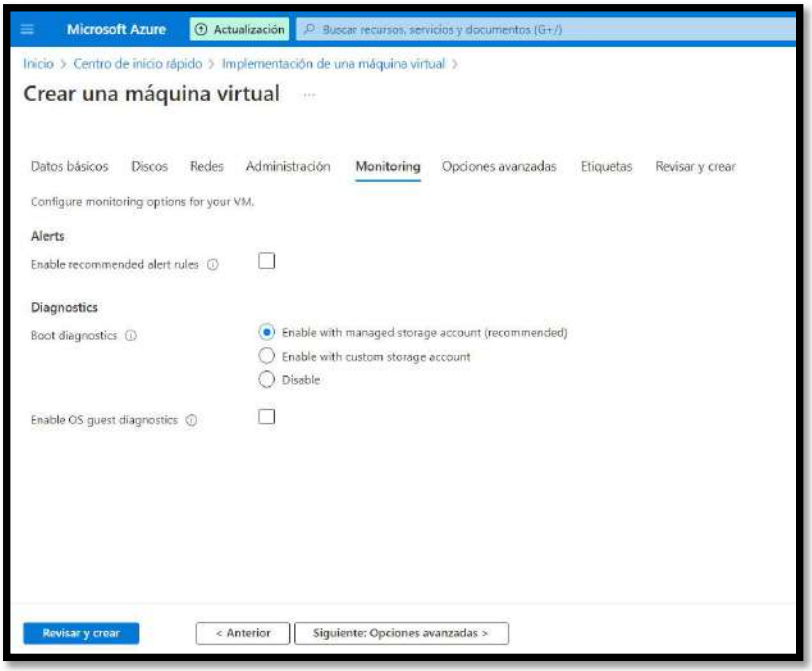
- Elegir las opciones configuradas en el VPN Site to Site y clic en Siguiente Administración



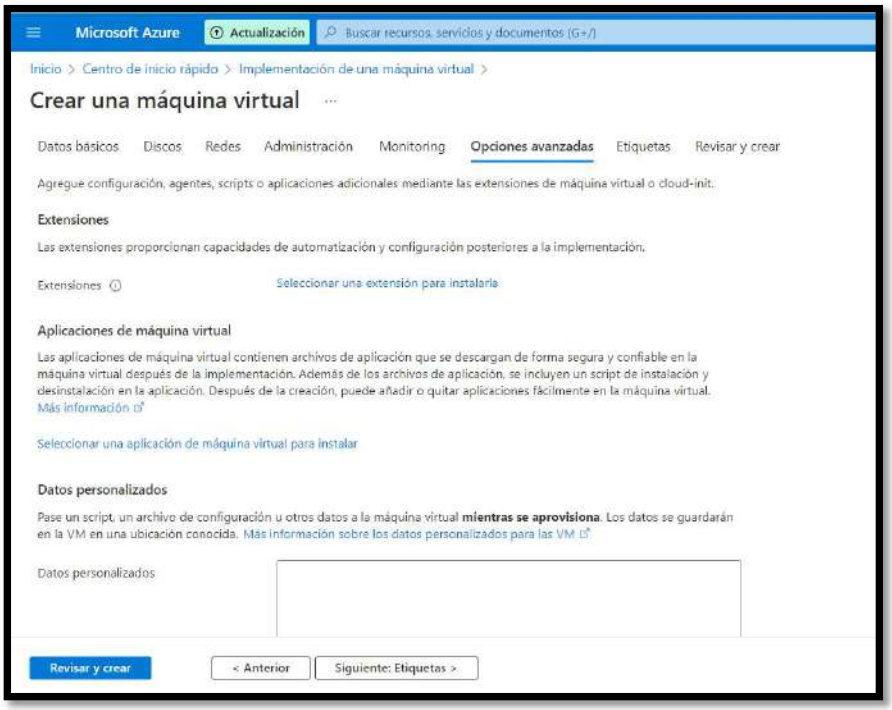
- Clic en Siguiente Monitoring



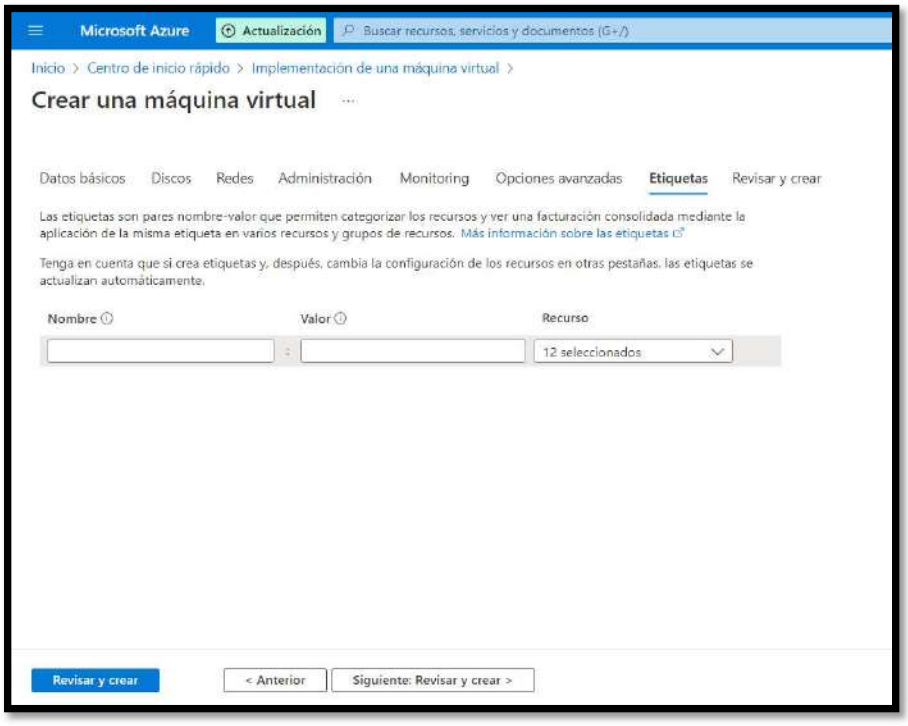
- Dejar igual, clic en Siguiente Opciones Avanzadas



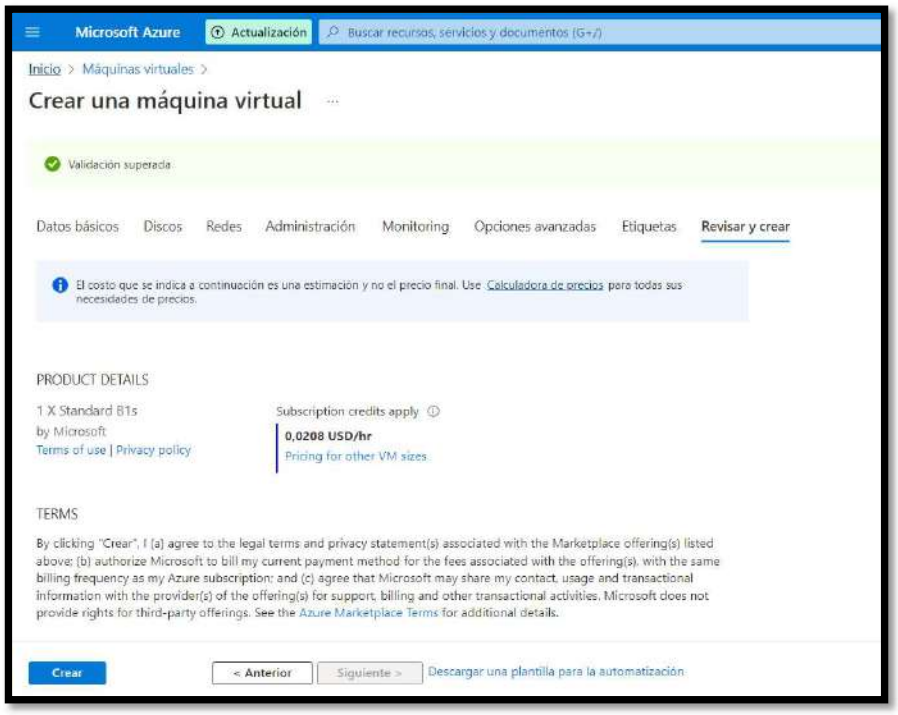
- Dejar tal cual, clic en Siguiente Etiquetas



- Clic en Revisar y Crear

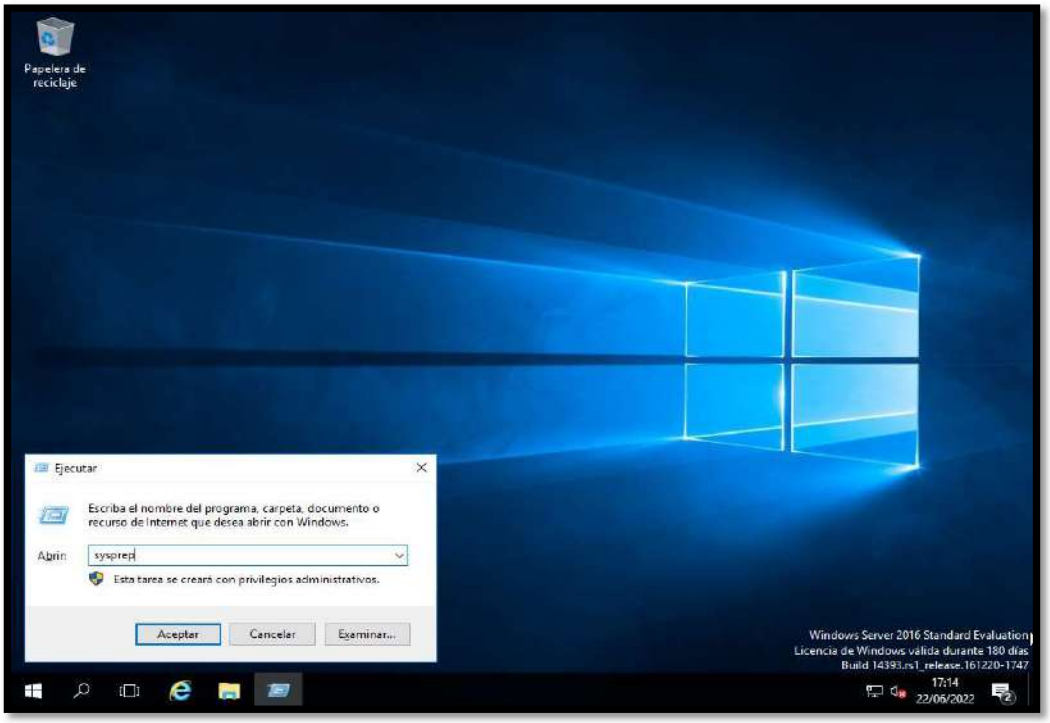


- Para finalizar el Azure te muestra el precio del uso de la MV por hora, de acuerdo a las opciones de disco, memoria y cores elegidos. Clic en Crear para crear la MV

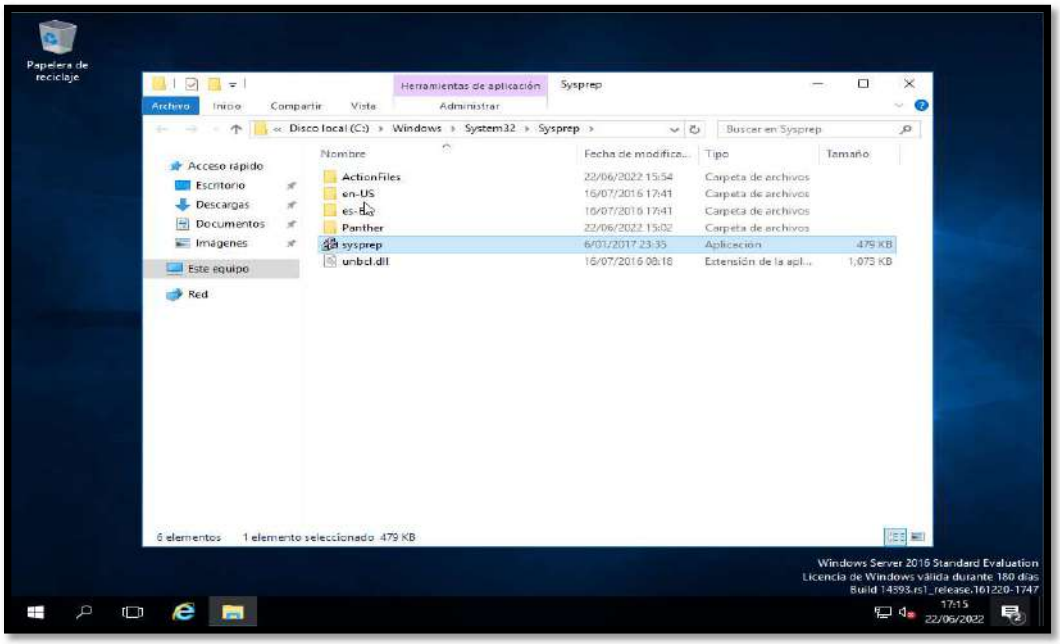


PASO 10 : EJECUCIÒN DEL EJECUTABLE OPEN SOURCE DEL WINDOWS “SYSPREP”

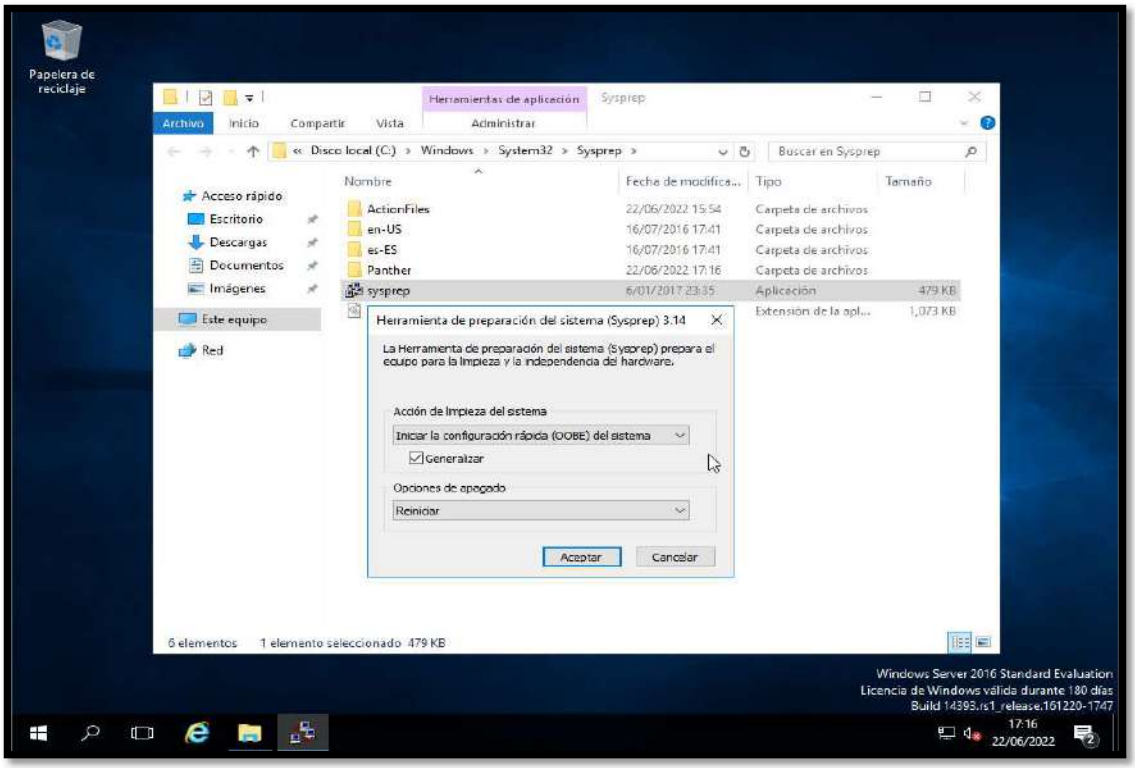
- Iniciar la MV del Azure y presionar las teclas Windows y R para abrir el Ejecutar, escribir Sysprep



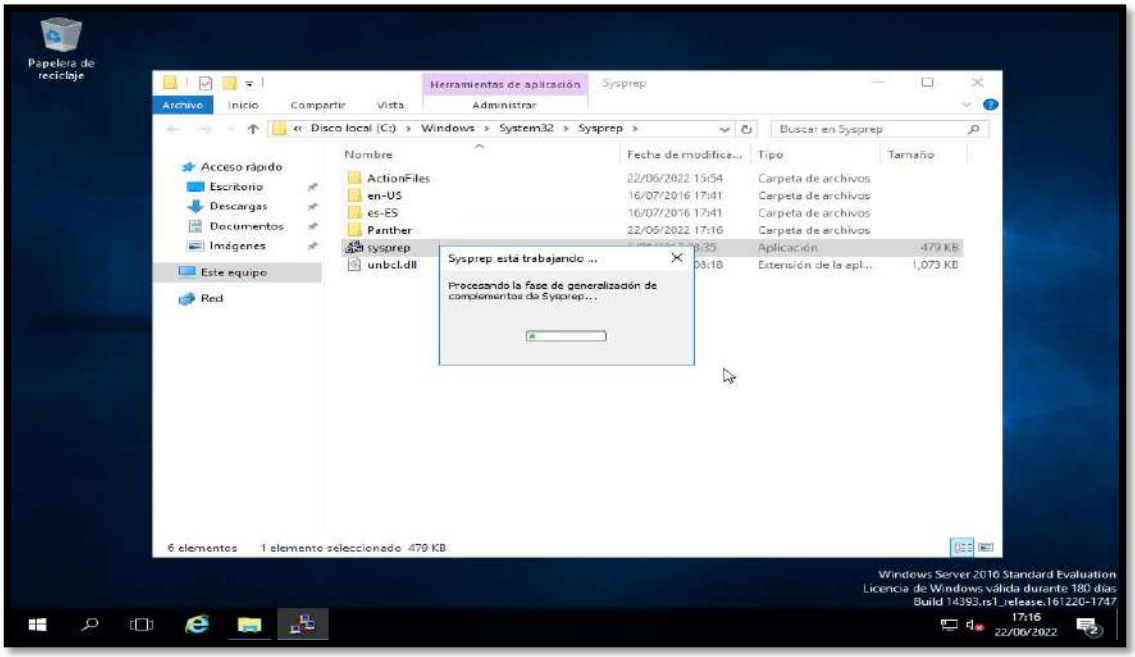
- Doble clic en Sysprep



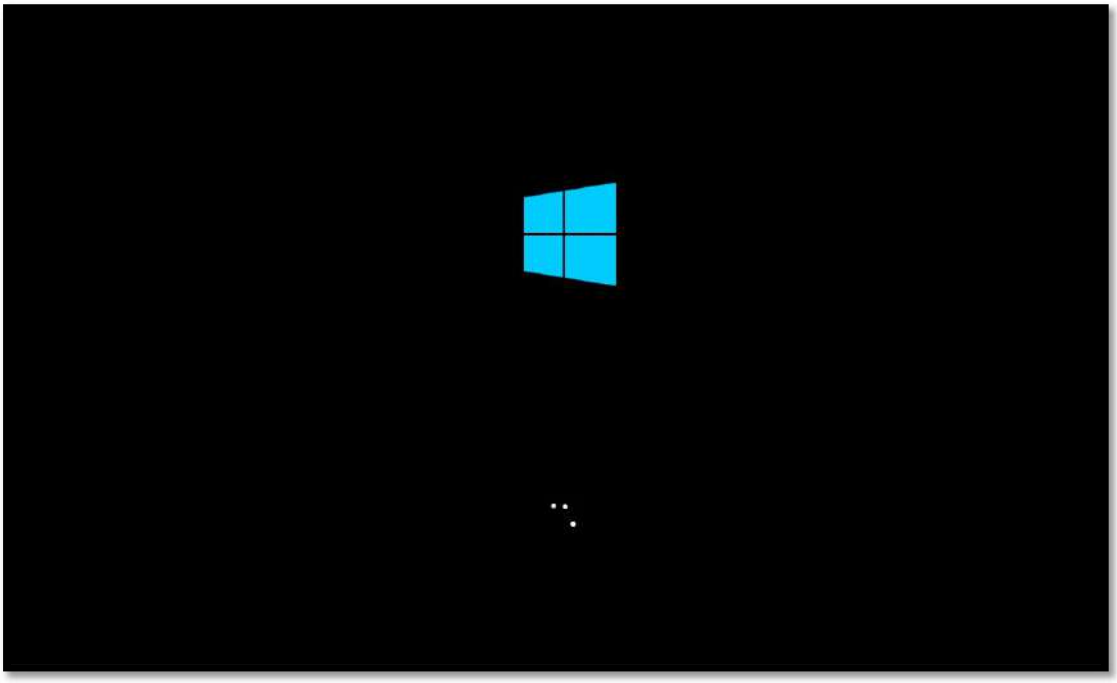
- Marcar la casilla de Generalizar y clic en Aceptar



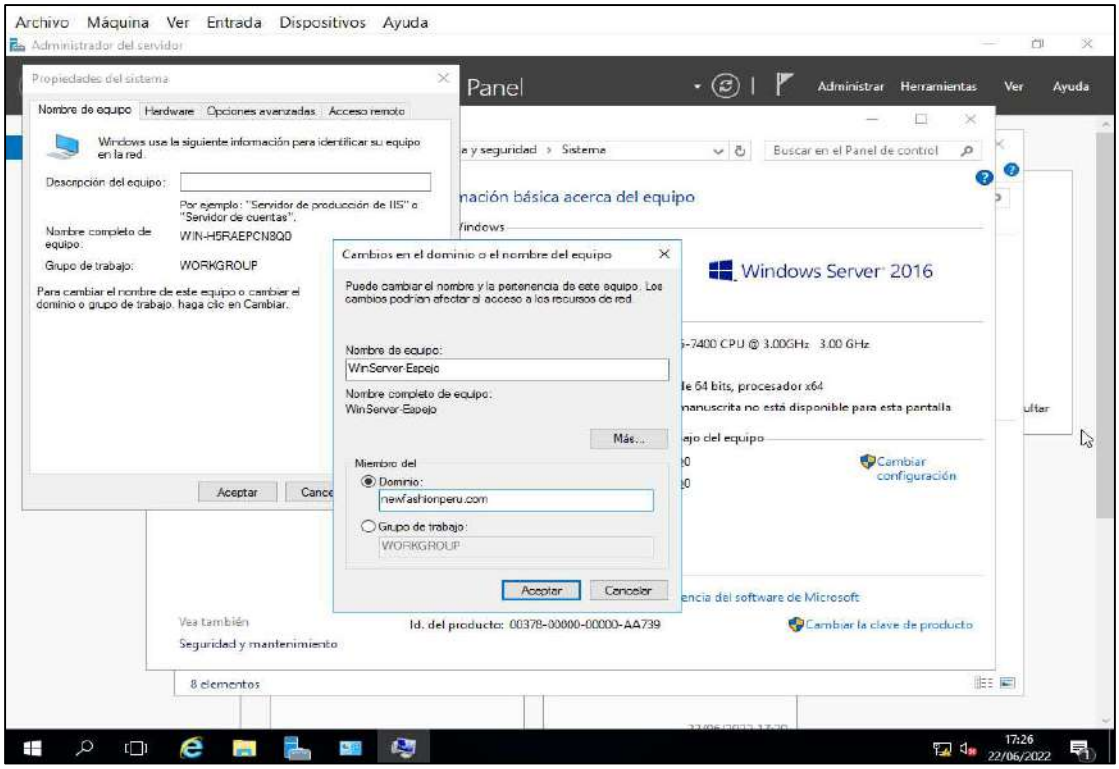
- Proceso de Instalación del software open source Sysprep



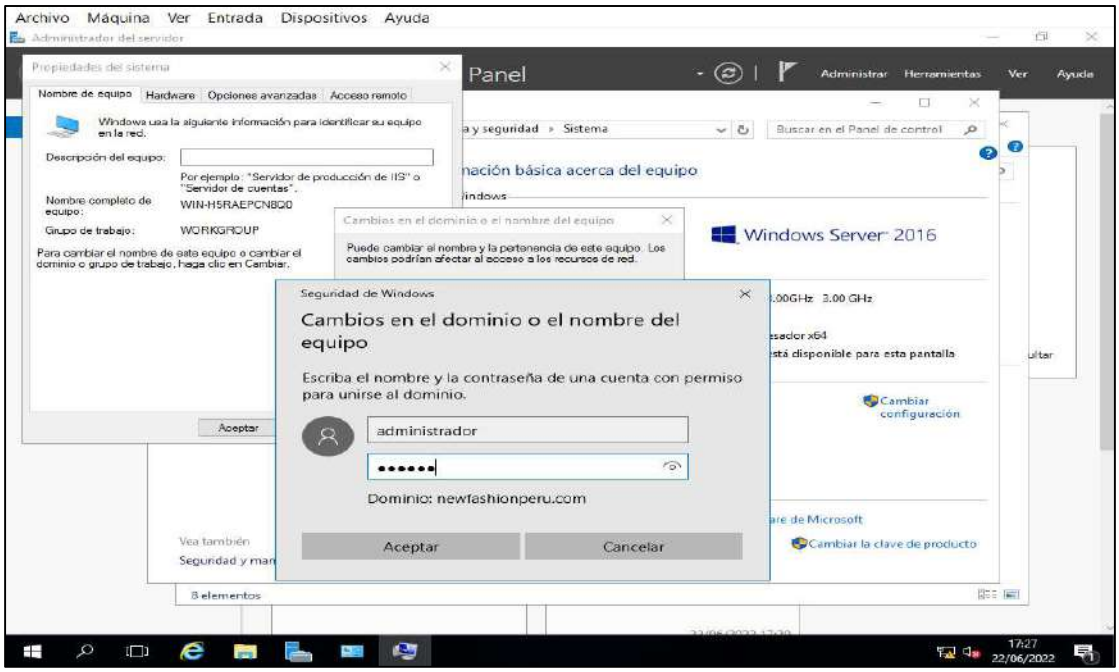
- Esperamos el proceso de instalación



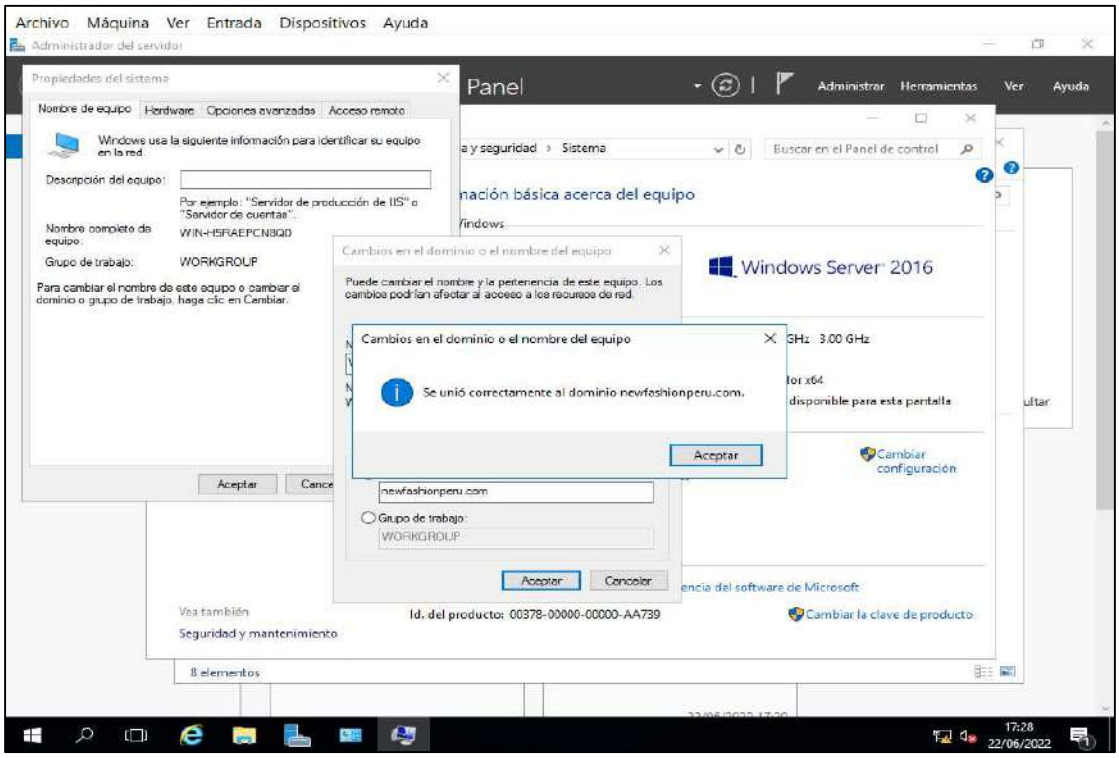
- Unir el Servidor Espejo al dominio principal



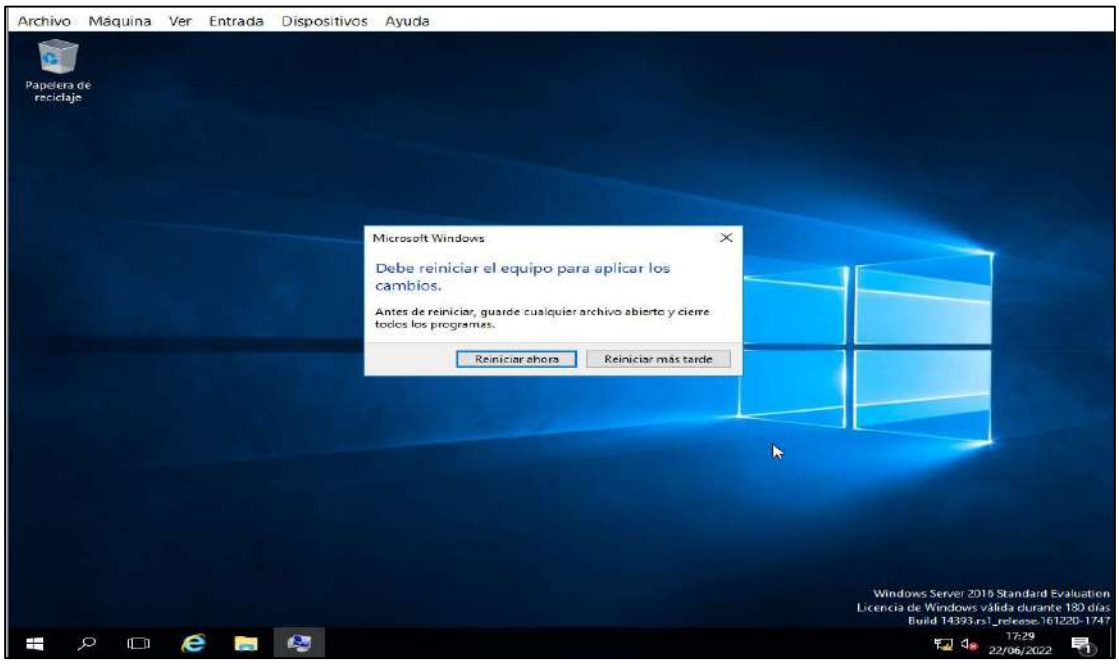
- Colocar las credenciales del Administrador del Servidor Principal



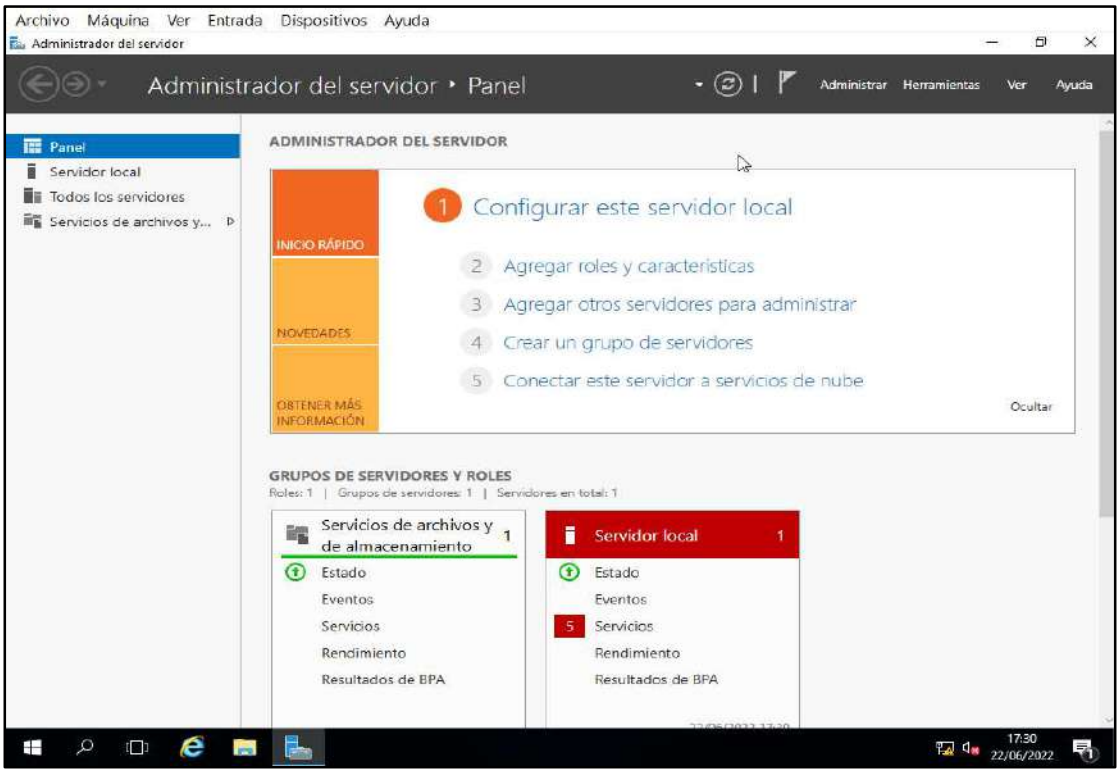
- Clic en Aceptar



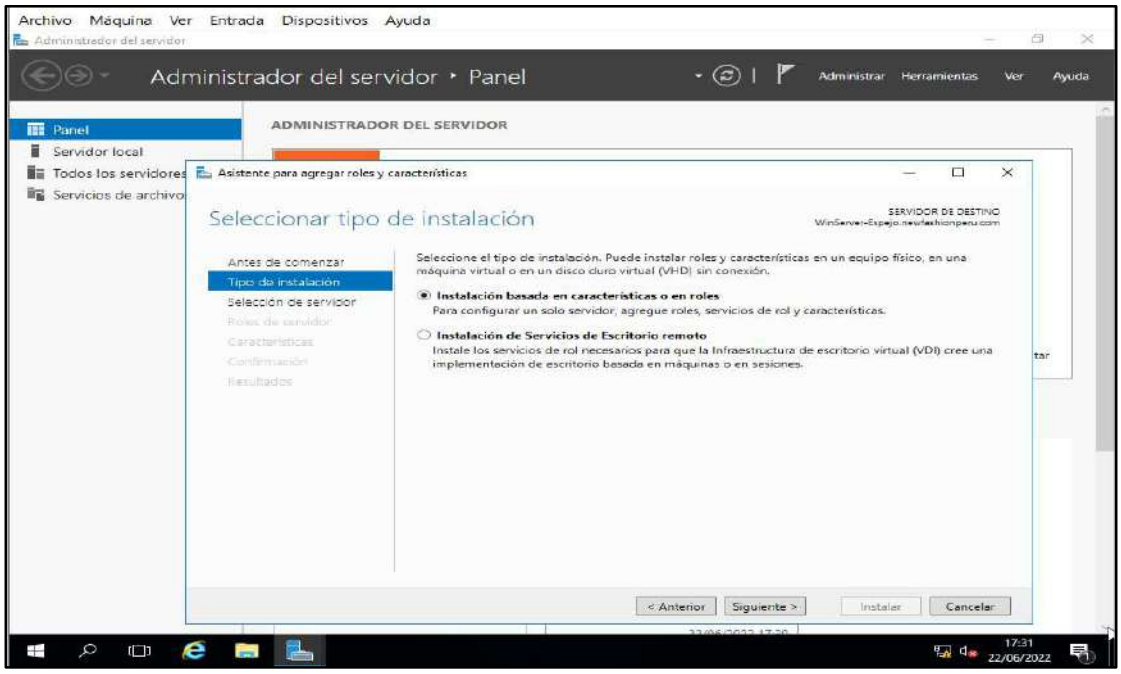
- Clic en Reiniciar ahora



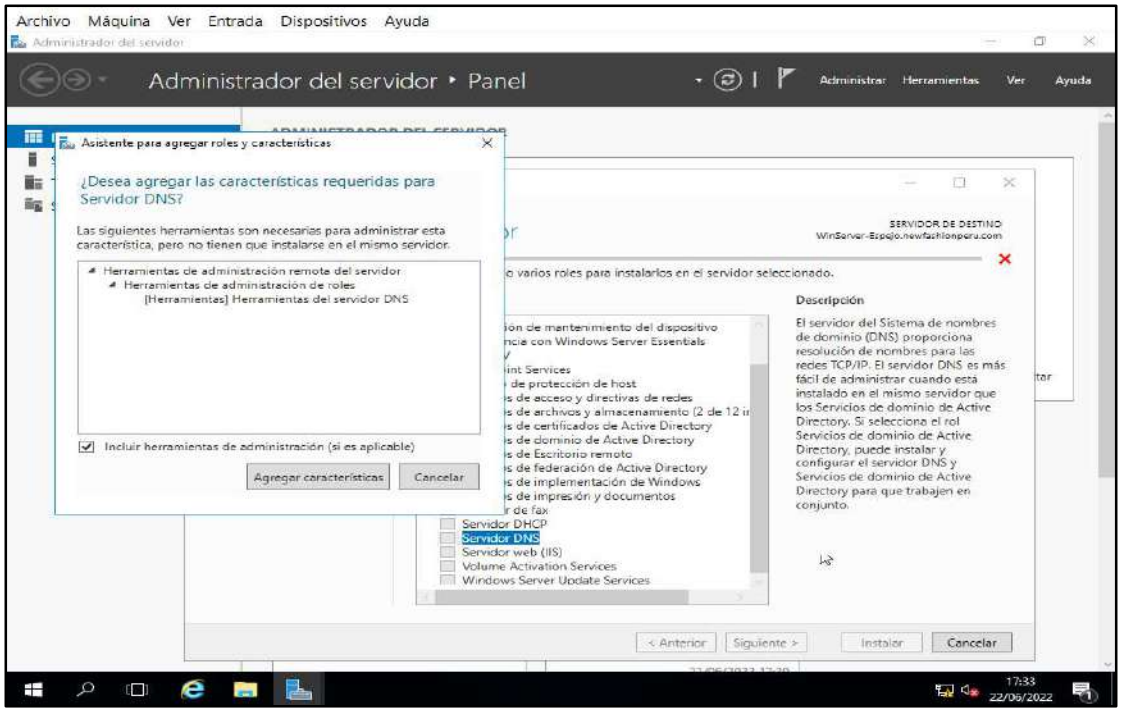
- Clic en agregar roles y características e instalar las mismas opciones del servidor principal



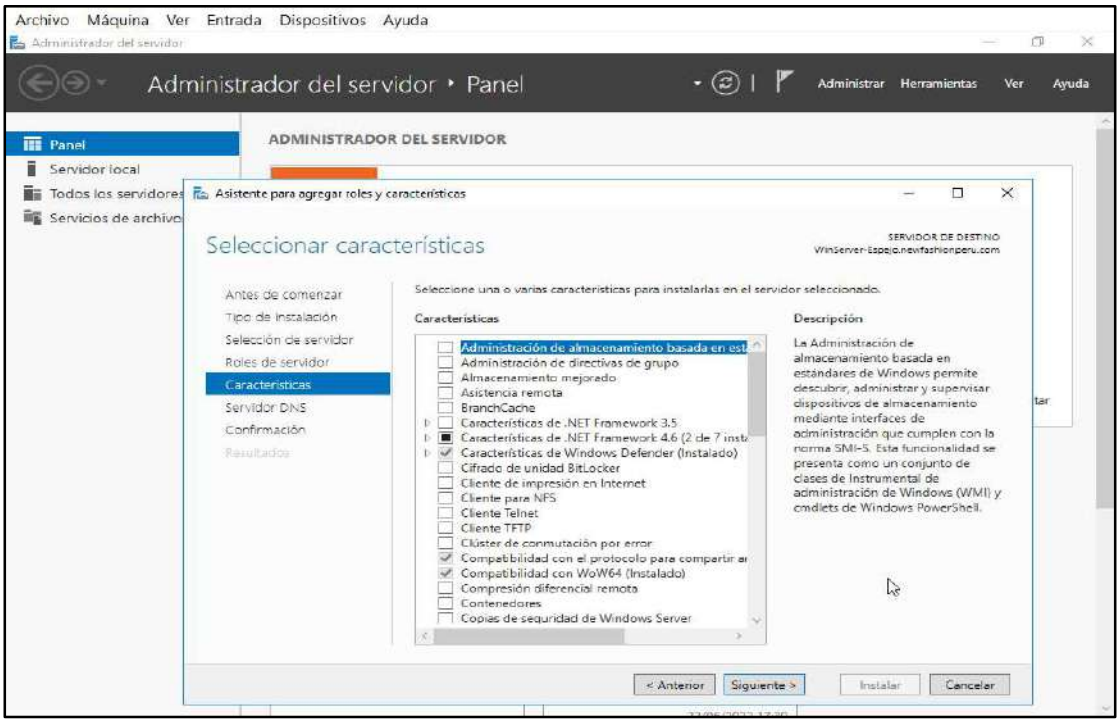
- Clic en Siguiente



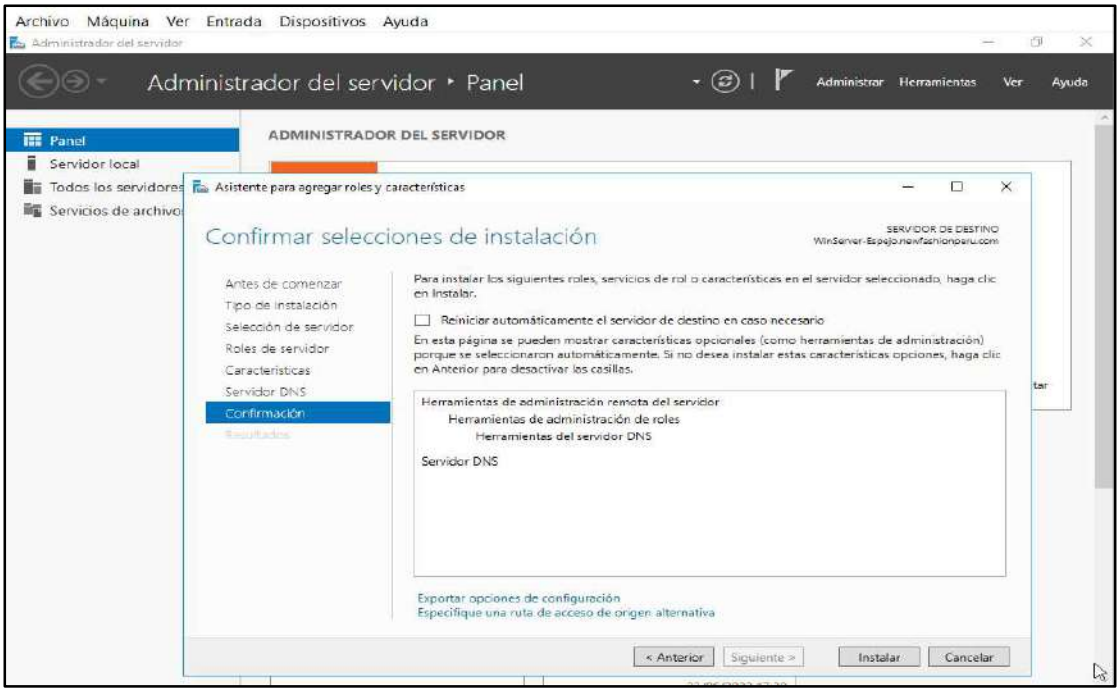
- Seleccionar Servidor DNS, clic en agregar características



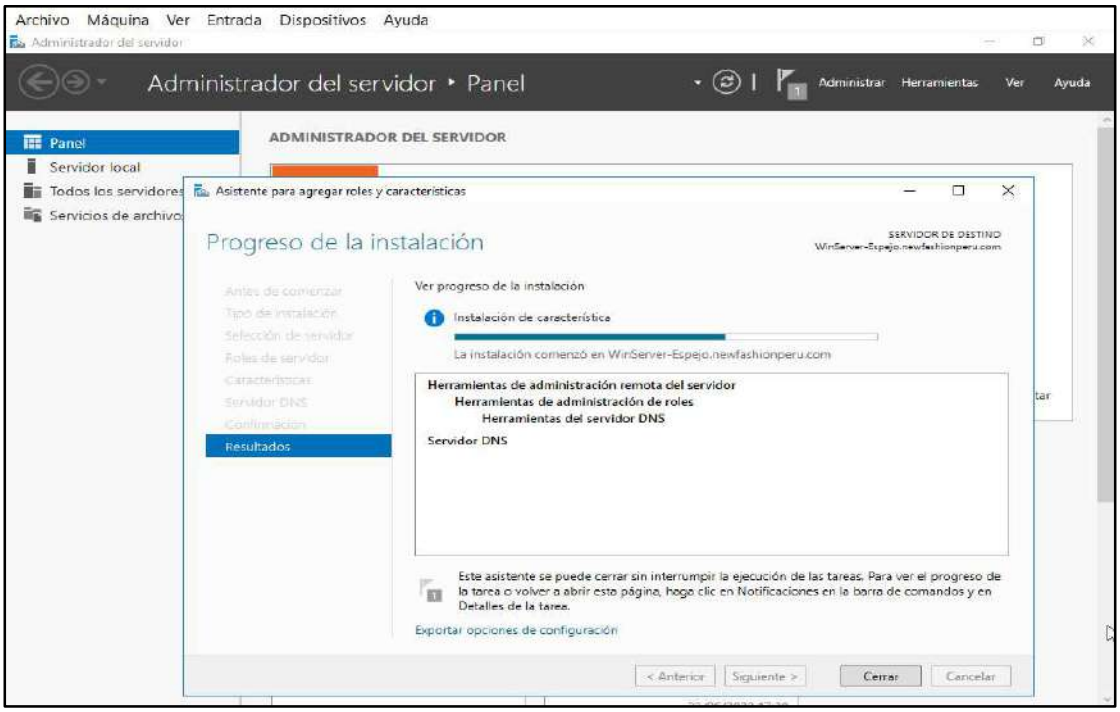
- Clic en siguiente



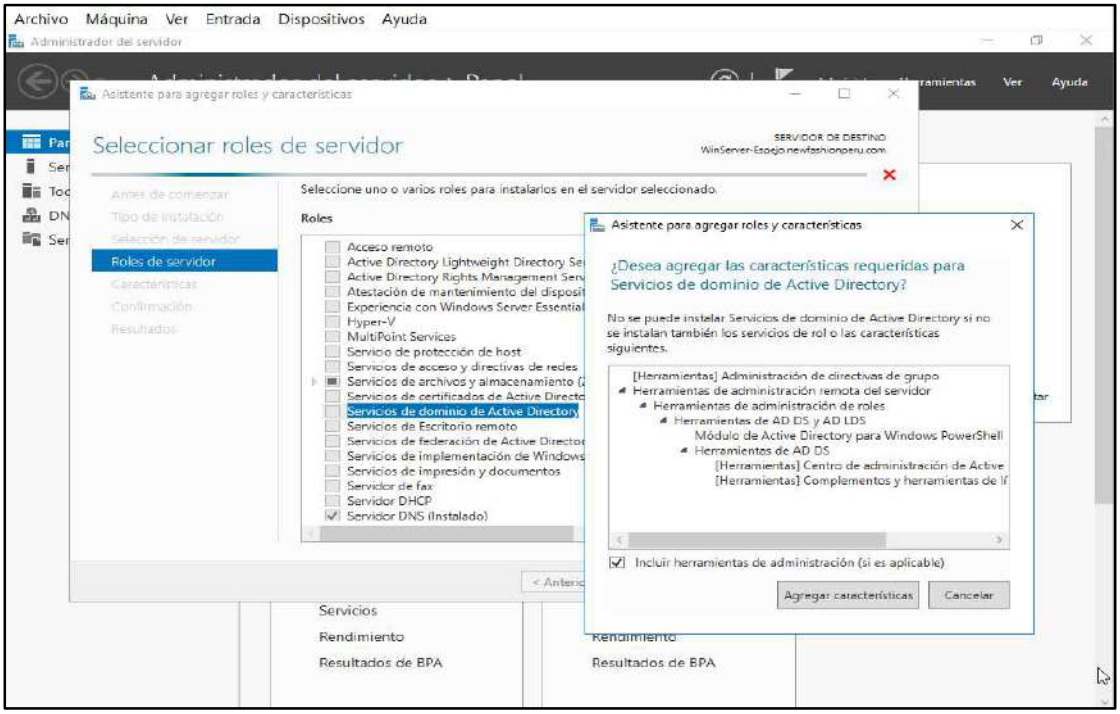
- Clic en Instalar



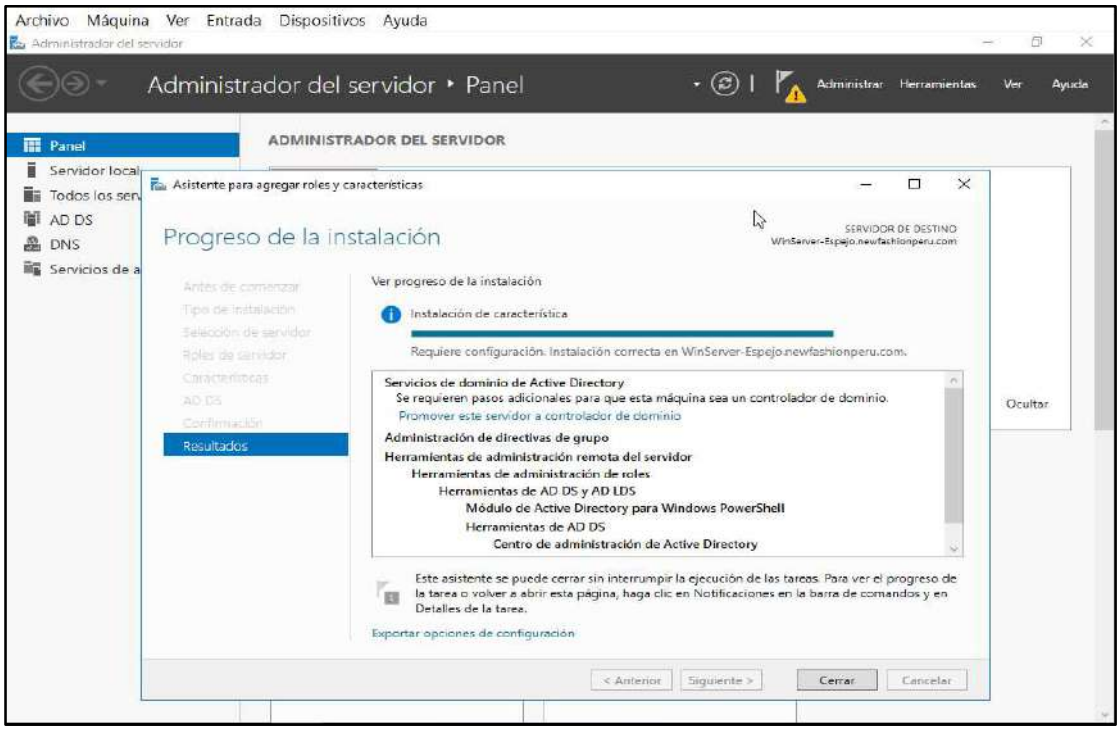
- Al terminar la instalación de las características, clic en siguiente



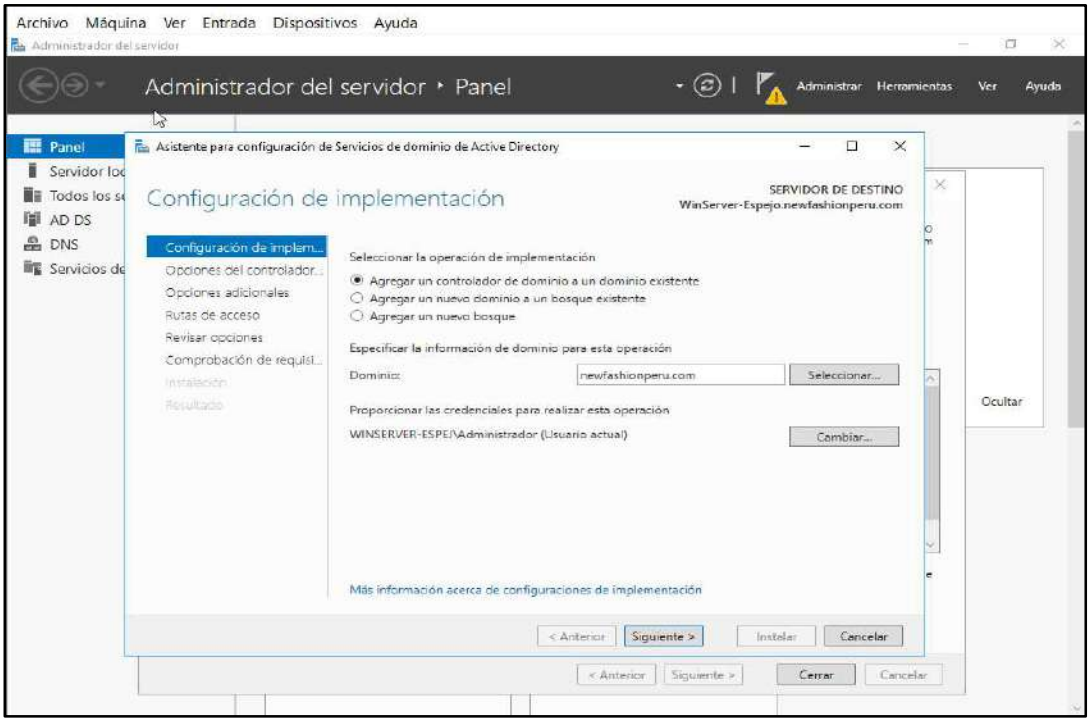
- Agregar la característica de Active Directory



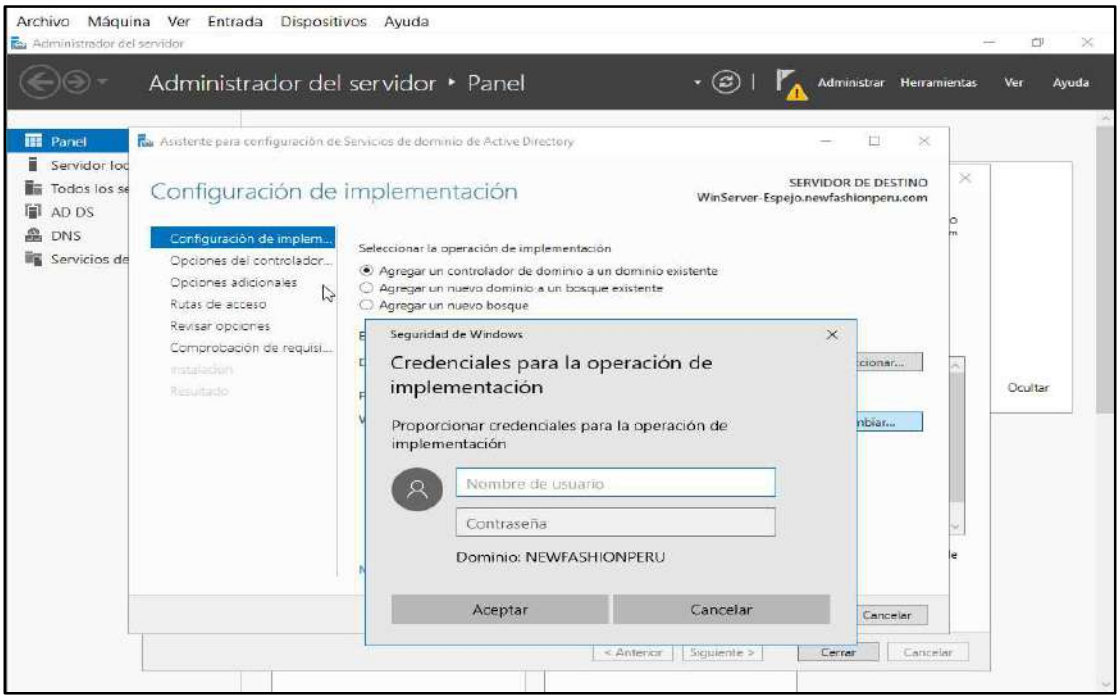
- Al terminar la instalación de las características, clic en siguiente



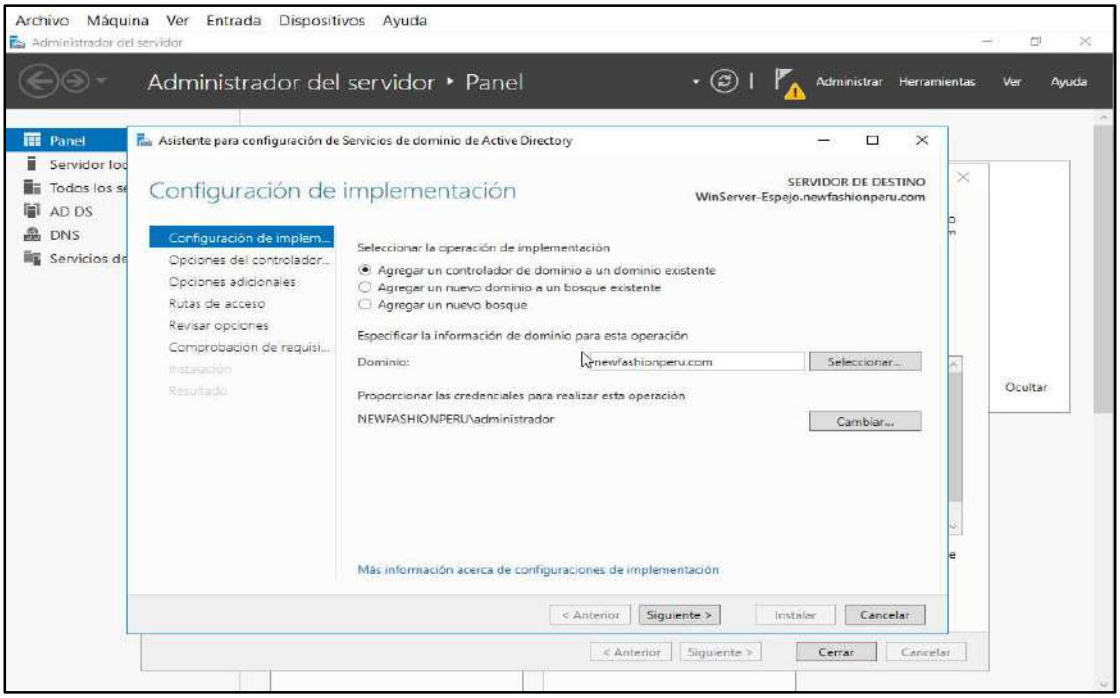
- Elegir Agregar un controlador de dominio a un dominio existente, clic en siguiente



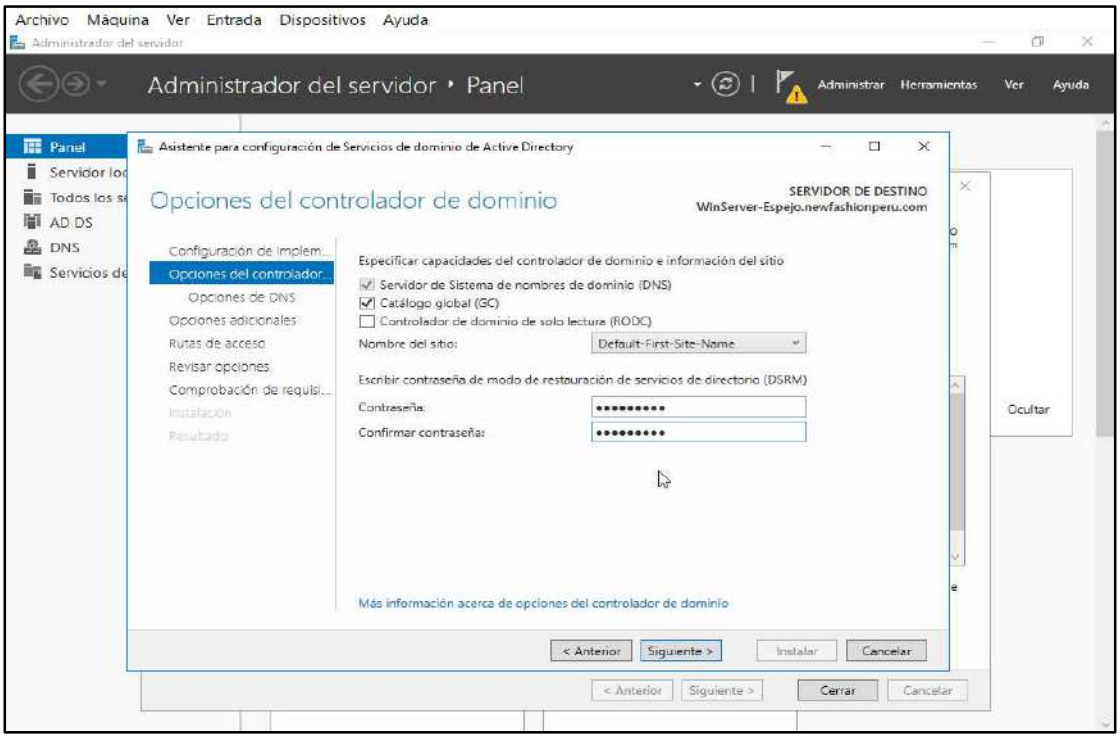
- Aquí colocar el Administrador y clave del Servidor de Dominio Principal



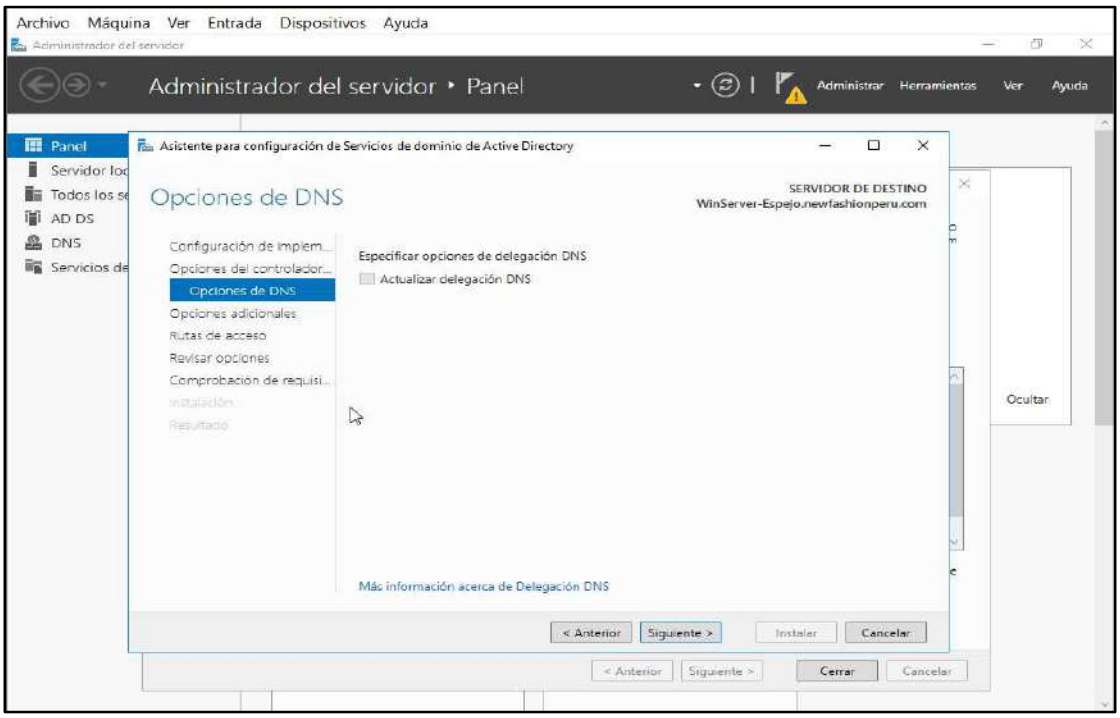
- Clic en siguiente



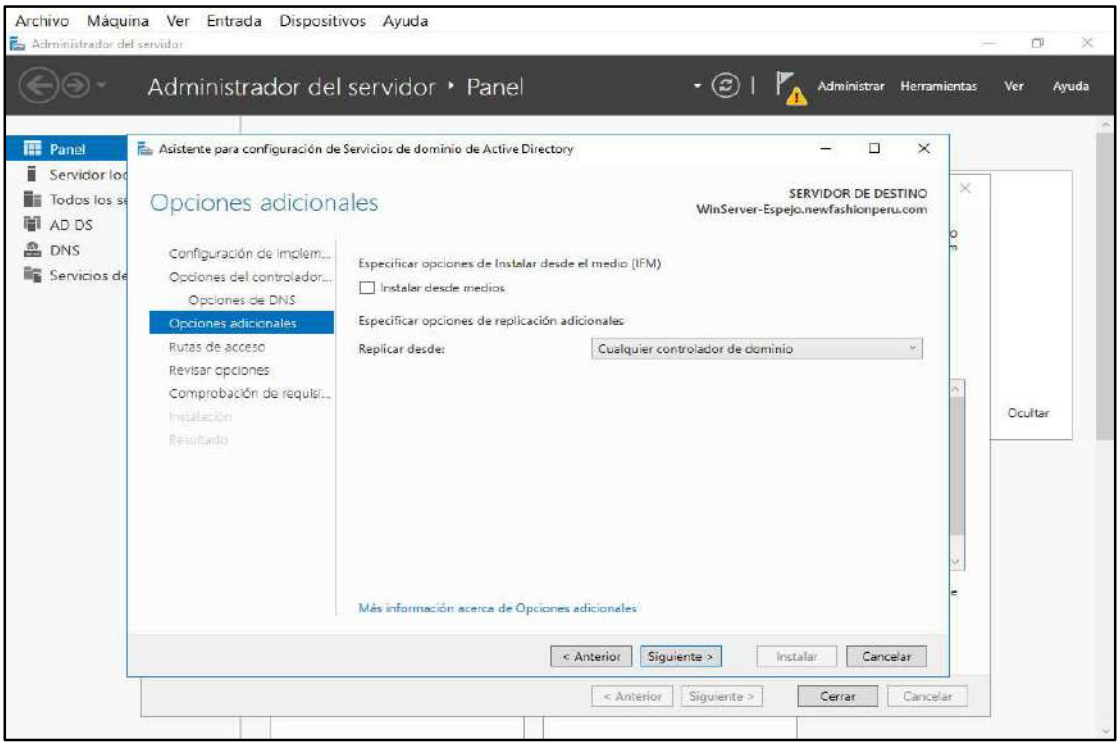
- Escribir una contraseña segura



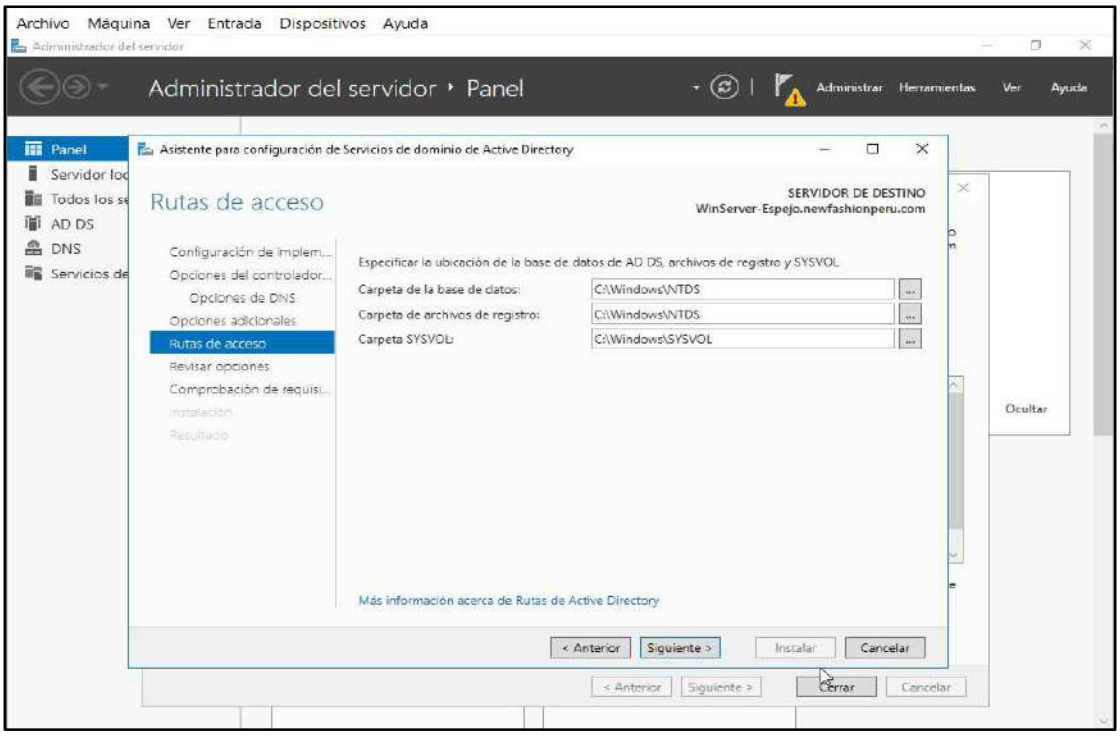
- Clic en siguiente



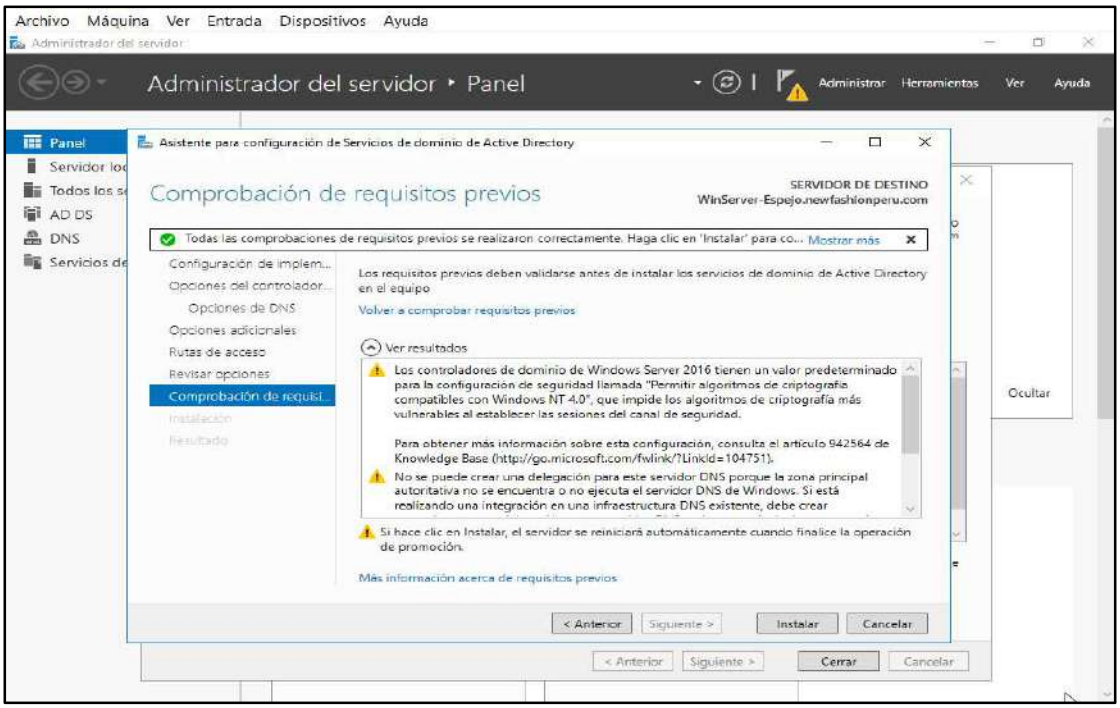
- Clic en siguiente



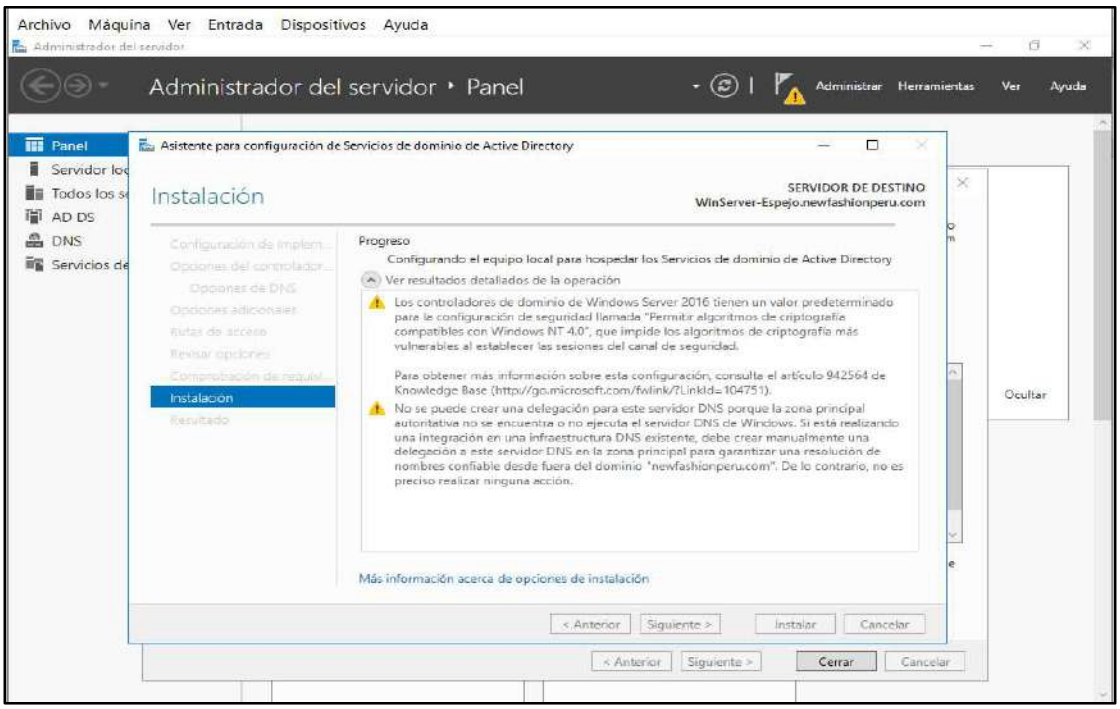
- Clic en siguiente



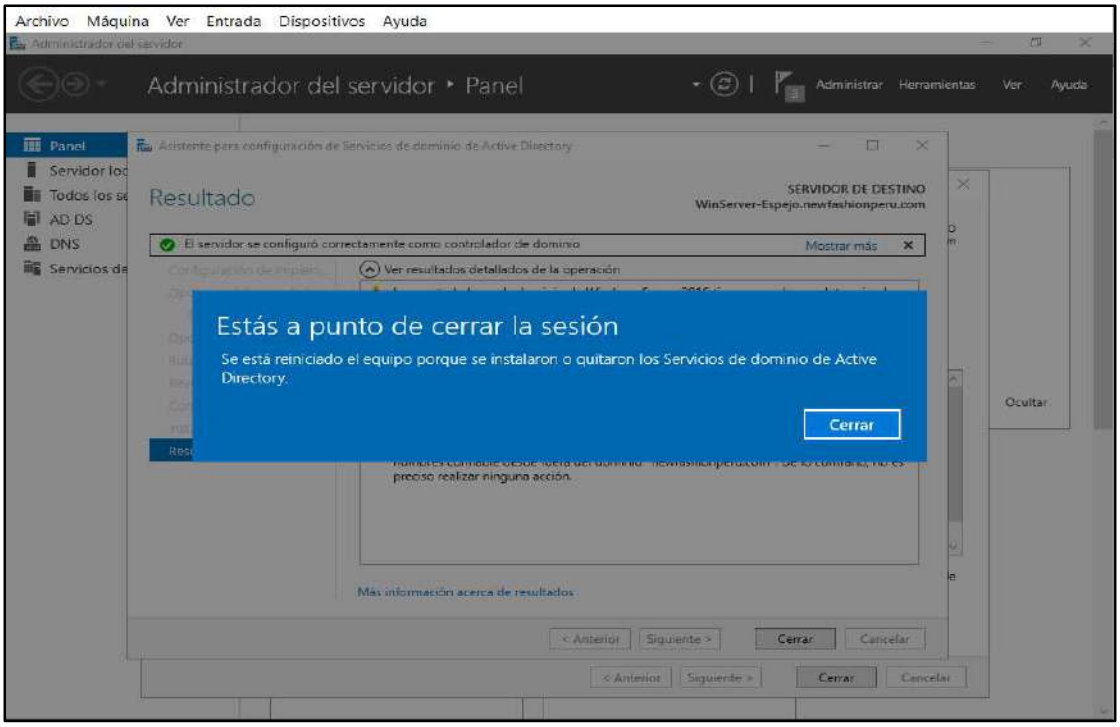
- Clic en Instalar



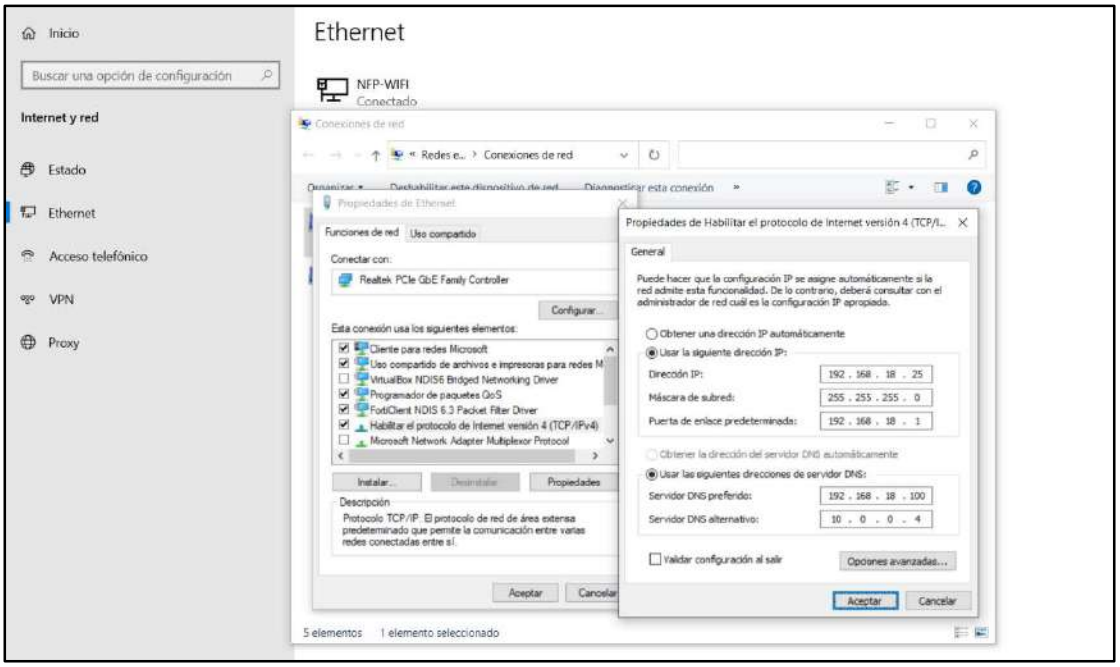
- Clic en Siguiente



- Clic en cerrar para que se reinicie el equipo, fin de la instalación



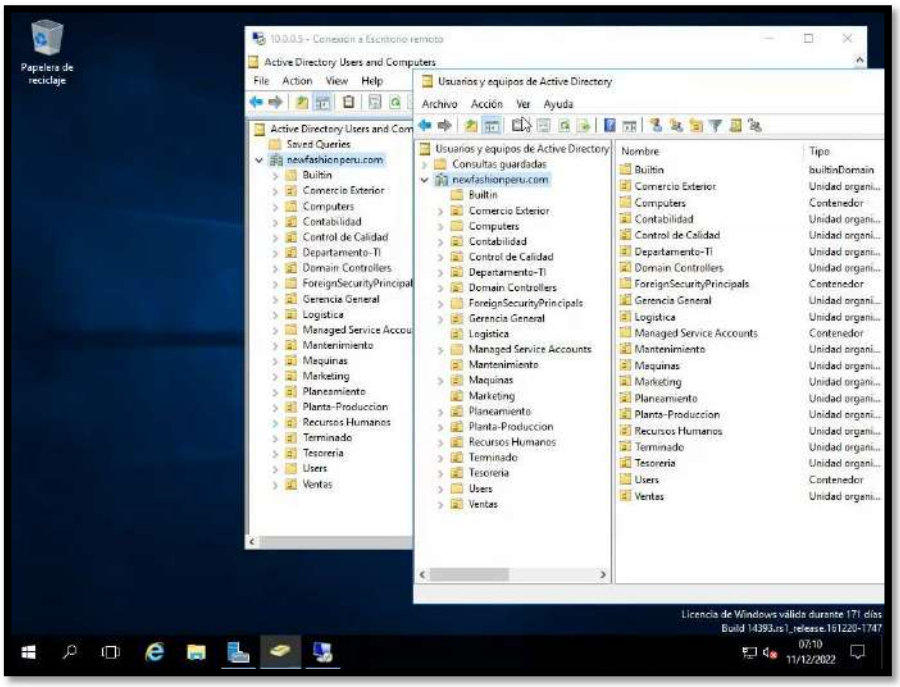
- Configuración del cliente en Windows 10 para conectarse al AD, en el DNS principal se coloca el IP del Servidor Principal y en el DNS Secundario se coloca el IP del Servidor Espejo en Azure.



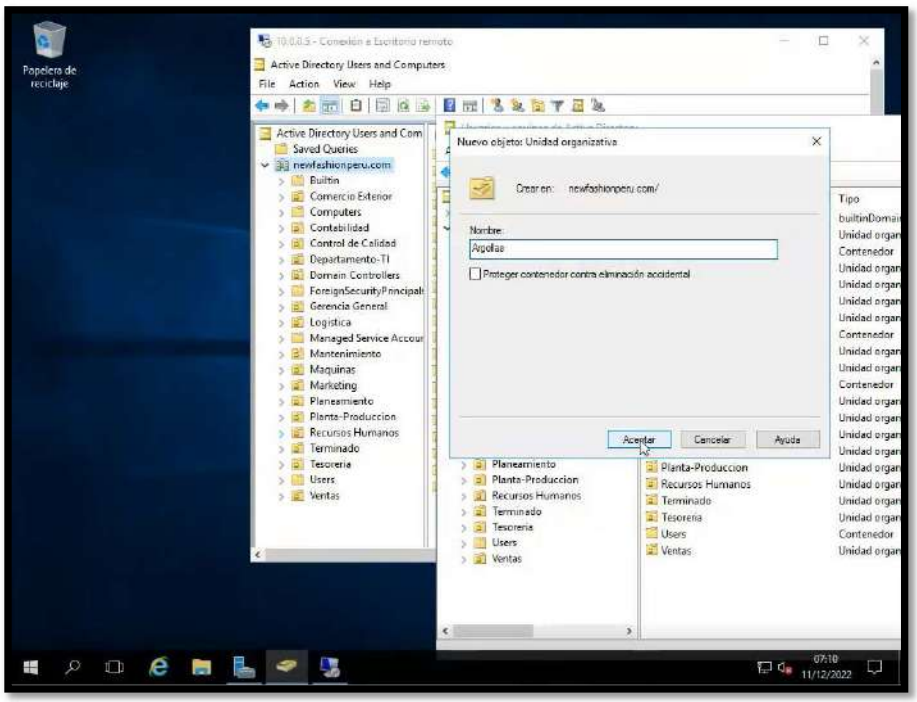
- Si por algún inconveniente el Servidor AD Principal deja de funcionar, automáticamente ingresa a trabajar el servidor AD en la nube de Azure ya que como se observa en la imagen ambos están configurados en los clientes de la red local.

PASO 11: Sincronizaciòn del servidor AD Principal y el AD en la nube

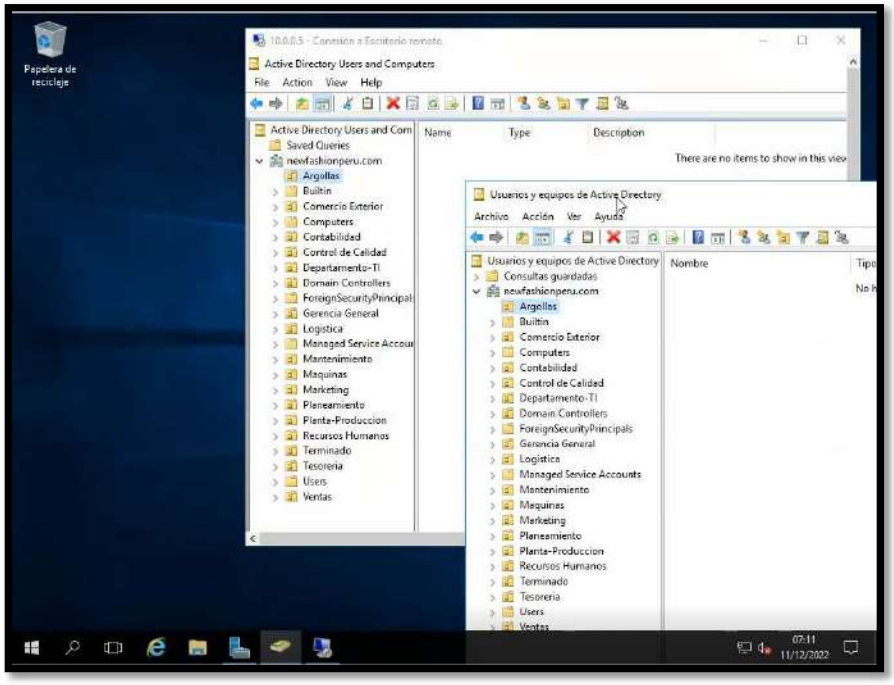
- Iniciamos el AD en ambos servidores



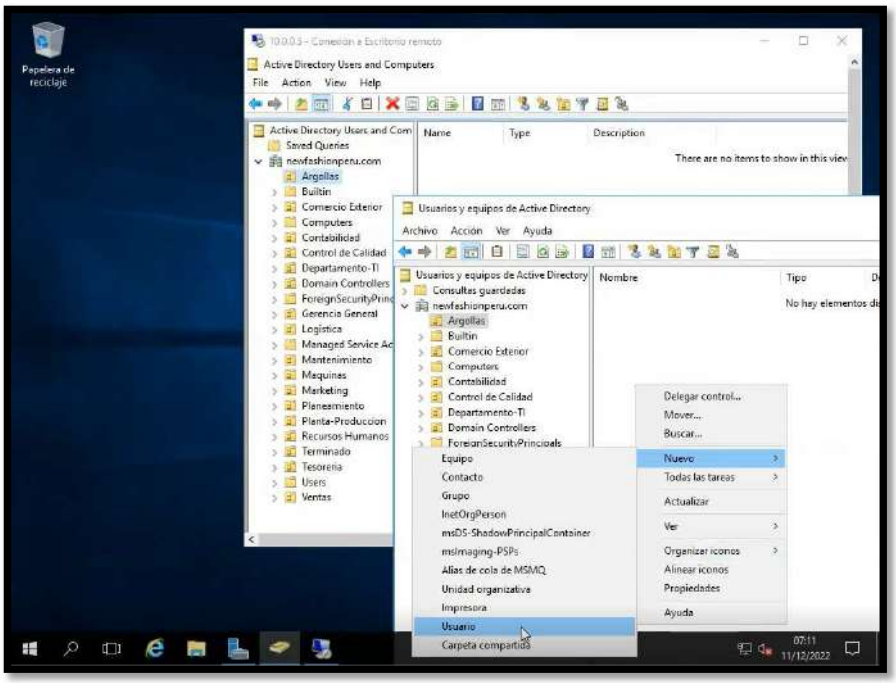
- Creamos las unidades organizativas en el servidor Principal y verificamos que se replica en el servidor en la nube



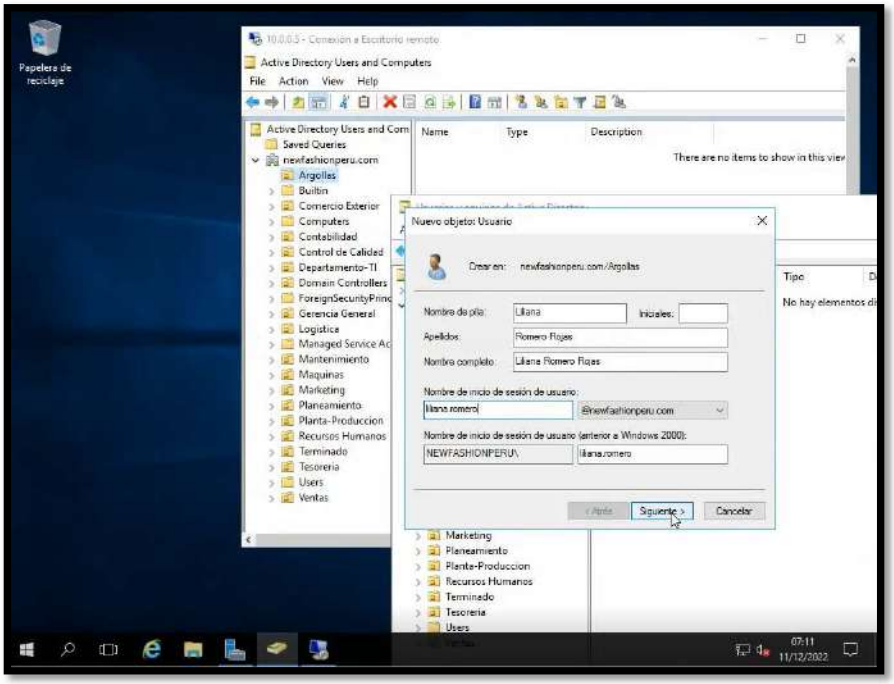
- Aquí podemos validar que la unidad organizativa “Argollas” se encuentra en el servidor principal y está respaldada en la nube



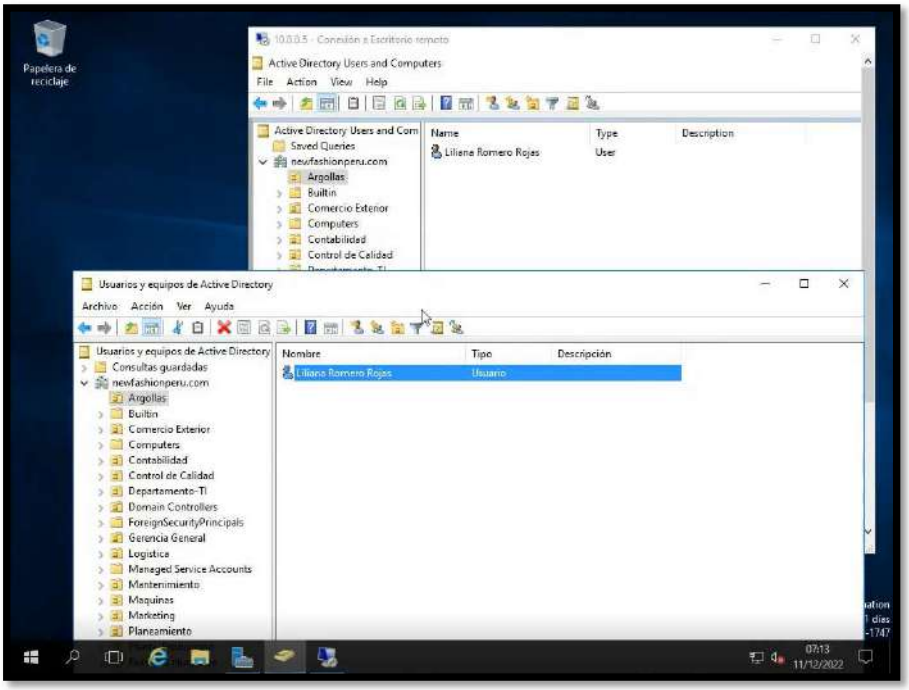
- Creamos un usuario en la Unidad organizativa “Argollas”



- Colocamos los datos del usuario y creamos una contraseña alfanumérica y con caracteres especiales.

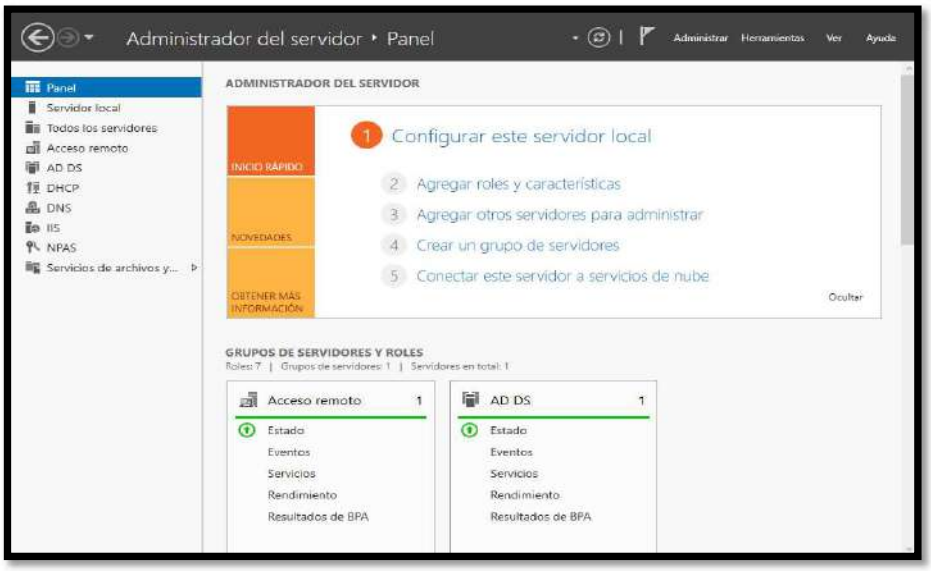


- Aquí validamos el usuario se ha replicado en el servidor espejo en la nube

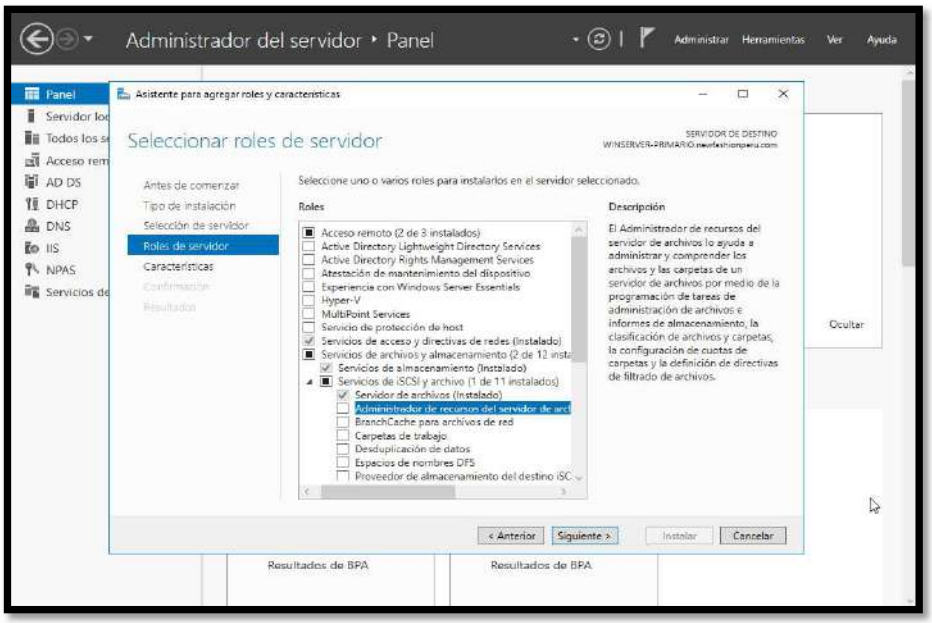


PASO 12: REPLICACIÒN DEL FILE SERVER EN LA NUBE

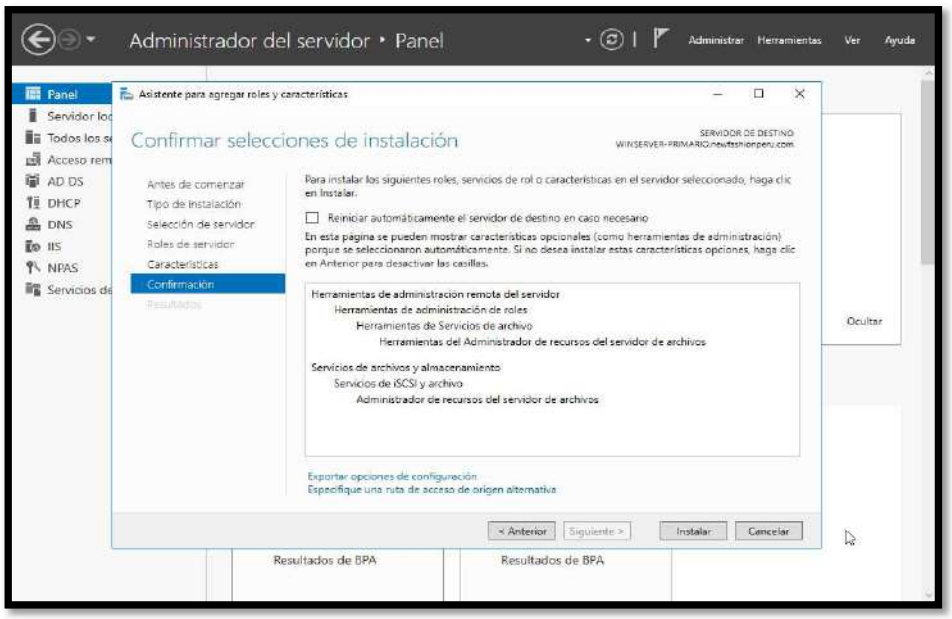
- Clic en Agregar Roles y Características



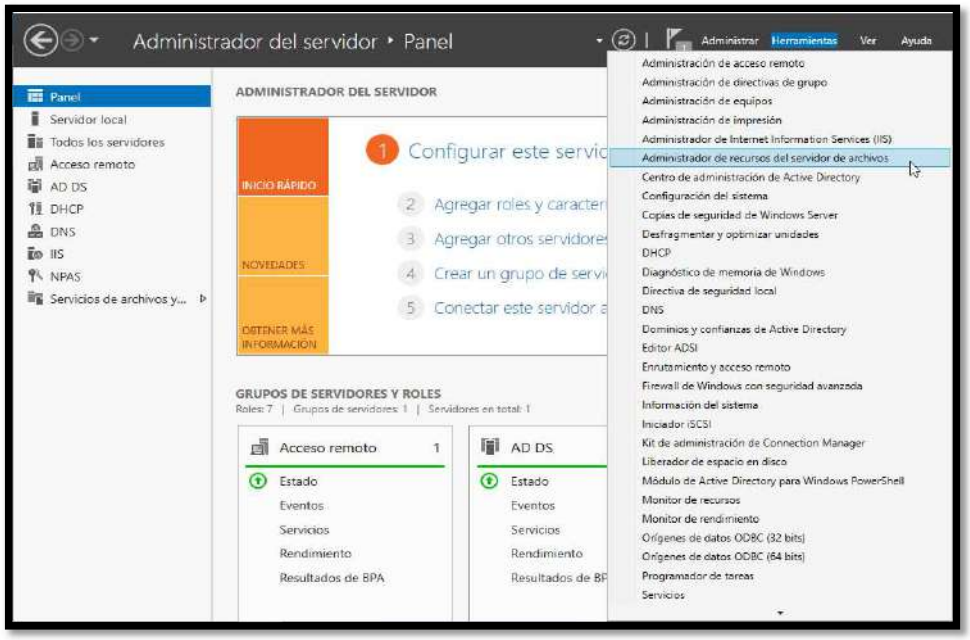
- Clic en Administrador de recursos del servidor. Siguiente.



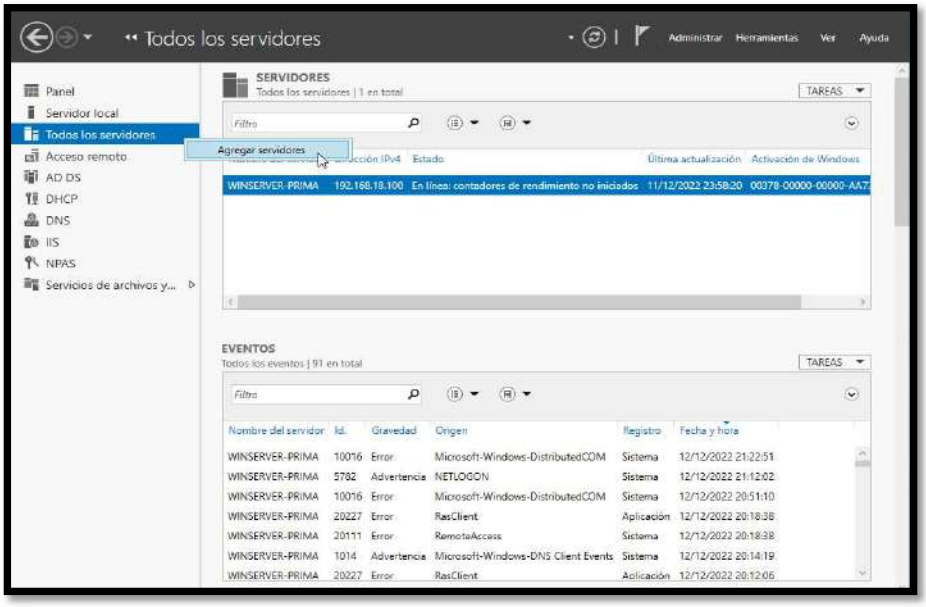
- Clic en Instalar



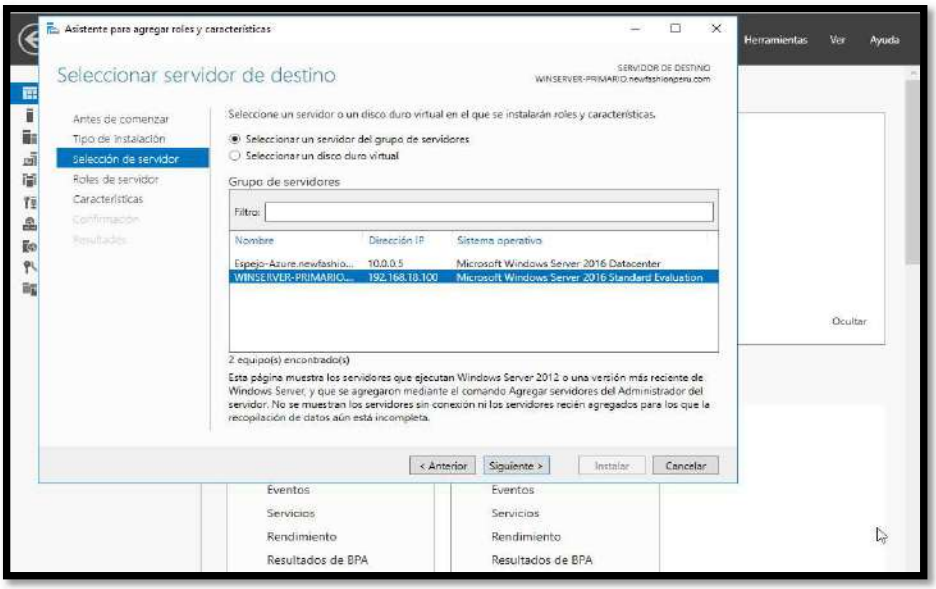
- Después de instalado, ingresar a Administrador de recursos del servidor de archivos



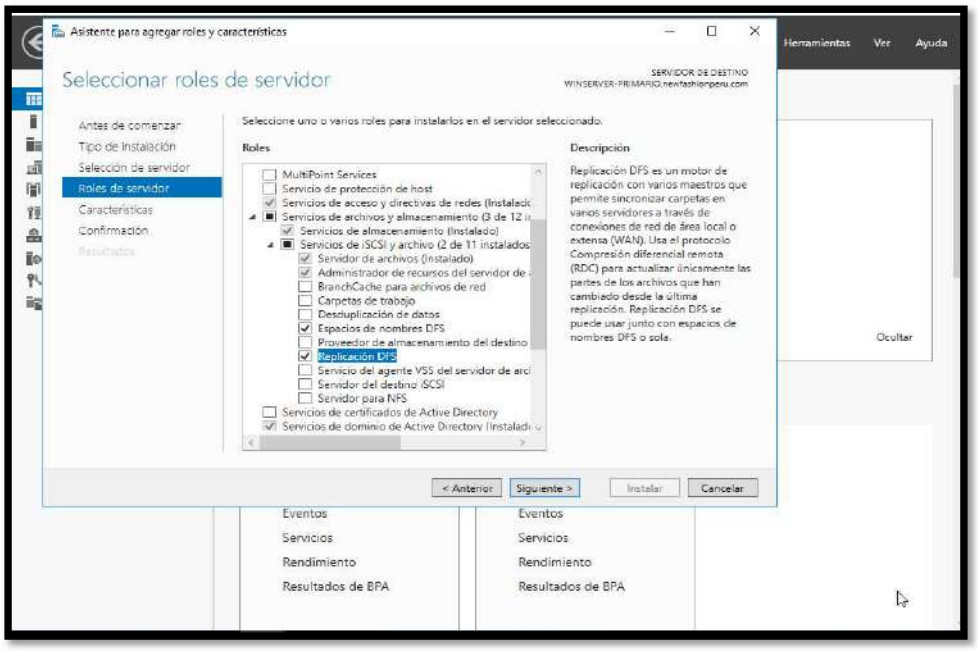
- Clic derecho agregar servidores y elegir el servidor principal



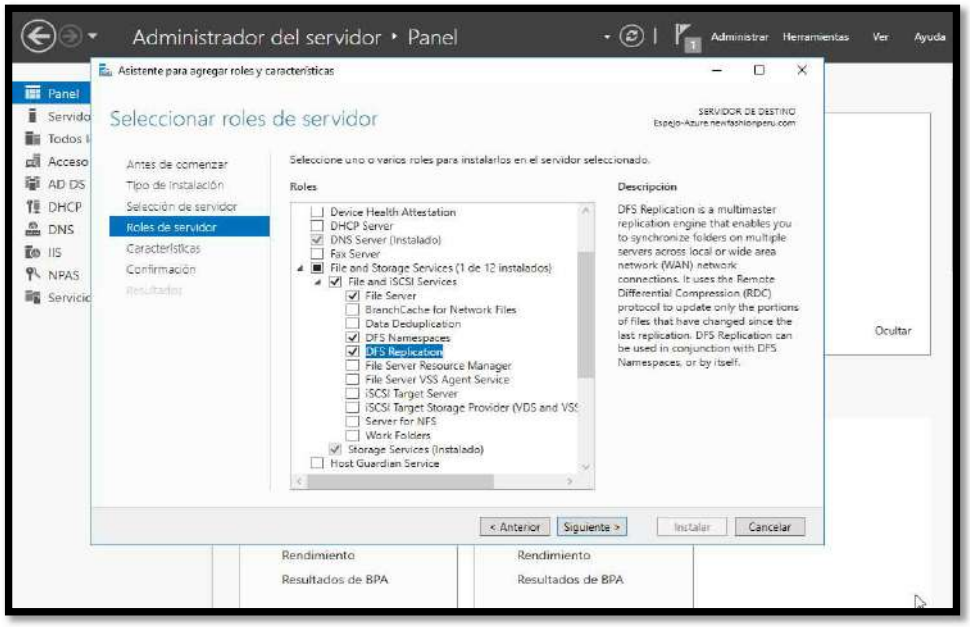
- Clic derecho agregar servidores y ahora elegir el servidor de Azure



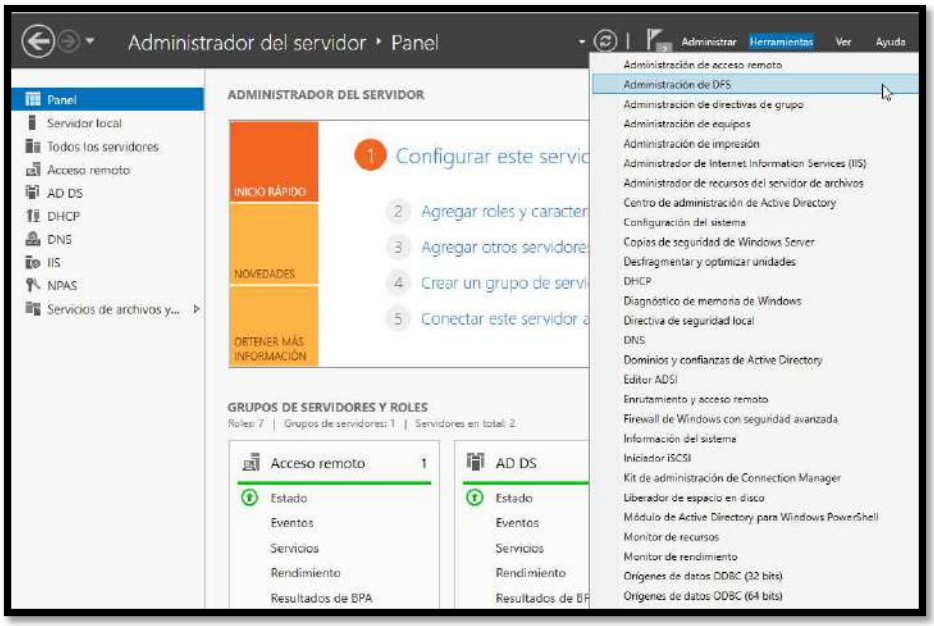
- Elegir Servicios de archivos y almacenamiento, luego Servidor de archivos y Espacios de nombres DFS y Replicación DFS. Luego Siguiente e Instalar.



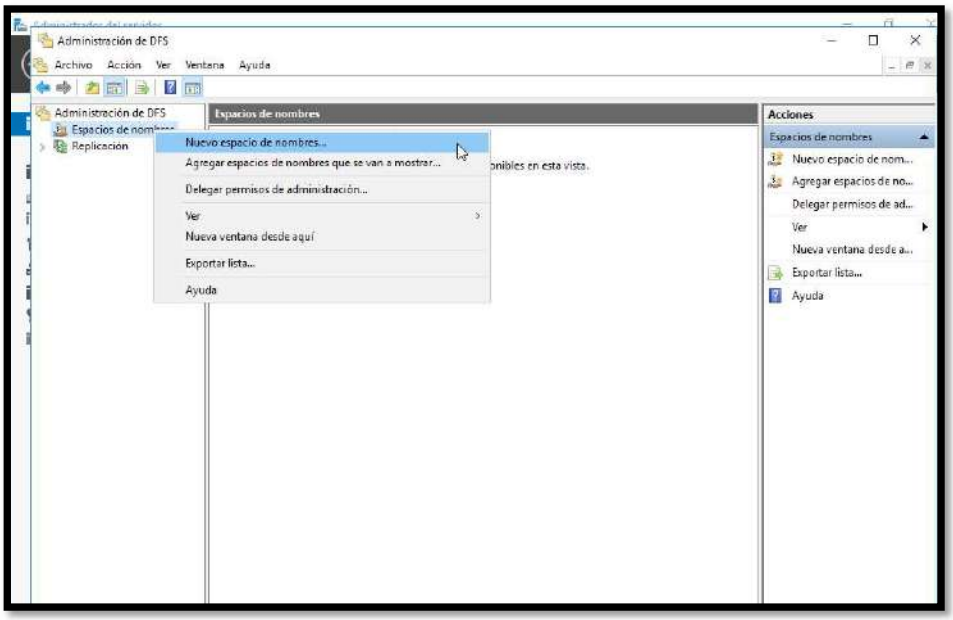
- Hacer la misma configuración igual para el Servidor en Azure.



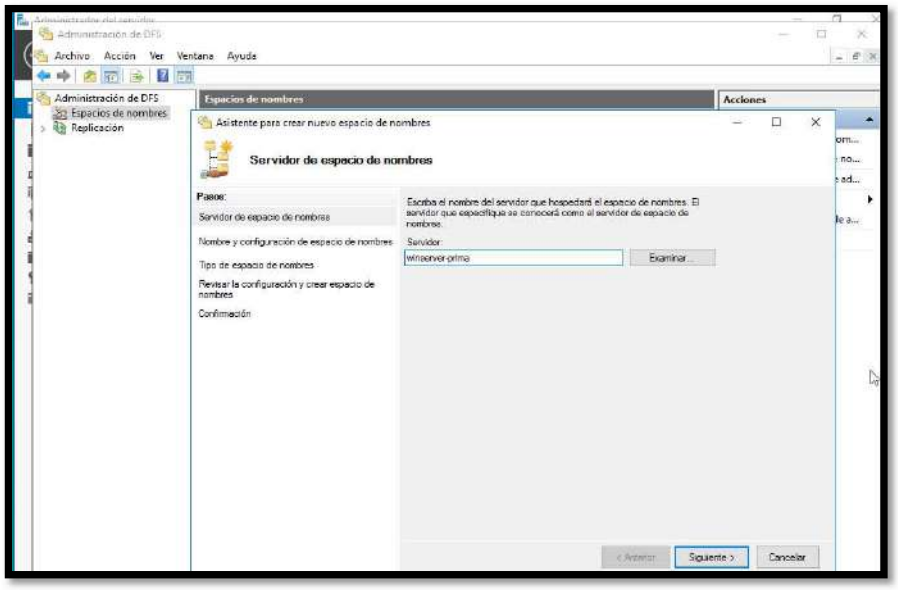
- Clic en Administración de DFS



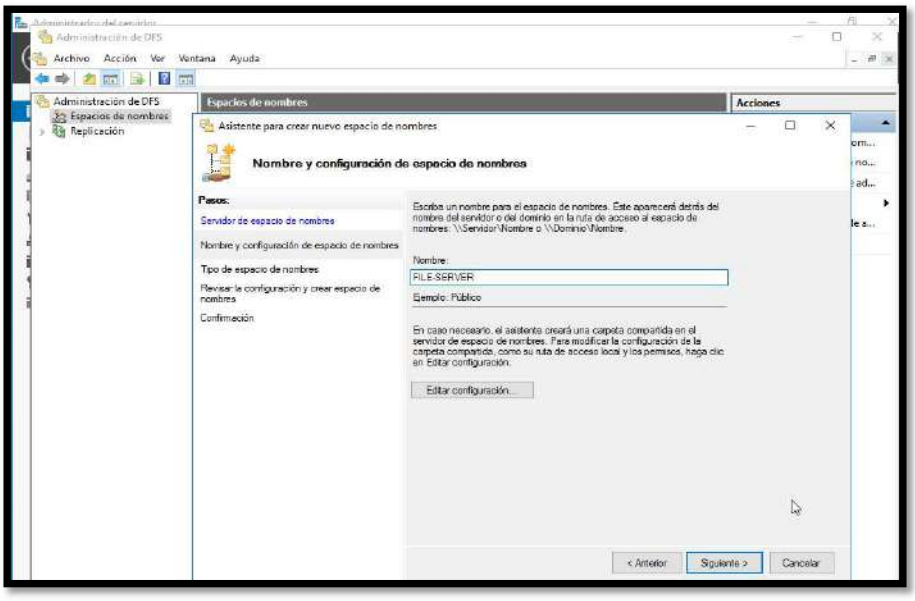
- Clic en Nuevo espacio de nombres



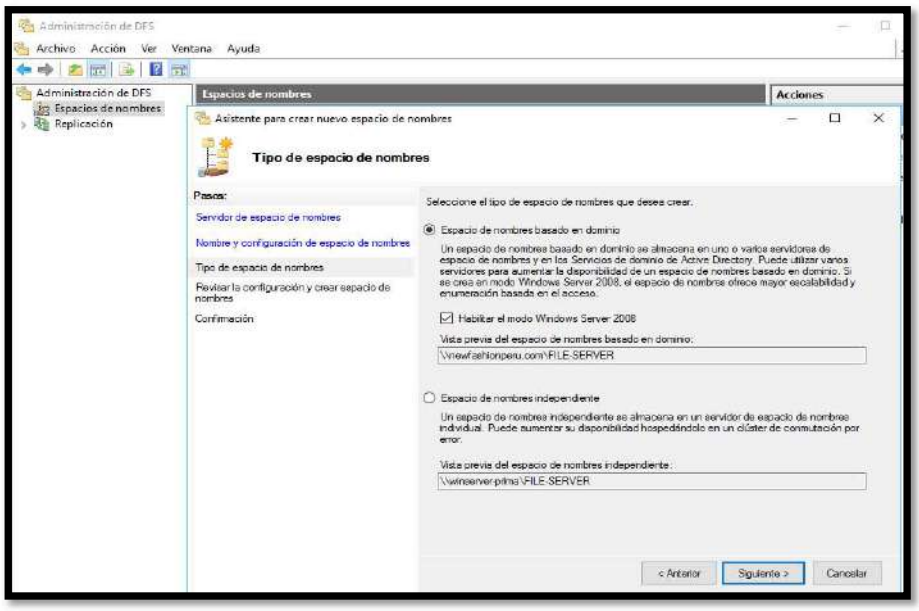
- Clic en examinar y elegir el servidor local primario



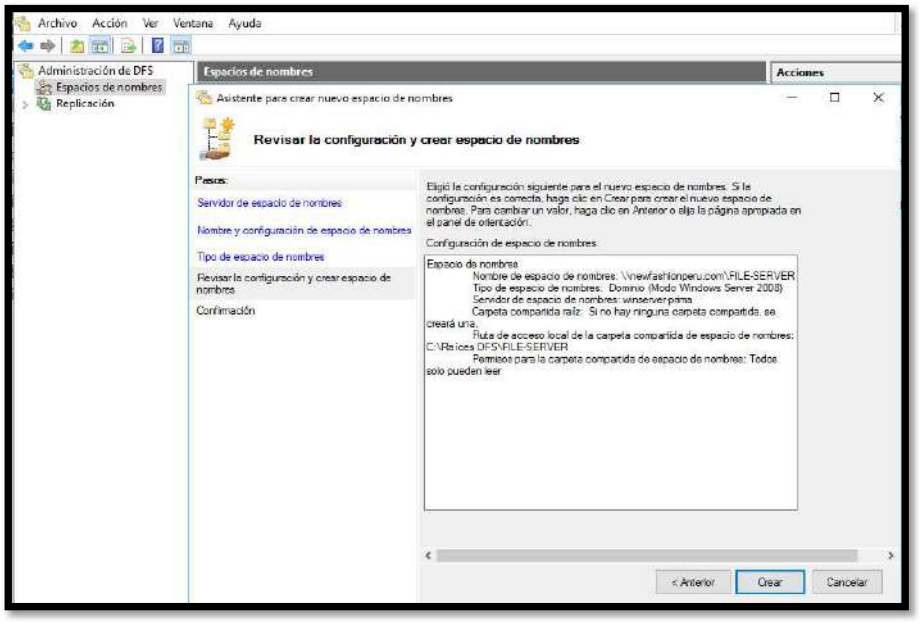
- Luego agregar un nombre para la carpeta compartida



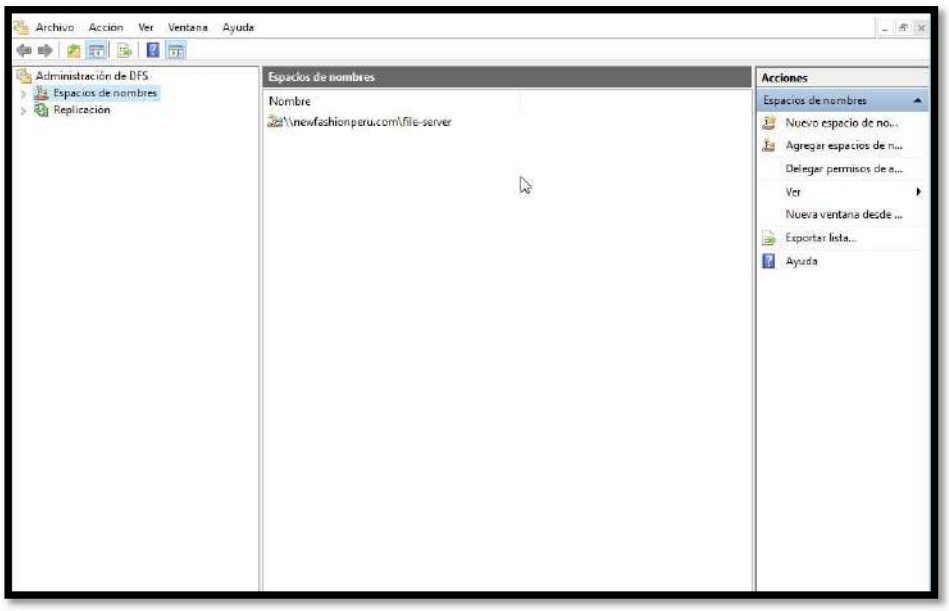
- Aquí se observa la ruta del servidor principal y la carpeta compartida. Siguiente.



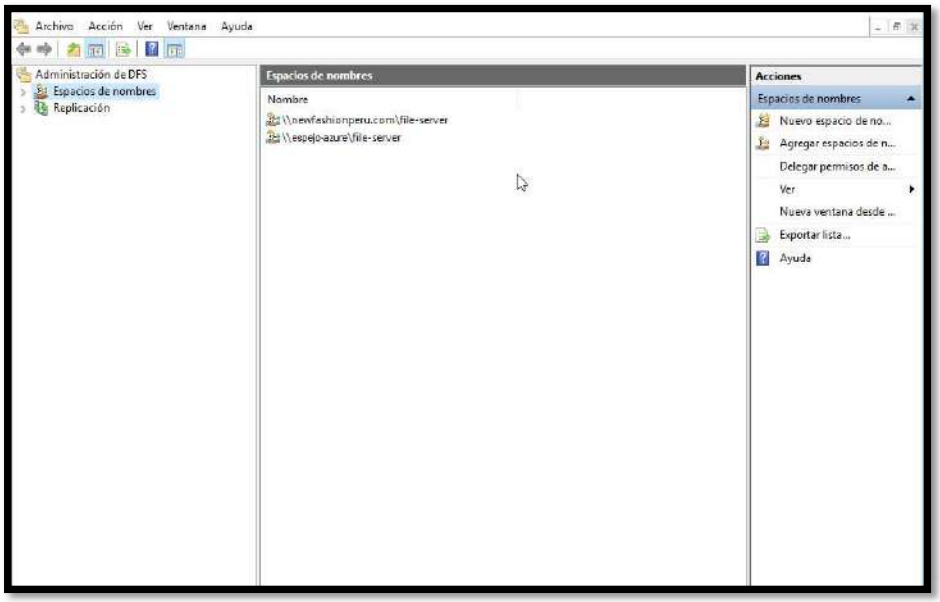
- Clic en Crear.



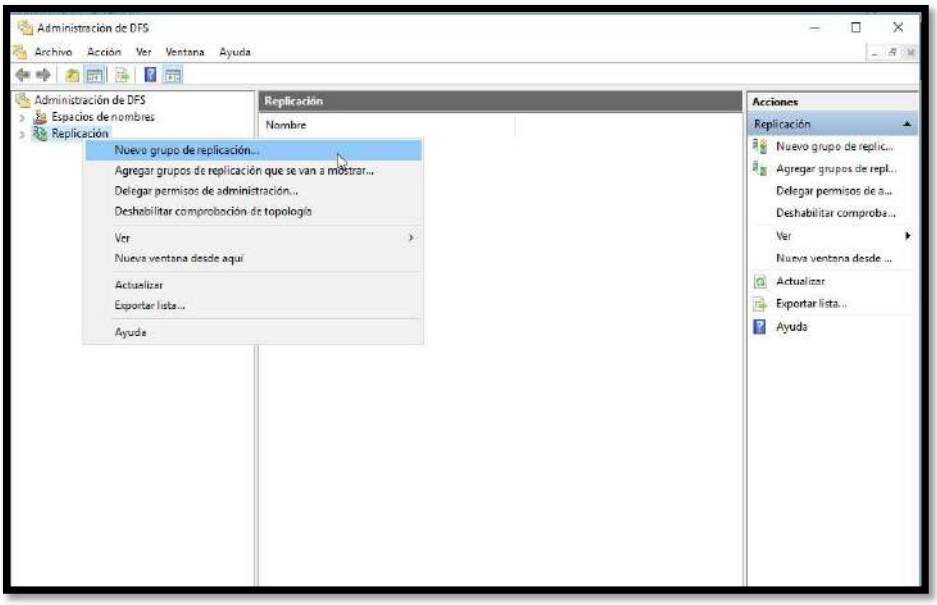
- Aquí se ve la carpeta file-server creada en el servidor principal, hacer los mismos pasos para el servidor en Azure



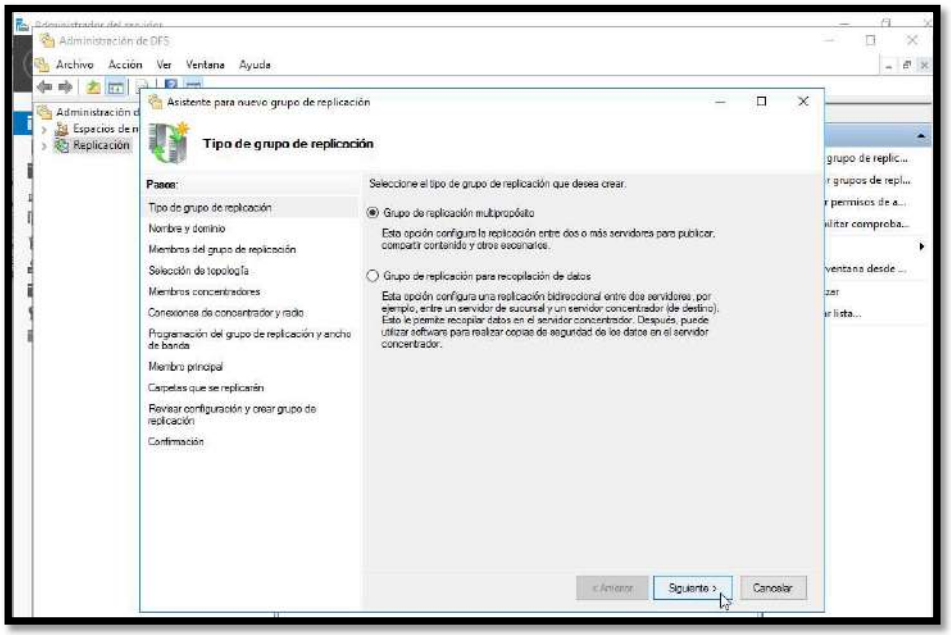
- Aquí ya se observa ambos servidores con sus carpetas compartidas



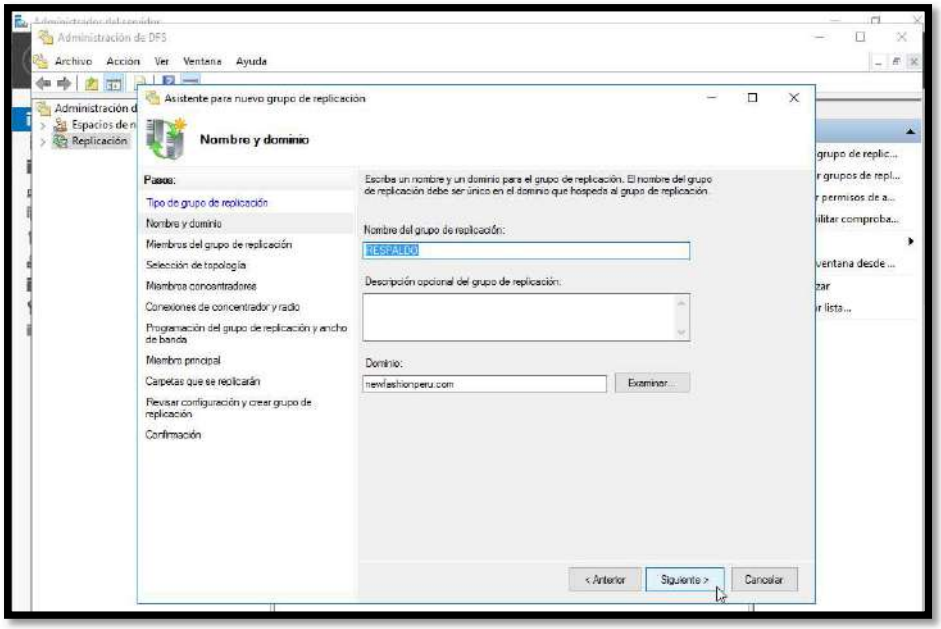
- Ahora agregamos un Nuevo grupo para la replicación



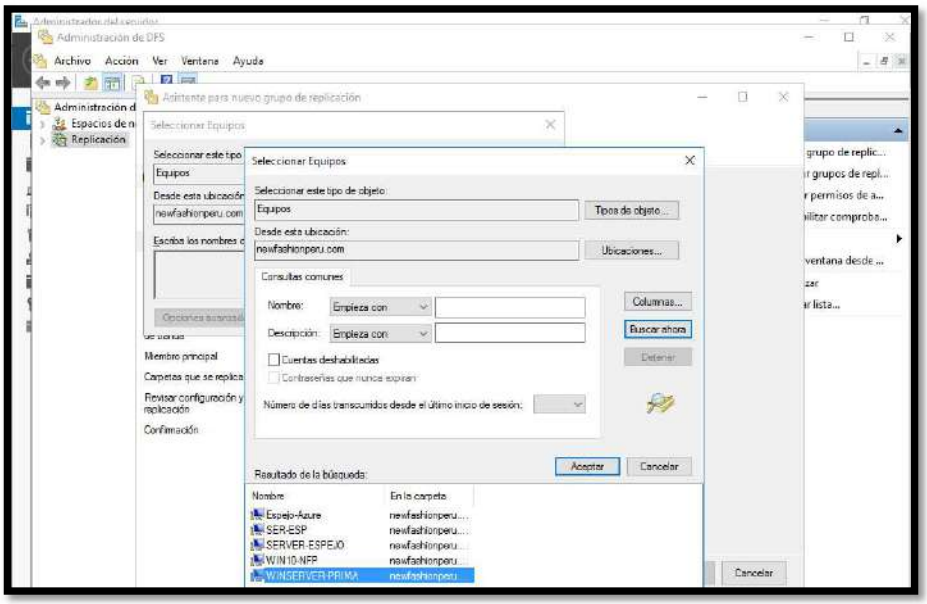
- Clic en Siguiente



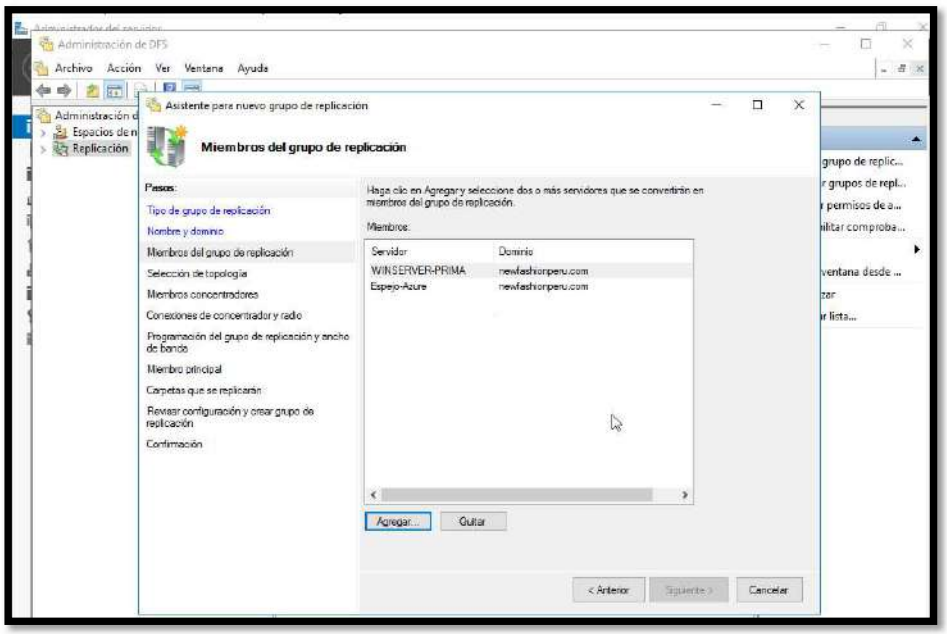
- Clic en examinar y elegir el servidor principal, luego colocar un nombre para la carpeta replicación, por ejemplo, Respaldo. Luego clic en Siguiente.



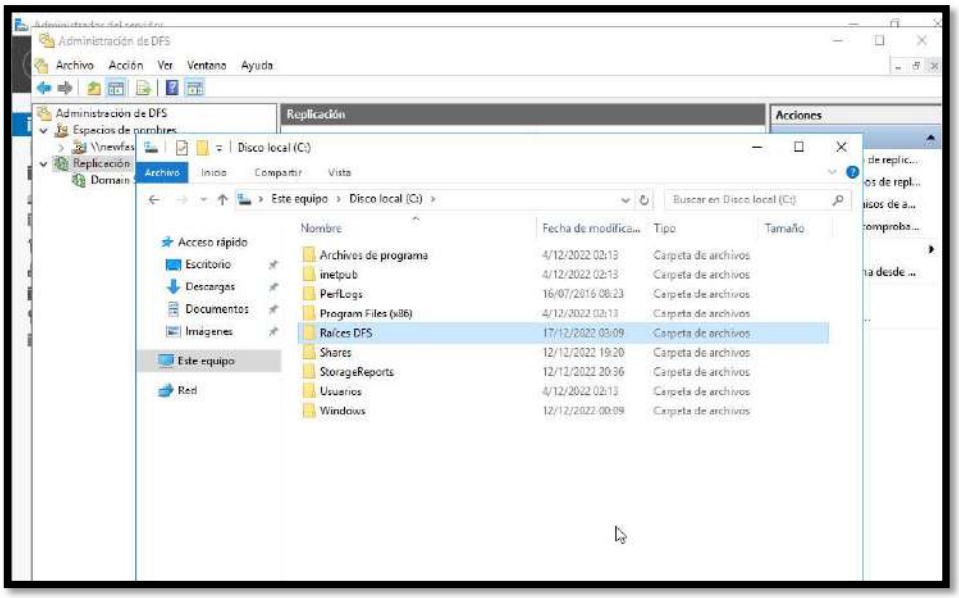
- Aquí se elige el Servidor principal, luego el servidor en Azure



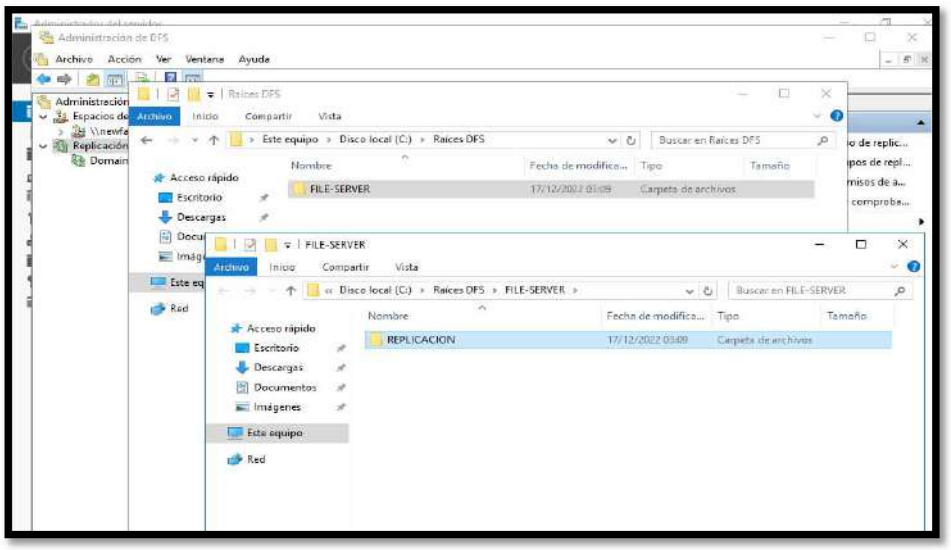
- Aquí ya se muestran los dos servidores que forman parte del grupo de Replicación



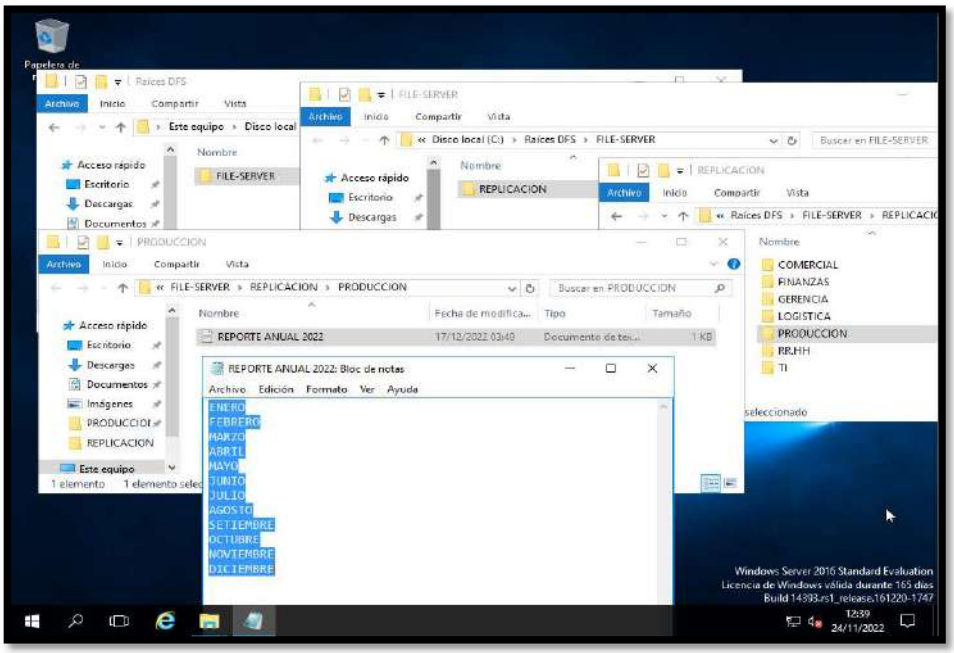
- Se observa en el explorador de Windows que hay una carpeta Raíces DFS



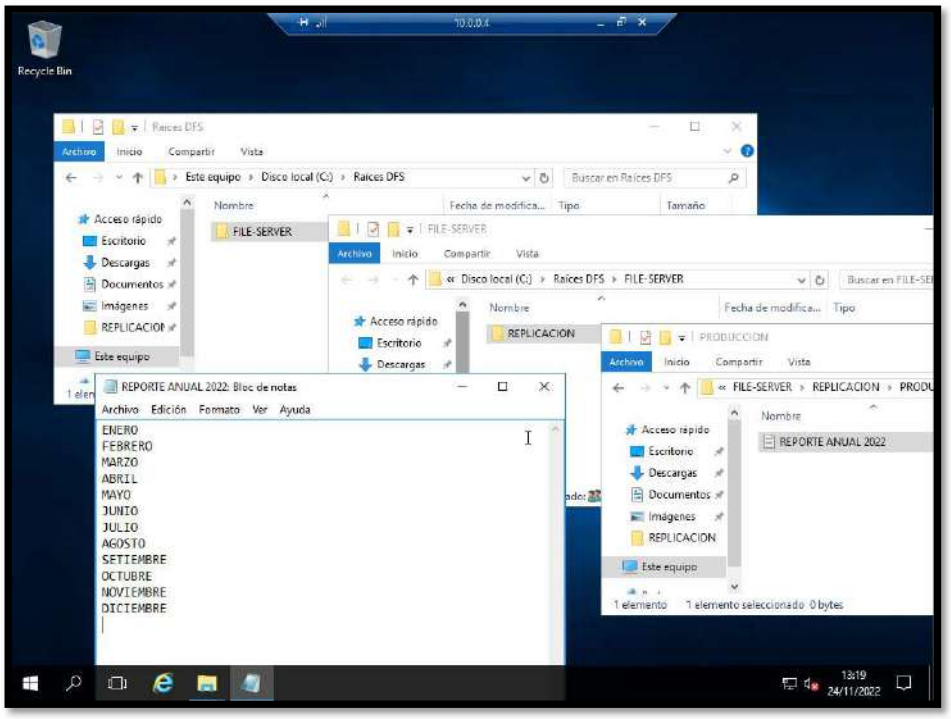
- Dentro de la carpeta Raíces DFS, dentro se encuentra la carpeta File-Server y dentro la carpeta Replicación



- Dentro de la carpeta Replicación en el servidor principal, se procede a crear como una prueba, un archivo de texto Reporte Anual 2022 y dentro carpetas con los meses del año.



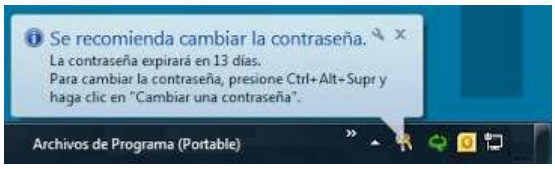
- Luego en el servidor en Azure vemos que la carpeta Replicación ha replicado correctamente el archivo Reporte Anual 2022 y su contenido con los doce meses.



Paso13: Implementar políticas de seguridad:

Procedimiento de Administración de contraseñas

Habilitar y configurar en el Active Directory las politicas de contraseñas, y verificar que se estén ejecutando correctamente.



Configuración del ad para la seguridad de las contraseñas

Actividad 1

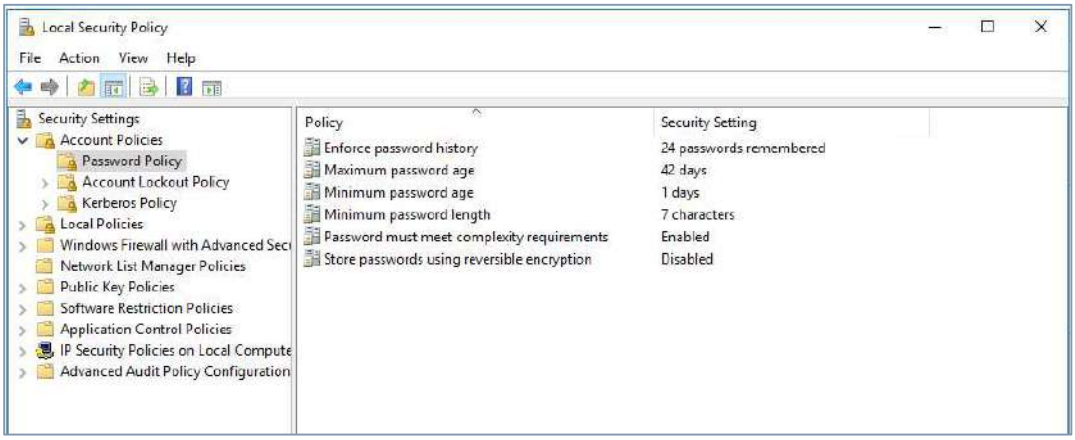
Ingresar al AD y dirigirse a la opción de políticas de seguridad.

Actividad 2

Dar clic para desplegar en la opción Account Policies.

Actividad 3

Dar doble clic en la opción Password Policy y configurar la política. Ver imagen



Actividad 4

Colocar en la configuración los siguientes parámetros:

- Exigir historial de contraseñas = **24 contraseñas recordadas** (Las contraseñas antiguas no se reutilizan continuamente).
- Vigencia máxima de la contraseña = **42 días** (La contraseña expira en 42 días)
- Vigencia mínima de la contraseña = **1 día** (La contraseña puede ser cambiado faltando 1 día).
- Longitud mínima de la contraseña = **7 caracteres**
- La contraseña debe cumplir los requisitos de complejidad = **Habilitado** (Las contraseñas deben contener mayúsculas, números y caracteres).
- Almacenar contraseñas con cifrado reversible = **Deshabilitado** (Se habilita para otros fines).

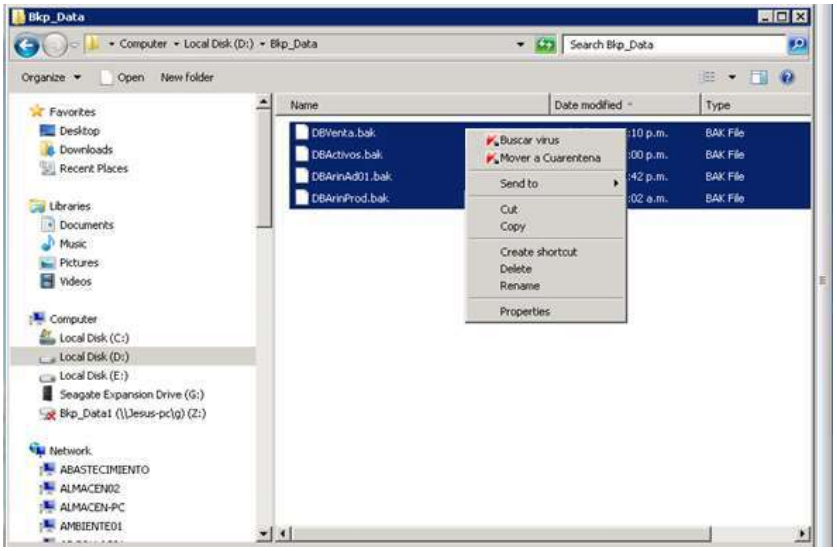
Procedimiento de copia de Backup de Base de Datos a Disco Externo

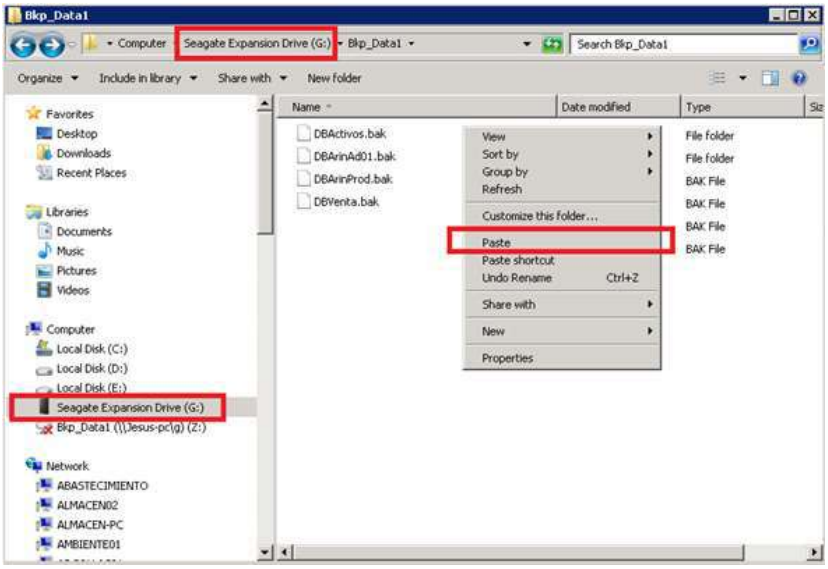
Actividad 1

Crear una tarea en el SQL que permita copiar los archivos .bkp de la BD a una carpeta compartida.

Actividad 2

Ingresar a la carpeta compartida y copiar los archivos a un disco externo. Ver imagenes.





Actividad 3

Realizar este procedimiento todos los días, tres veces al día.

Procedimiento de Backus a disco externo y entrega a personal a cargo

Actividad 1

Elaborar un formato para registrar nombre y apellidos, cargo, fecha y firma. Ver imagen.

FORMATO DE GUARDADO EXTERNO DE DISCO BACKUP

DE LA BASE DE DATOS DE NEW FASHION PERÚ

NOMBRE Y APELLIDOS	CARGO	FECHA	FIRMA

Actividad 2

Este formato debe ser llenado por las personas encargadas que se van a llevar una de las copias de la BD en un disco externo a su domicilio.

Actividad 3

Este procedimiento se debe de realizar diario o Inter diario.

Políticas de Licenciamiento:

- Los servidores deben estar licenciados
- Todas las maquinas de los usuarios deben ser licenciadas
- El office debe estar debidamente licenciado en cada maquina
- Los programas de diseño deben ser licenciados
- Todo software nuevo adquirido debe ser revisado por el responsable de sistemas

Políticas de carpetas compartidas

- Se delimitan los accesos a las carpetas, solo se dio permisos a las personas autorizadas por cada área.
-

VERIFICAR

Verificación del AD

Después de haber sincronizado y replicado el servidor de Active directory, y el file server se obtuvo un resultado favorable en cuanto a mejorar los procesos de seguridad de los datos de la empresa, verificamos que el tener un servidor en la nube ayuda a tener un plan de contingencia ante cualquier eventualidad que pueda ocurrir , como ciber ataques, desastres naturales u otro tipo de problema, los datos del servidor de dominio fueron respaldados satisfactoriamente en el servidor espejo en la nube aumentando la seguridad de los datos de los usuarios y guardando las políticas de seguridad del sistema.

Verificación del File server

El file server se sincronizo exitosamente en la nube, aumentando el nivel de confidencialidad, integridad y disponibilidad de los datos de la organización, todas las carpetas del servidor principal se resguardaron en la nube, mediante copias de seguridad, eso quiere decir que la disponibilidad de los archivos siempre estará en un 100%,

En la siguiente tabla se muestra cómo se encontraba la organización antes de implementar el método de seguridad de información con servidor espejo, aquí podemos notar que la confidencialidad se encontraba a un 100.0 % del nivel de incumplimiento, la integridad se encontraba a un 85.7% del nivel de incumplimiento y la disponibilidad se encontraba a un 100.0% del nivel de incumplimiento lo cual generaba que la información de la empresa este expuesta antes cualquier situación de peligro.

Pilares de la seguridad de la información	Niveles de cumplimiento		
	No cumple	Cumple parcialmente	Cumple
Nivel de confidencialidad de la empresa	100.0	0.0	0.0
Nivel de integridad de la empresa	85.7	14.3	0.0
Nivel de disponibilidad de la empresa	100.0	0.0	0.0

En la tabla siguiente mostramos como se encuentra la confidencialidad , integridad y disponibilidad de los datos de la organización después de implementar el método

con políticas de seguridad de información con servidor espejo en la nube, lo cual nos muestra un cambio positivo donde podemos mostrar que la confidencialidad de los datos se encuentran a un nivel de cumplimiento del 85.7 % después de haber implementado el método y la integridad se encuentra a un nivel de cumplimiento del 71.4% para resguardar los datos del sistema y la disponibilidad subió a un 100.0% lo cual nos conlleva que la implementación de procesos mediante el PHVA cumple con resguardar la seguridad de la información en las pymes.

Pilares de la seguridad de la información	Niveles de cumplimiento		
	No cumple	Cumple parcialmente	Cumple
Nivel de confidencialidad de la empresa	0.0	14.3	85.7
Nivel de integridad de la empresa	0.0	28.6	71.4
Nivel de disponibilidad de la empresa	0.0	0.0	100.0

ETAPA 3: EJECUCIÒN DEL METODO Y PRUEBAS

El metodo se ejecuto en la empresa NEW FASHION, donde se tomaron las diferentes areas con las que contaba la empresa, se empezo identificando los activos de informaciòn luego se procedio a observar como era el flujo de trabajo con los datos del sistemas, el metodo se ejecuto desde las oficinas del area de sistemas, se analizo y verifico los servidores que contaba la empresa, luego de hacer un analisis se concluyo que la mejor opcion era respaladar la seguridad de los datos en la nube y asi poder mantener la confidenciabilidad, integridad y disponibilidad de los datos de la empresa y por ello se adquirio el acceso a la nube para implementar el metodo mediante el servidor espejo, lo cual se procedio en sincronizar el Active Directory y servidor de File server , tambien se sincronizo el DNS de la empresa, se sincronizo los rangos de IP, se sincronizo la ip inversa que nos ayuda a la busqueda por nombre, las area con que cuenta la empresa son Gerencia, Logistica, Finanzas, Recursos Humanos, Sistemas, Asesoria Legal y Producciòn.

Esta ejecuciòn tomo alrededor de 30 dias donde se empezo evaluando las distintas areas con que cuenta la empresa, se empezo por el area de sistema donde se identifico los activos de informaciòn y se obtubo un resultado bajo sobre el respaldo de la seguridad de sus datos, ya que contaba con servidores fisicos pero sus datos no estaban protegidos y mucho menos contaban con copias de seguridad, ademas de verificar que los servidores no se encontraban en un ambiente adecuado , ya que mucho personal transcurria por esas oficinas, luego se verifico las otras areas nombradas donde se pudo obtener un resultado que la confidencialidad ,integridad y disponbibilidad de sus datos no estaban respaldas ni ptotegidas ante cualquier eventualidad negativa que pudiera ocurrir en la empresa y esto era grabe debido a que en cualquier momento podrian sufrir una perdidad de su datos por no contar con un metodo de seguridad de respaldo.

Para evaluar la confidencialibilidad de los datos de cada area de la empresa se tomo en cuenta 6 indicadores los cuales ayudaron a determinar si la empresa cumplia con los requisitos minimos para proteger su informaciòn , los indicadores utilizados fueron:

- Gestiòn de los incidente de la seguridad de la informaciòn
- Control de Documentos
- Gestiòn de Contraseñas
- Gestion de seguridad de datos
- Gestiòn de fugas de informaciòn
- Soporte de lo datos de informaciòn

Para evaludar la integridad de los datos del sistema por cada area de la empresa tambien se uso 3 indicadores los cuales fueron:

- Incidentes en la integridad de los documentos.
- Frecuencia de incidentes en la integridad de los datos del sistema.
- Integridad de documentos y Control.

Para evaluar la disponibilidad de los datos del sistema tambien se utilizaron tres indicaros que ayudaron a tener un resultado de como se encontraban las area, los indicadores fueron:

- Seguridad Fisica y del entorno.
- Incidentes en la disponibilidad de la informaciòn.
- Disponibilidad de serviciòs de informaciòn.

Estos indicadores ayudaron a reemplantear una estrategia que ayude a mejorar la seguridad de informaciòn de los datos del sistema, lo cual se utlizo el metodo implementado mediante un servidor espejo.

ETAPA 4: Evaluación de efectividad del método

Primer Lugar:

Fue efectiva ya que obtuvimos una reducción de riesgos debido al establecimiento y seguimiento de controles, se logro reducir las amenazas y se logro alcanzar un nivel asumible en la organización, de este modo si se produce una incidencia, los daños se minimizan y la continuidad del negocio esta asegurada.

Segundo Lugar:

Fue efectiva ya que se obtuvo un ahorro de costos derivado de una racionalización de los recursos, se eliminaron las inversiones innecesarias e ineficientes.

Tercer Lugar:

La seguridad paso a estar organizado y transformarse en un ciclo de vida metódico y controlado en el que participa toda la organización.

Cuarto Lugar:

Fue efectivo porque se logro el cumplimiento de los procedimientos y políticas de seguridad y así se evitó riesgos y costos innecesarios.

Quinto Lugar:

La implementaciòn del metodo de suguridad de informaciòn mediante el servidor espesjo en la nube con herramientas open source fue evaluado su efectividad mediante una lista de cotejo que ayudo a verificar si la empresa mejoro su confidencialidad , integridad y disponibilidad de los datos, esta lista de cotejo contenia diferentes indicadores que ayudaron a evaluar los tres pilares de la informaciòn en la empresa.

Mejoras despues de la implemenetaciòn del metodo

- Despues de la implementaciòn del metodo los servidores del active directory y file server ya cuentan con un respaldo de toda su informaciòn

- La infraestructura mejoro en cuanto a creaciòn de politicas de seguridad por usuario.
- Se crearon nuevas politicas de contraseñas para el personal de la empresa
- Todos los documentos fueron almacenados en los servidores y hicieron copias de seguridad de los datos
- Las carpetas en red fueron delimitados por cada usuario de la empresa
- Se crearon politicas de acceso mediante USB
- Se reestringio el acceso a la red a los proveedores
- Disminuyo la perdida de informaciòn de los datos del sistema
- Verificamos que los activos de la empresa se encuentra en ambientes adecuados

Se evaluo el metodo mediante una lista de cotejo que contenia las 3 dimensiones de la seguridad de la informaciòn las cuales eran confidenciabilidad, integridad, y disponibilidad, cada dimensiòn contenia indicadores que aportaron a tener una evaluaciòn eficaz acerca de como se encontraba la seguridad de los datos de la empresa, la lista de cotejo fue evaluado mediante “No cumple” ,”Cumple Parcialmente” “Si cumple”, lo cual nos ayudo a tener un resultado de como se encontraba la empresa.

La lista de cotejo de confidencialidad se evaluo con 6 indicadores , cada indicador contaba con 5 preguntas especificas para verificar los resultados de la implementaciòn del metodo.

La lista de cotejo de integridad se evaluo con 3 indicadores , cada indicador contaba con 5 preguntas especificas para verificar los resultados de la implementaciòn del metodo.

La lista de cotejo de disponibilidad se evaluo con 3 indicadores , cada indicador contaba con 5 preguntas especificas para verificar los resultados de la implementaciòn del metodo.

Finalmente se concluyo que el metodo implementado de seguridad de la información mediante servidor espejo con herramientas open source aumentaron

el nivel de confidencialidad, integridad y disponibilidad en gran eficacia lo cual nos muestra que la protección de los datos se encuentra en un porcentaje aceptable

UNIVERSIDAD CÉSAR VALLEJO

Anexo 03

Matriz de la lista de cotejos – pre test

N°	Preguntas																															
	Seguridad de la Información																															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
	Confidencialidad																															
1	3	2	3	1	1	3	1	1	3	1	1	2	2	3	1	1	1	3	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	2
2	3	3	3	3	3	3	1	1	3	2	1	2	2	3	1	1	1	3	1	1	2	1	1	1	1	2	3	2	1	1	1	1	1	2
3	3	2	3	1	1	3	1	1	1	1	1	2	2	3	1	1	1	3	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	2
4	3	1	3	1	1	3	1	1	1	1	1	2	2	3	1	1	1	3	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	2
5	1	1	3	1	1	3	1	1	1	1	1	2	2	3	1	1	1	2	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	2
6	3	1	2	1	1	3	1	1	1	1	1	2	2	3	1	1	1	3	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	2
7	1	1	3	1	1	1	1	1	1	1	1	2	2	3	1	1	1	2	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	2

N°	Preguntas												
	Seguridad de la Información												
	1	2	3	4	5	6	7	8	9	10	11	12	13
	Integridad												
1	2	2	1	1	1	1	2	1	1	1	1	2	1
2	2	2	2	2	1	1	2	2	2	1	1	2	1
3	2	1	1	1	1	1	2	1	1	1	1	2	1
4	2	1	1	1	1	1	2	1	1	1	1	2	1
5	2	1	1	1	1	1	2	1	1	1	1	2	1
6	2	1	1	1	1	1	2	1	1	1	1	2	1
7	2	1	1	1	1	1	2	1	1	1	1	2	1

N°	Preguntas												
	Seguridad de la Información												
	1	2	3	4	5	6	7	8	9	10	11	12	13
	Disponibilidad												
1	1	2	1	1	1	1	1	1	1	1	3	1	1
2	2	2	1	1	1	1	1	1	2	1	3	1	1
3	1	2	1	1	1	1	1	1	1	1	3	1	1
4	1	2	1	1	1	1	1	1	1	1	3	1	1
5	1	2	1	1	1	1	1	1	1	1	3	1	1
6	1	2	1	1	1	1	1	1	1	1	3	1	1
7	1	2	1	1	1	1	1	1	1	1	3	1	1

Matriz de la lista de cotejos – post test

N°	Preguntas																															
	Seguridad de la Información																															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
	Confidencialidad																															
1	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	2	3	3	2	3	3	3	3	3	3	3	2	3	3	3	3	3	3	2
2	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	2	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2
3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	2	3	3	2	3	3	3	3	3	3	3	2	3	3	3	3	3	3	2
4	3	3	3	3	3	3	3	3	3	3	2	3	3	3	2	2	3	3	2	3	3	3	3	3	3	3	2	2	3	3	3	3	3	2
5	3	3	3	3	3	3	2	3	3	3	2	3	3	3	3	2	3	3	2	3	3	3	3	3	3	3	2	3	3	3	3	3	3	2
6	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	2	3	3	2	3	3	3	3	3	3	3	2	3	3	3	3	3	3	2
7	3	3	3	3	3	2	2	3	3	3	2	3	3	3	2	2	3	3	2	3	3	3	3	3	3	3	2	2	3	3	3	3	3	2

N°	Preguntas												
	Seguridad de la Información												
	1	2	3	4	5	6	7	8	9	10	11	12	13
	Integridad												
1	3	3	3	3	2	3	3	3	3	3	3	3	3
2	3	3	3	3	2	3	3	3	3	3	3	3	3
3	3	3	3	3	2	3	3	3	3	3	3	3	3
4	3	3	3	3	2	3	3	3	3	2	2	3	2
5	3	3	3	3	2	3	3	3	3	3	3	3	3
6	3	3	3	3	2	3	3	3	3	3	3	3	3
7	3	3	3	3	2	3	3	3	3	2	2	3	2

N°	Preguntas												
	Seguridad de la Información												
	1	2	3	4	5	6	7	8	9	10	11	12	13
	Disponibilidad												
1	3	3	3	3	2	3	3	3	3	3	3	3	3
2	3	3	3	3	2	3	3	3	3	3	3	3	3
3	3	3	3	3	2	3	3	3	3	3	2	3	3
4	3	3	3	3	2	3	3	3	3	3	2	3	3
5	3	3	3	3	2	3	3	3	3	3	2	3	3
6	3	3	3	3	2	3	3	3	3	3	3	3	3
7	3	3	3	3	2	3	3	3	3	3	2	3	3

UNIVERSIDAD CÉSAR VALLEJO

Instrumento de Medición: Seguridad de Información para NEW FASHION PERÚ S.A.

Lista de Cotejo

El presente cuestionario, tiene por finalidad obtener información sobre la Seguridad de Información de la empresa New Fashion Perú S.A. Este instrumento es anónimo y los resultados obtenidos son de uso exclusivo para la investigación.

A continuación, se presenta las preguntas, que se responderán mediante la observación en las diferentes áreas de la empresa.

Nivel de cumplimiento:	
3	Si cumple
2	Cumple Parcialmente
1	No cumple

Área:					**Fecha:**	
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple						
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la compañía.						
Elaboración: Propia						

LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA						
PREGUNTAS		**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?					

P.1.2	¿El área cuenta con políticas de seguridad en el servidor?					
P.1.3	¿El área establece controles de acceso a la información de los datos?					
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?					
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?					
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?					
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?					
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?					
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?					
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?					
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?					
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?					
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?					

P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?					
P.1.15	¿El área asegura que la distribución de los documentos sea segura?					
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?					
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?					
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?					
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?					
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?					
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?					
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?					
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?					
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?					
	Gestión de Fugas de Información					

P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?					
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?					
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?					
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?					
P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?					
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?					
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?					
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?					
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?					
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?					

UNIVERSIDAD CÉSAR VALLEJO

LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA COMPAÑÍA						
PREGUNTAS		NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?					
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?					
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?					
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?					
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?					
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?					
P.2.7	¿El área de TI realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?					
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?					

P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?					
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?					
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?					
P.2.12	¿El área cumple en guardar los documentos en la red?					
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?					

LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA COMPAÑÍA						
PREGUNTAS		**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?					
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?					

P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?					
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?					
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?					
	Incidentes en la disponibilidad de la información					
P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?					
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?					
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?					
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?					
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?					
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la					

	disponibilidad de la información en la empresa?					
P.3.12	¿El área cuenta con un buen orden de sus documentos que se almacenan en sus servidores?					
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?					

Anexo 04: Carta de conformidad

NEW FASHION PERÚ S.A.

"Año del Fortalecimiento de la Soberanía Nacional"

Señores:

Laymito Lozano Jesús Martín
Ocampo Gutiérrez, Jhonattan Walter

Presente;
De nuestra consideración:

Sirva la presente para saludarle cordialmente y a la vez comunicarle que su solicitud de autorización para realizar su proyecto de investigación titulado "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES", ha sido aceptada por nuestra institución.

- Título del proyecto de investigación: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES".
- Objetivo: Determinar la efectividad de la implementación de un servidor espejo como solución para el respaldo de la información del servidor principal.

Es importante recordarles que deberán mantenerse la confidencialidad de la información, la cual es propiedad de NEW FASHION PERÚ, así como el compromiso de entregamos su proyecto final de investigación y comunicamos la fecha exacta de sustentación del mismo. Esperamos que su investigación sea de gran aporte para nuestra institución como para la comunidad. Sin otro particular, me despido.

Atentamente;

Lima, 30 de junio de 2022

RUBÉN FALLA CARBAJAL
Jefe de Producción

Anexo 05: Validación de Expertos

UNIVERSIDAD CÉSAR VALLEJO

CARTA DE PRESENTACIÓN

Mgtr. Nemias Saboya Rios

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante de la Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo, en la Filial Lima Norte, requiero su pronta ayuda para validar los instrumentos con los cuales recojo la información necesaria para poder desarrollar mi investigación.

El título de mi proyecto de investigación es: **Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación educativa.

El expediente de validación, que le hacemos llegar contiene documentos de:

Información general	Instrumento de uso del validador	Instrumentos a validar
- Carta de presentación. - Matriz de Operacionalización de las variables. - Matriz de consistencia. - Instrumentos a validar (3 fichas).	- Tabla de validación (1 por cada indicador) - Certificado de validez de contenido de los instrumentos.	Ficha de: 1. Lista de Cotejo sobre la dimensión de confiabilidad en seguridad de información 2. Lista de Cotejo sobre la dimensión de integridad en seguridad de información 3. Lista de Cotejo sobre la dimensión de disponibilidad en seguridad de información

Expresándole nuestros sentimientos de respeto y consideración nos despedimos de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

Ocampo Gutierrez Jhonattan Walter
DNI: 74087380

Laymito Lozano Jesús Martín
DNI: 08143412

UNIVERSIDAD CÉSAR VALLEJO

DEFINICIÓN CONCEPTUAL DE LAS VARIABLES Y DIMENSIONES

Variable Independiente: Servidor espejo

Un Servidor Espejo es la réplica de la información que tiene un servidor principal, su función es brindar seguridad a los datos que tiene una organización respaldándolo en otro servidor. Esta réplica nos ayuda a proteger los datos o base de datos que existe en los servidores de una empresa, ya que mantiene una alta disponibilidad de la seguridad de información que se manejan en las PyMES. (Hillmann et al., 2016)

Variable Dependiente: Seguridad de información

La finalidad en la seguridad de la información, es un concepto de medidas preventivas que ayudan a resguardar los datos de los sistemas en las organizaciones. (Juan A. Figueroa-Suárez. (Juan A. Figueroa-Suárez, n.d., 2018)

Dimensión: Confidencialidad

La confidencialidad busca prevenir el acceso a la información de forma controlada, es un principio fundamental que la información tenga un nivel de tratamiento que prevenga su divulgación no autorizada. La disponibilidad informática es la característica de proteger la fiabilidad y el acceso a los datos y recursos que maneja una organización. (Hernández, 2018)

Dimensión: Integridad

La integridad de la información garantiza la seguridad de los datos transportados o almacenados, asegurando que no haya ninguna alteración, pérdida o destrucción de la información ya sea de forma intencionada o accidental. (Colonia, P., 2019)

Dimensión: Disponibilidad

La disponibilidad es una característica que brinda una fiabilidad en los datos y accesos oportunos por parte de los usuarios autorizados, la disponibilidad asegura que se pueda recuperar la información en el momento que se necesite evitando su bloqueo o pérdida, y pueda ser utilizado solamente por personas autorizadas en el momento que sea requerido. (Quiroz S. & Macías, 2017).

UNIVERSIDAD CÉSAR VALLEJO

Matriz de Operacionalización de variable

TITULO: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES"

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	DATOS	INSTRUMENTO
Seguridad de información	La finalidad en la seguridad de la información es un concepto de medidas preventivas que ayudan a resguardar los datos de los sistemas en las organizaciones (Juan A. Figueroa-Suárez, n.d 2018))	Esta variable utilizará la técnica de observación y el instrumento de lista de cotejo para determinar las dimensiones de los pilares de la seguridad de la información, que son la confidencialidad, integridad y disponibilidad.	Confidencialidad	Incidentes de acceso indebido a los documentos.	Incidentes de acceso indebido.	Observación Lista de Cotejo
				Control de documentos	Accesos indebidos a los documentos	
				Contraseñas	Claves de seguridad	
				Seguridad de datos	Datos controlados	
				Fugas de información	Equipos portátiles.	
				Soporte de los datos de información	Soportes deinformación.	
			Integridad	Incidentes en la integridad de los documentos	Incidentes de impacto a la integridad más comunes	Observación Lista de Cotejo
				Frecuencia de incidentes en la integridad de los datos de información	Incidentes de impacto enla integridad.	
				Integridad de documentos y control.	Documentos y controlde versiones.	
			Disponibilidad	Seguridad Física y del entorno	Disponibilidad de los activos	Observación Lista de Cotejo
				Incidentes en la disponibilidad de la información	Disponibilidad de documentos comunes	
				Disponibilidad de servicios de información	Vectores de pérdida de disponibilidad de información.	

UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTOS A VALIDAR

A continuación, se presentan los instrumentos que deberá revisar para su respectiva validación. Estos se encuentran reflejados en la matriz de consistencia y se mencionan a continuación.

Ficha de:

1. Lista de Cotejo sobre la dimensión de confiabilidad en seguridad de información
2. Lista de Cotejo sobre la dimensión de integridad en seguridad de información
3. Lista de Cotejo sobre la dimensión de disponibilidad en seguridad de información

UNIVERSIDAD CÉSAR VALLEJO

1. Lista de Cotejo: Confidencialidad de la Información

Instrucciones: La lista de cotejo se evaluará mediante indicadores de la Norma ISO 27001. Así mismo la evaluación se hará en la empresa

EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN		
SEGURIDAD DE INFORMACIÓN DE LAS PYMES - ISO 27001		
Área:	**Fecha:**	
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la compañía.		
Elaboración: Propia		

LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA							
PREGUNTAS		NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?					
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?					
P.1.3	¿El área establece controles de acceso a la información de los datos?					
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?					
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?					
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?					
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?					
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?					

P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?					
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?					
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?					
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?					
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?					
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?					
P.1.15	¿El área asegura que la distribución de los documentos sea segura?					
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?					
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?					
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?					
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?					
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?					
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?					
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?					
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?					

P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?					
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?					
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?					
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?					
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?					
P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?					
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?					
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?					
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?					
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?					
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?					

UNIVERSIDAD CÉSAR VALLEJO

2. Lista de Cotejo: Integridad de la Información

Instrucciones: La lista de cotejo se evaluará mediante indicadores de la Norma ISO 27001. Así mismo la evaluación se hará en la empresa

EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN			
SEGURIDAD DE INFORMACIÓN DE LAS PYMES - ISO 27001			
Área:		**Fecha:**	
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple			
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la compañía.			
Elaboración: Propia			

LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA COMPAÑÍA							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?					
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?					
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?					
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?					
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?					
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?					
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?					

P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?					
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?					
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?					
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?					
P.2.12	¿El área cumple en guardar los documentos en la red?					
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?					

UNIVERSIDAD CÉSAR VALLEJO

3. Lista de Cotejo: Disponibilidad de la Información

Instrucciones: La lista de cotejo se evaluará mediante indicadores de la Norma ISO 27001. Así mismo la evaluación se hará en la empresa

EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN		
SEGURIDAD DE INFORMACIÓN DE LAS PYMES - ISO 27001		
Área:	**Fecha:**	
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la compañía.		
Elaboración: Propia		

LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA COMPAÑÍA							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?					
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?					
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?					
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?					
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?					
	Incidentes en la disponibilidad de la información					
P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?					

P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?					
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?					
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?					
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?					
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?					
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?					
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?					

UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTOS DE USO PARA EL EXPERTO

A continuación, se presentan los instrumentos que deberá utilizar para validar la lista de cotejo utilizadas en este estudio. Estos instrumentos ya se encuentran clasificados por cada indicador y a continuación se muestra la lista de los instrumentos por completar y enviar al investigador.

Tabla de validación para el experto:

1. Lista de Cotejo sobre la dimensión de confiabilidad en seguridad de información
2. Lista de Cotejo sobre la dimensión de integridad en seguridad de información
3. Lista de Cotejo sobre la dimensión de disponibilidad en seguridad de información

UNIVERSIDAD CÉSAR VALLEJO

1. TABLA DE VALIDACIÓN PARA EL EXPERTO: LISTA DE COTEJO SOBRE LA DIMENSIÓN DE CONFIABILIDAD EN SEGURIDAD DE INFORMACIÓN

TESIS: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES"	**Fecha** 15/07/2022

Instrucciones: Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71 -80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100% **(colocar el puntaje porcentual en el cuadro que considere)**. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

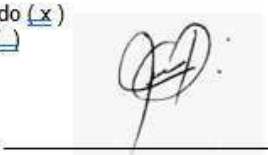
I. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
1. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
4. Organización	Existe una organización lógica.					X
5. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
6. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
7. Consistencia	Está basado en aspectos teóricos y científicos.					X
8. Coherencia	En los datos respecto al indicador.					X
9. Metodología	Responde al propósito de investigación.					X
10. Pertenencia	El instrumento es adecuado al tipo de investigación.					X
	Promedio Total	98				
	Sugerencias					

II. OPCIÓN DE APLICABILIDAD

El instrumento puede ser aplicado, tal como está elaborado (x)
El instrumento debe ser mejorado antes de ser aplicado ( )

III. FIRMA DEL EXPERTO



Mgtr. Nemias Saboya Ríos

UNIVERSIDAD CÉSAR VALLEJO

2. TABLA DE VALIDACIÓN PARA EL EXPERTO LISTA DE COTEJO SOBRE LA DIMENSIÓN DE INTEGRIDAD EN SEGURIDAD DE INFORMACIÓN

TESIS: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES"	**Fecha** 15/07/2022

Instrucciones: Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71 -80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100% **(colocar el puntaje porcentual en el cuadro que considere)**. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

I. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
1. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
4. Organización	Existe una organización lógica.					X
5. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
6. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
7. Consistencia	Está basado en aspectos teóricos y científicos.					X
8. Coherencia	En los datos respecto al indicador.					X
9. Metodología	Responde al propósito de investigación.					X
10. Pertenencia	El instrumento es adecuado al tipo de investigación.					X
	Promedio Total	98				
	Sugerencias					

II. OPCIÓN DE APLICABILIDAD

El instrumento puede ser aplicado, tal como está elaborado (x)
El instrumento debe ser mejorado antes de ser aplicado ( )

III. FIRMA DEL EXPERTO

Mgtr. Nemias Saboya Ríos

UNIVERSIDAD CÉSAR VALLEJO

3. TABLA DE VALIDACIÓN PARA EL EXPERTO: LISTA DE COTEJO SOBRE LA DIMENSIÓN DE DISPONIBILIDAD EN SEGURIDAD DE INFORMACIÓN

TESIS: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES"	**Fecha** 15/07/2022

Instrucciones: Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71 -80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100% **(colocar el puntaje porcentual en el cuadro que considere)**. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

I. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
1. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
4. Organización	Existe una organización lógica.					X
5. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
6. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
7. Consistencia	Está basado en aspectos teóricos y científicos.					X
8. Coherencia	En los datos respecto al indicador.					X
9. Metodología	Responde al propósito de investigación.					X
10. PERTENENCIA	El instrumento es adecuado al tipo de investigación.					X
	Promedio Total	98				
	Sugerencias					

II. OPCIÓN DE APLICABILIDAD

El instrumento puede ser aplicado, tal como está elaborado (x)
El instrumento debe ser mejorado antes de ser aplicado ( )

III. FIRMA DEL EXPERTO

Mgtr. Nemias Saboya Ríos

UNIVERSIDAD CÉSAR VALLEJO

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	INDICADOR: Lista de Cotejo sobre la dimensión de confiabilidad en seguridad de información	Si	No	Si	No	Si	No	
1		X		X		X		
	INDICADOR: Lista de Cotejo sobre la dimensión de integridad en seguridad de información	Si	No	Si	No	Si	No	
2		X		X		X		
	INDICADOR: Lista de Cotejo sobre la dimensión de disponibilidad en seguridad de información	Si	No	Si	No	Si	No	
3		X		X		X		

Observaciones (precisar si hay suficiencia): ---

Opinión de aplicabilidad: Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]

Especialidad del validador:

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

15 de julio del 2022

Mgtr. Nemias Saboya Ríos

DNI: 42001721

UNIVERSIDAD CÉSAR VALLEJO

1. Lista de Cotejo sobre la dimensión de confiabilidad en seguridad de información
2. Lista de Cotejo sobre la dimensión de integridad en seguridad de información
3. Lista de Cotejo sobre la dimensión de disponibilidad en seguridad de información

UNIVERSIDAD CÉSAR VALLEJO

INTRUMENTO DE VALIDEZ DE CONTENIDO DE LA PROPUESTA DE INGENIERIA

TESIS: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES"	Fecha 15/07/2022

ESCALA DE EVALUACIÓN
MUY MALO (1) MALO (2) REGULAR (3) BUENO (4) EXCELENTE (5)

Mediante la evaluación de expertos usted tiene la facultad de calificar el instrumento para validar la propuesta tecnológica utilizando la tabla de validación del instrumento. Esta tabla presenta escalas del 1 al 5 con su respectivo indicador de evaluación, se exhorta calificar de acuerdo a lo que Ud. considera como experto. Y proceda a realizar la sumatorias de los valores para establecer su validación.

I. ASPECTOS DE VALIDACIÓN

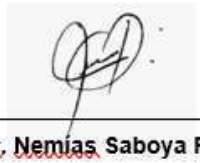
		VALORACIÓN				
INDICADOR	CRITERIO	1	2	3	4	5
1. Claridad	Es formulado con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Organización	Esta organizado considerando las dimensiones e indicadores					X
4. Suficiencia	Las preguntas por dimensión consideran que son suficientes					X
5. Intencionalidad	Adecuado para valorar los aspectos del desarrollo de la aplicación presentada en la investigación.					X
6. Consistencia	Se encuentra basado en aspectos teóricos y científicos.					X
7. Coherencia	Las preguntas están relacionadas al indicador.					X
8. Metodología	Responde al propósito de evaluación del producto tecnológico para investigación.					X
9. Pertenencia	El instrumento es adecuado al tipo de usuario al cual será aplicado.					X
	TOTAL	98				

	Sugerencias	

II. OPCIÓN DE APLICABILIDAD

El instrumento puede ser aplicado, tal como está elaborado (x)
El instrumento debe ser mejorado antes de ser aplicado ( )

III. FIRMA DEL EXPERTO



Mgtr. Nemias Saboya Ríos

UNIVERSIDAD CÉSAR VALLEJO

UNIVERSIDAD CÉSAR VALLEJO

CARTA DE PRESENTACIÓN

Mgtr. Yohan Alarcón Cajas

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante de la Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo, en la Filial Lima Norte, requiero su pronta ayuda para validar los instrumentos con los cuales recojo la información necesaria para poder desarrollar mi investigación.

El título de mi proyecto de investigación es: **Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación educativa.

El expediente de validación, que le hacemos llegar contiene documentos de:

Información general	Instrumento de uso del validador	Instrumentos a validar
- Carta de presentación. - Matriz de Operacionalización de las variables. - Matriz de consistencia. - Instrumentos a validar (3 fichas).	- Tabla de validación (1 por cada indicador) - Certificado de validez de contenido de los instrumentos.	Ficha de: 1. Lista de Cotejo sobre la dimensión de confiabilidad en seguridad de información 2. Lista de Cotejo sobre la dimensión de integridad en seguridad de información 3. Lista de Cotejo sobre la dimensión de disponibilidad en seguridad de información

Expresándole nuestros sentimientos de respeto y consideración nos despedimos de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

Ocampo Gutierrez Jhonattan Walter
DNI: 74087380

Laymito Lozano Jesús Martín
DNI: 08143412

UNIVERSIDAD CÉSAR VALLEJO

DEFINICIÓN CONCEPTUAL DE LAS VARIABLES Y DIMENSIONES

Variable Independiente: Servidor espejo

Un Servidor Espejo es la réplica de la información que tiene un servidor principal, su función es brindar seguridad a los datos que tiene una organización respaldándolo en otro servidor. Esta réplica nos ayuda a proteger los datos o base de datos que existe en los servidores de una empresa, ya que mantiene una alta disponibilidad de la seguridad de información que se manejan en las PyMES. (Hillmann et al., 2016)

Variable Dependiente: Seguridad de información

La finalidad en la seguridad de la información, es un concepto de medidas preventivas que ayudan a resguardar los datos de los sistemas en las organizaciones. (Juan A. Figueroa-Suárez, n.d., 2018)

Dimensión: Confidencialidad

La confidencialidad busca prevenir el acceso a la información de forma controlada, es un principio fundamental que la información tenga un nivel de tratamiento que prevenga su divulgación no autorizada. La disponibilidad informática es la característica de proteger la fiabilidad y el acceso a los datos y recursos que maneja una organización. (Hernández, 2018)

Dimensión: Integridad

La integridad de la información garantiza la seguridad de los datos transportados o almacenados, asegurando que no haya ninguna alteración, pérdida o destrucción de la información ya sea de forma intencionada o accidental. (Colonia, P., 2019)

Dimensión: Disponibilidad

La disponibilidad es una característica que brinda una fiabilidad en los datos y accesos oportunos por parte de los usuarios autorizados, la disponibilidad asegura que se pueda recuperar la información en el momento que se necesite evitando su bloqueo o pérdida, y pueda ser utilizado solamente por personas autorizadas en el momento que sea requerido. (Quiroz S. & Macías, 2017).

UNIVERSIDAD CÉSAR VALLEJO

Matriz de Operacionalización de variable

TITULO: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES"

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	DATOS	INSTRUMENTO
Seguridad de información	La finalidad en la seguridad de la información es un concepto de medidas preventivas que ayudan a resguardar los datos de los sistemas en las organizaciones (Juan A. Figueroa-Suárez, n.d 2018))	Esta variable utilizará la técnica de observación y el instrumento de lista de cotejo para determinar las dimensiones de los pilares de la seguridad de la información, que son la confidencialidad, integridad y disponibilidad.	Confidencialidad	Incidentes de acceso indebido a los documentos.	Incidentes de acceso indebido.	Observación Lista de Cotejo
				Control de documentos	Accesos indebidos a los documentos	
				Contraseñas	Claves de seguridad	
				Seguridad de datos	Datos controlados	
				Fugas de información	Equipos portátiles.	
				Soporte de los datos de información	Soportes deinformación.	
			Integridad	Incidentes en la integridad de los documentos	Incidentes de impacto a la integridad más comunes	Observación Lista de Cotejo
				Frecuencia de incidentes en la integridad de los datos de información	Incidentes de impacto enla integridad.	
				Integridad de documentos y control.	Documentos y controlde versiones.	
			Disponibilidad	Seguridad Física y del entorno	Disponibilidad de los activos	Observación Lista de Cotejo
				Incidentes en la disponibilidad de la información	Disponibilidad de documentos comunes	
				Disponibilidad de servicios de información	Vectores de pérdida de disponibilidad de información.	

UNIVERSIDAD CÉSAR VALLEJO

MATRIZ DE CONSISTENCIA

TITULO: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES"

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES	METODOS Y TECNICAS DE INVESTIGACION
PROBLEMA GENERAL ¿Cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source para PyMES? **PROBLEMAS ESPECÍFICOS** ¿Cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source en la **confidencialidad** de la seguridad de información para PyMES? ¿Cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source en la **integridad** de la seguridad de información para PyMES? ¿Cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source en la **disponibilidad** de la seguridad de información para PyMES?	**OBJETIVO GENERAL** Determinar cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source para pymes. **OBJETIVOS ESPECÍFICOS** **O1:** Determinar cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source en la confidencialidad de la seguridad de información para pymes **O2:** Determinar cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source en la integridad de la seguridad de información para pymes **O3:** Determinar cómo influye el método de seguridad de información basado en tecnología de servidores espejos en la nube con herramientas Open Source en la disponibilidad de la seguridad de información para pymes	**HIPÓTESIS GENERAL** El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source influye en la seguridad de información para PyMES **HIPÓTESIS ESPECÍFICOS** **H1:** El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source influye en la **confidencialidad** de la seguridad de información en las PyMES **H2**: El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source influye en la **integridad** de la seguridad de información en las PyMES **H3**: El método de seguridad de información basado en tecnología de Servidores Espejos en la nube con herramientas Open Source influye en la **disponibilidad** de la seguridad de información en las PyMES	**VARIABLE INDEPENDIENTE:** El método basado en tecnología de servidores espejo en la nube **VARIABLE DEPENDIENTE:** Seguridad de información **Indicadores:** **D1.** Confidencialidad - Gestión Incidentes de acceso indebido a los documentos. - Control de documentos. - Gestión de Contraseñas. - Gestión de Seguridad de datos. - Gestión de Fugas de información. -soportes de los datos de información. **D2.** Integridad - Incidentes en la integridad de los documentos. -Frecuencia de incidentes en la integridad de los datos de información. -Integridad de documentos y control. **D3.** Disponibilidad -Seguridad Física y del entorno -Incidentes en la disponibilidad de la información - Disponibilidad de servicios de información.	Métodos: Diseño: Aplicativo, Pre Experimental GE: 01 x 02 Donde: G.E. Estudiantes de la empresa New Fashion 01: Implementación de un servidor espejo usando herramientas open source en la nube (pre test). X: Implementación del servidor espejo 02: Implementación de un servidor espejo usando herramientas open source en la nube (Post test) Técnicas e Instrumentos de recolección de datos • Observación • Lista de cotejo

UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTOS A VALIDAR

A continuación, se presentan los instrumentos que deberá revisar para su respectiva validación. Estos se encuentran reflejados en la matriz de consistencia y se mencionan a continuación.

Ficha de:

1. Lista de Cotejo sobre la dimensión de confiabilidad en seguridad de información
2. Lista de Cotejo sobre la dimensión de integridad en seguridad de información
3. Lista de Cotejo sobre la dimensión de disponibilidad en seguridad de información

UNIVERSIDAD CÉSAR VALLEJO

1. Lista de Cotejo: Confidencialidad de la Información

Instrucciones: La lista de cotejo se evaluará mediante indicadores de la Norma ISO 27001. Así mismo la evaluación se hará en la empresa

EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN		
SEGURIDAD DE INFORMACIÓN DE LAS PYMES - ISO 27001		
Área:	**Fecha:**	
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la compañía.		
Elaboración: Propia		

LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?					
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?					
P.1.3	¿El área establece controles de acceso a la información de los datos?					
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?					
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?					
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?					
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?					
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?					

P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?					
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?					
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?					
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?					
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?					
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?					
P.1.15	¿El área asegura que la distribución de los documentos sea segura?					
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?					
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?					
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?					
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?					
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?					
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?					
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?					
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?					

P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?					
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?					
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?					
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?					
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?					
P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?					
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?					
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?					
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?					
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?					
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?					

UNIVERSIDAD CÉSAR VALLEJO

2. Lista de Cotejo: Integridad de la Información

Instrucciones: La lista de cotejo se evaluará mediante indicadores de la Norma ISO 27001. Así mismo la evaluación se hará en la empresa

EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN		
SEGURIDAD DE INFORMACIÓN DE LAS PYMES - ISO 27001		
Área:	**Fecha:**	
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la compañía.		
Elaboración: Propia		

LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA COMPAÑÍA							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?					
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?					
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?					
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?					
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?					
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?					
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?					

P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?					
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?					
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?					
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?					
P.2.12	¿El área cumple en guardar los documentos en la red?					
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?					

UNIVERSIDAD CÉSAR VALLEJO

3. Lista de Cotejo: Disponibilidad de la Información

Instrucciones: La lista de cotejo se evaluará mediante indicadores de la Norma ISO 27001. Así mismo la evaluación se hará en la empresa

EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN		
SEGURIDAD DE INFORMACIÓN DE LAS PYMES - ISO 27001		
Área:	**Fecha:**	
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la compañía.		
Elaboración: Propia		

LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA COMPAÑÍA							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?					
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?					
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?					
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?					
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?					
	Incidentes en la disponibilidad de la información					
P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?					

P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?					
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?					
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?					
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?					
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?					
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?					
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?					

UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTOS DE USO PARA EL EXPERTO

A continuación, se presentan los instrumentos que deberá utilizar para validar la lista de cotejo utilizadas en este estudio. Estos instrumentos ya se encuentran clasificados por cada indicador y a continuación se muestra la lista de los instrumentos por completar y enviar al investigador.

Tabla de validación para el experto:

1. Lista de Cotejo sobre la dimensión de confiabilidad en seguridad de información
2. Lista de Cotejo sobre la dimensión de integridad en seguridad de información
3. Lista de Cotejo sobre la dimensión de disponibilidad en seguridad de información

UNIVERSIDAD CÉSAR VALLEJO

I. TABLA DE VALIDACION PARA EL EXPERTO: LISTA DE COTEJO SOBRE LA DIMENSIÓN DE CONFIABILIDAD EN SEGURIDAD DE INFORMACIÓN

TESIS: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES"	Fecha 15/07/2022

Instrucciones: Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71 -80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100% **(colocar el puntaje porcentual en el cuadro que considere)**. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

I. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	CRITERIO	0-20%	21-50%	51-70%	71-80%	81-100%
1. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
4. Organización	Existe una organización lógica.					X
5. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
6. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
7. Consistencia	Está basado en aspectos teóricos y científicos.					X
8. Coherencia	En los datos respecto al indicador.					X
9. Metodología	Responde al propósito de investigación.					X
10. Pertenencia	El instrumento es adecuado al tipo de investigación.					X
	Promedio Total	96				
	Sugerencias					

II. OPCIÓN DE APLICABILIDAD

El instrumento puede ser aplicado, tal como está elaborado (x)
El instrumento debe ser mejorado antes de ser aplicado ( )

III. FIRMA DEL EXPERTO

Mgtr. Yohan Alarcón Cajas

UNIVERSIDAD CÉSAR VALLEJO

2. TABLA DE VALIDACIÓN PARA EL EXPERTO LISTA DE COTEJO SOBRE LA DIMENSIÓN DE INTEGRIDAD EN SEGURIDAD DE INFORMACIÓN

TESIS: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES"	Fecha 15/07/2022

Instrucciones: Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71 -80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100% **(colocar el puntaje porcentual en el cuadro que considere)**. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la

I. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	CRITERIO	0-20%	21-50%	51-70%	71-80%	81-100%
1. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
4. Organización	Existe una organización lógica.					X
5. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
6. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
7. Consistencia	Está basado en aspectos teóricos y científicos.					X
8. Coherencia	En los datos respecto al indicador.					X
9. Metodología	Responde al propósito de investigación.					X
10. Pertenencia	El instrumento es adecuado al tipo de investigación.					X
	Promedio Total	96				
	Sugerencias					

II. OPCIÓN DE APLICABILIDAD

coherencia de los indicadores para su valoración.

El instrumento puede ser aplicado, tal como está elaborado (x)
El instrumento debe ser mejorado antes de ser aplicado ( )

III. FIRMA DEL EXPERTO

Mgtr. Yohan Alarcón Cajas

UNIVERSIDAD CÉSAR VALLEJO

3. TABLA DE VALIDACIÓN PARA EL EXPERTO: LISTA DE COTEJO SOBRE LA DIMENSIÓN DE DISPONIBILIDAD EN SEGURIDAD DE INFORMACIÓN

TESIS: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES"	Fecha 15/07/2022

Instrucciones: Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71 -80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100% **(colocar el puntaje porcentual en el cuadro que considere)**. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la

I. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	CRITERIO	0-20%	21-50%	51-70%	71-80%	81-100%
1. Claridad	La ficha de observación es formulada con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Actualidad	Es adecuado el avance, la ciencia y tecnología.					X
4. Organización	Existe una organización lógica.					X
5. Suficiencia	Comprende los aspectos de cantidad y calidad.					X
6. Intencionalidad	Adecuado para valorar los aspectos del sistema metodológico y científico.					X
7. Consistencia	Está basado en aspectos teóricos y científicos.					X
8. Coherencia	En los datos respecto al indicador.					X
9. Metodología	Responde al propósito de investigación.					X
10. PERTENENCIA	El instrumento es adecuado al tipo de investigación.					X
	Promedio Total	96				
	Sugerencias					

II. OPCIÓN DE APLICABILIDAD

coherencia de los indicadores para su valoración.

El instrumento puede ser aplicado, tal como está elaborado (x)
El instrumento debe ser mejorado antes de ser aplicado ( )

III. FIRMA DEL EXPERTO

Mgtr. Yohan Alarcón Cajas

UNIVERSIDAD CÉSAR VALLEJO

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	INDICADOR: Lista de Cotejo sobre la dimensión de confiabilidad en seguridad de información	Si	No	Si	No	Si	No	
1		X		X		X		
	INDICADOR: Lista de Cotejo sobre la dimensión de integridad en seguridad de información	Si	No	Si	No	Si	No	
2		X		X		X		
	INDICADOR: Lista de Cotejo sobre la dimensión de disponibilidad en seguridad de información	Si	No	Si	No	Si	No	
3		X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Especialidad del validador:

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

15 de julio del 2022

Mgtr. Yohan Alarcón Cajas
DNI: 46189705

UNIVERSIDAD CÉSAR VALLEJO

1. Lista de Cotejo sobre la dimensión de confiabilidad en seguridad de información
2. Lista de Cotejo sobre la dimensión de integridad en seguridad de información
3. Lista de Cotejo sobre la dimensión de disponibilidad en seguridad de información

UNIVERSIDAD CÉSAR VALLEJO

UNIVERSIDAD CÉSAR VALLEJO

INTRUMENTO DE VALIDEZ DE CONTENIDO DE LA PROPUESTA DE INGENIERIA

TESIS: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES"	Fecha 15/07/2022

ESCALA DE EVALUACIÓN

MUY MALO (1) MALO (2) REGULAR (3) BUENO (4) EXCELENTE (5)

Mediante la evaluación de expertos usted tiene la facultad de calificar el instrumento para validar la propuesta tecnológica utilizando la tabla de validación del instrumento. Esta tabla presenta escalas del 1 al 5 con su respectivo indicador de evaluación, se exhorta calificar de acuerdo a lo que Ud. considera como experto. Y proceda a realizar la sumatorias de los valores para establecer su validación.

I. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	CRITERIO	1	2	3	4	5
1. Claridad	Es formulado con lenguaje apropiado.					X
2. Objetividad	Está expresado en conducta observable.					X
3. Organización	Esta organizado considerando las dimensiones e indicadores					X
4. Suficiencia	Las preguntas por dimensión consideran que son suficientes					X
5. Intencionalidad	Adecuado para valorar los aspectos del desarrollo de la aplicación presentada en la investigación.					X
6. Consistencia	Se encuentra basado en aspectos teóricos y científicos.					X
7. Coherencia	Las preguntas están relacionadas al indicador.					X
8. Metodología	Responde al propósito de evaluación del producto tecnológico para investigación.					X
9. Pertenencia	El instrumento es adecuado al tipo de usuario al cual será aplicado.					X
	TOTAL	96				

	Sugerencias	

II. OPCIÓN DE APLICABILIDAD

El instrumento puede ser aplicado, tal como está elaborado (x)
El instrumento debe ser mejorado antes de ser aplicado ( )

III. FIRMA DEL EXPERTO

Mgtr. Yohan Alarcón Cajas

UNIVERSIDAD CÉSAR VALLEJO

ANEXO: CARTA DE APLICABILIDAD

Ate, 24 de noviembre de 2022

Director(a) de la escuela de Ingeniería Sistemas

Universidad César Vallejo - Sede Lima Norte

AUTORIZACIÓN PARA LA REALIZACIÓN Y DIFUSIÓN DE RESULTADOS DE LA INVESTIGACIÓN

Por medio del presente documento, Yo CLEMENTE GUEVARA SALVATIERRA identificado con DNI Nº 10610787, teniendo como número de contacto 993140682, y siendo el representante legal de NEW FASHION PERÚ S.A., autorizo a LAYMITO LOZANO JESÚS MARTÍN Y OCAMPO GUTIERREZ JHONATTAN WALTER identificados con los DNI Nº 08143412 y 74087380 a realizar la investigación titulada "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES" y a difundir los resultados de la investigación utilizando el nombre de NEW FASHION PERÚ S.A.

Atentamente.

New Fashion Perú S.A.
CLEMENTE GUEVARA S.
GERENTE GENERAL

UNIVERSIDAD CÉSAR VALLEJO

ANEXO: LISTAS DE COTEJO
GERENCIA (PRE TEST)

Área: GERENCIA	Fecha:	10-10-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME		
Elaboración: Propia		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?	X				
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?		X			
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?			X		
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?			X		
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?	X				
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?			X		
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?			X		
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?	X				
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?			X		
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?			X		
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?		X			
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?		X			
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?			X		
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?			X		
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?			X		
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?	X				
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?			X		
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?			X		
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?		X			
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?			X		
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?			X		
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?			X		
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?			X		
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?		X			
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?			X		

P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?		X			
P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?			X		
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?			X		
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?			X		
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?			X		
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?			X		
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	2	1		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?		X			
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?		X			
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?			X		
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?			X		
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?			X		
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?			X		
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?		X			
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?			X		
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?			X		
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?			X		
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?			X		
P.2.12	¿El área cumple en guardar los documentos en la red?		X			
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?			X		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	2	1		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?			X		
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?		X			
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?			X		
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?			X		

P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?			X		
	Incidentes en la disponibilidad de la información					
P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?			X		
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?			X		
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?			X		
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?			X		
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?			X		
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?	X				
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?			X		
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?			X		

UNIVERSIDAD CÉSAR VALLEJO

SISTEMAS (PRE TEST)

Área: T.I	Fecha:	16-10-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME		
Elaboración: Propia		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME

	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?	X				
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?	X				
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?	X				
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?	X				
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?	X				
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?			X		
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?			X		
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?	X				
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?		X			
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?			X		
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?		X			
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?		X			
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?			X		
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?			X		
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?			X		
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?	X				
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?			X		
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?			X		
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?		X			
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?			X		
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?			X		
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?			X		
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?			X		
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?		X			
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?	X				
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?		X			

P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?			X		
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?			X		
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?			X		
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?			X		
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?			X		
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	2	1		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?		X			
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?		X			
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?		X			
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?		X			
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?			X		
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?			X		
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?		X			
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?		X			
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?		X			
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?			X		
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?			X		
P.2.12	¿El área cumple en guardar los documentos en la red?		X			
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?			X		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	2	1		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?		X			
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?		X			
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?			X		
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?			X		
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?			X		
	Incidentes en la disponibilidad de la información					

P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?			X		
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?			X		
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?			X		
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?		X			
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?			X		
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?	X				
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?			X		
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?			X		

JEFE DE PRODUCCIÓN V°B° NFP

UNIVERSIDAD CÉSAR VALLEJO

RR. HH (PRE-TEST)

Área: RR.HH	Fecha:	10-10-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME		
Elaboración: Propia		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME

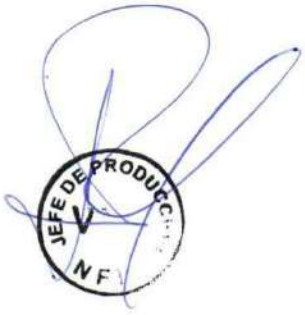
	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?	X				
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?		X			
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?			X		
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?			X		
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?	X				
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?			X		
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?			X		
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?			X		
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?			X		
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?			X		
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?		X			
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?		X			
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?			X		
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?			X		
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?			X		
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?	X				
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?			X		
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?			X		
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?		X			
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?			X		
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?			X		
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?			X		
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?			X		
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?		X			
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?			X		
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?		X			
P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?			X		
	Soporte de los Datos de Información					

P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?			X		
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?			X		
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?			X		
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?			X		
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
PREGUNTAS		NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?		X			
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?			X		
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?			X		
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?			X		
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?			X		
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?			X		
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?		X			
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?			X		
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?			X		
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?			X		
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?			X		
P.2.12	¿El área cumple en guardar los documentos en la red?		X			
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?			X		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
PREGUNTAS		NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?			X		
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?		X			
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?			X		
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?			X		
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?			X		
	Incidentes en la disponibilidad de la información					
P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?			X		
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?			X		
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?			X		

P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?			X		
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?			X		
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?	X				
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?			X		
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?			X		



UNIVERSIDAD CÉSAR VALLEJO

LOGISTICA (PRE TEST)

Área: LOGÍSTICA	**Fecha:** 10-10-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple	
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME	
Elaboración: Propia	

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME

	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?	X				
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?			X		
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?			X		
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?			X		
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?	X				
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?			X		
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?			X		
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?			X		
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?			X		
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?			X		
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?		X			
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?		X			
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?			X		
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?			X		
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?			X		
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?	X				
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?			X		
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?			X		
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?		X			
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?			X		
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?			X		
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?			X		
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?			X		
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?		X			
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?			X		
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?		X			

P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?			X		
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?			X		
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?			X		
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?			X		
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?			X		
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	2	1		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?		X			
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?			X		
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?			X		
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?			X		
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?			X		
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?			X		
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?		X			
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?			X		
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?			X		
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?			X		
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?			X		
P.2.12	¿El área cumple en guardar los documentos en la red?		X			
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?			X		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	2	1		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?			X		
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?		X			
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?			X		
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?			X		
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?			X		
	Incidentes en la disponibilidad de la información					
P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?			X		

P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?			X		
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?			X		
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?			X		
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?			X		
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?	X				
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?			X		
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?			X		

UNIVERSIDAD CÉSAR VALLEJO

COMERCIAL (PRE TEST)

Área: COMERCIAL	Fecha:	10-10-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME		
Elaboración: Propia		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?			X		
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?			X		
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?			X		
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?			X		
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?	X				
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?			X		
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?			X		
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?			X		
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?			X		
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?			X		
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?		X			
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?		X			
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?			X		
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?			X		
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?			X		
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?		X			
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?			X		
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?			X		
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?		X			
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?			X		
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?			X		
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?			X		
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?			X		
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?		X			
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?			X		
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?		X			

P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?			X		
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?			X		
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?			X		
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?			X		
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?			X		
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
PREGUNTAS		**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?		X			
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?			X		
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?			X		
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?			X		
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?			X		
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?			X		
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?		X			
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?			X		
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?			X		
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?			X		
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?			X		
P.2.12	¿El área cumple en guardar los documentos en la red?		X			
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?			X		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
PREGUNTAS		**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?			X		
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?		X			
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?			X		
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?			X		
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?			X		
	Incidentes en la disponibilidad de la información					

P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?			X		
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?			X		
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?			X		
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?			X		
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?			X		
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?	X				
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?			X		
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?			X		

UNIVERSIDAD CÉSAR VALLEJO

FINANZAS (PRE TEST)

Área: FINANZAS	Fecha:	10-10-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME		
Elaboración: Propia		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME

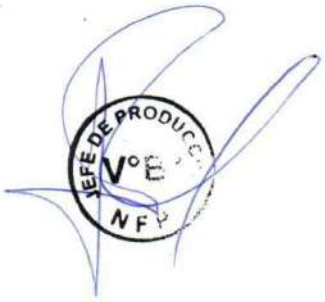
	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?	X				
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?			X		
P.1.3	¿El área establece controles de acceso a la información de los datos?		X			
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?			X		
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?			X		
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?	X				
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?			X		
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?			X		
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?			X		
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?			X		
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?			X		
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?		X			
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?		X			
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?			X		
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?			X		
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?			X		
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?	X				
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?			X		
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?			X		
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?		X			
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?			X		
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?			X		
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?			X		
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?			X		
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?		X			
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?			X		
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?		X			

P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?			X		
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?			X		
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?			X		
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?			X		
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?			X		
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	2	1		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?		X			
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?			X		
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?			X		
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?			X		
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?			X		
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?			X		
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?		X			
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?			X		
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?			X		
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?			X		
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?			X		
P.2.12	¿El área cumple en guardar los documentos en la red?		X			
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?			X		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	2	1		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?			X		
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?		X			
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?			X		
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?			X		
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?			X		
	Incidentes en la disponibilidad de la información					
P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?			X		
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?			X		

P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?			X		
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?			X		
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?			X		
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?	X				
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?			X		
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?			X		



UNIVERSIDAD CÉSAR VALLEJO

PRODUCCIÒN (PRE TEST)

Área: PRODUCCIÓN	Fecha:	10-10-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME		
Elaboración: Propia		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME

	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?			X		
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?			X		
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?			X		
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?			X		
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?			X		
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?			X		
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?			X		
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?			X		
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?			X		
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?			X		
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?		X			
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?		X			
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?			X		
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?			X		
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?			X		
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?		X			
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?			X		
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?			X		
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?		X			
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?			X		
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?			X		
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?			X		
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?			X		
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?		X			
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?			X		
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?		X			

P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?			X		
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?			X		
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?			X		
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?			X		
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?			X		
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	2	1		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?		X			
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?			X		
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?			X		
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?			X		
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?			X		
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?			X		
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?		X			
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?			X		
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?			X		
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?			X		
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?			X		
P.2.12	¿El área cumple en guardar los documentos en la red?		X			
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?			X		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	2	1		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?			X		
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?		X			
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?			X		
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?			X		
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?			X		
	Incidentes en la disponibilidad de la información					

P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?			X		
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?			X		
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?			X		
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?			X		
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?			X		
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?	X				
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?			X		
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?			X		

UNIVERSIDAD CÉSAR VALLEJO

ANEXO: LISTAS DE COTEJO

GERENCIA (POST TEST)

Área: GERENCIA	Fecha:	15-11-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME		
Elaboración: Propia		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?	X				
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?	X				
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?	X				
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?	X				
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?	X				
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?	X				
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?	X				
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?	X				
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?	X				
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?		X			
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?	X				
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?	X				
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?	X				
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?		X			
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?	X				
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?	X				
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?		X			
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?	X				
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?	X				
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?	X				
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?	X				
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?	X				
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?	X				
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?	X				
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?		X			

P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?	X				
P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?	X				
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?	X				
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?	X				
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?	X				
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?	X				
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?	X				
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?	X				
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?	X				
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?	X				
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?		X			
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?	X				
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?	X				
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?	X				
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?	X				
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?	X				
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?	X				
P.2.12	¿El área cumple en guardar los documentos en la red?	X				
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?	X				

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?	X				
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?	X				
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?	X				
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?	X				

P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?		X			
	Incidentes en la disponibilidad de la información					
P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?	X				
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?	X				
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?	X				
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?	X				
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?	X				
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?	X				
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?	X				
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?	X				

UNIVERSIDAD CÉSAR VALLEJO

SISTEMAS (POST TEST)

Área: T.I	**Fecha:** 15-11-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple	
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME	
Elaboración: Propia	

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME

	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?	X				
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?	X				
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?	X				
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?	X				
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?	X				
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?	X				
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?	X				
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?	X				
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?	X				
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?		X			
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?	X				
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?	X				
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?	X				
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?		X			
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?	X				
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?	X				
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?		X			
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?	X				
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?	X				
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?	X				
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?	X				
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?	X				
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?	X				
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?	X				
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?	X				
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?	X				

P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?	X				
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?	X				
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?	X				
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?	X				
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?	X				
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?	X				
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?	X				
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?	X				
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?	X				
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?		X			
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?	X				
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?	X				
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?	X				
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?	X				
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?	X				
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?	X				
P.2.12	¿El área cumple en guardar los documentos en la red?	X				
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?	X				

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?	X				
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?	X				
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?	X				
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?	X				
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?		X			
	Incidentes en la disponibilidad de la información					

P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?	X				
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?	X				
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?	X				
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?	X				
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?	X				
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?	X				
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?	X				
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?	X				

UNIVERSIDAD CÉSAR VALLEJO

RR. HH (POST TEST)

Área: RR.HH	**Fecha:** 15-11-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple	
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME	
Elaboración: Propia	

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME

	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?	X				
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?	X				
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?	X				
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?	X				
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?	X				
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?	X				
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?	X				
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?	X				
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?	X				
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?		X			
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?	X				
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?	X				
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?	X				
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?		X			
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?	X				
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?	X				
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?		X			
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?	X				
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?	X				
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?	X				
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?	X				
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?	X				
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?	X				
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?	X				
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?		X			
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?	X				
P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?	X				
	Soporte de los Datos de Información					

P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?	X				
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?	X				
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?	X				
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?	X				
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
PREGUNTAS		NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
2	**INTEGRIDAD**						
	Incidentes en la integridad de los documentos						
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?	X				
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?	X				
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?	X				
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?	X				
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?		X			
	Frecuencia de incidentes en la integridad de los datos de información						
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?	X				
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?	X				
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?	X				
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?	X				
	Integridad de documentos y control.						
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?	X				
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?	X				
P.2.12	¿El área cumple en guardar los documentos en la red?	X				
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?	X				

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
PREGUNTAS		NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
3	**DISPONIBILIDAD**						
	Seguridad física y del entorno.						
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?	X				
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?	X				
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?	X				
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?	X				
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?		X			
	Incidentes en la disponibilidad de la información						
P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?	X				
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?	X				
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?	X				

P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?	X				
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?	X				
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?		X			
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?	X				
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?	X				

LOGISTICA (POST TEST)

Área: LOGÍSTICA	**Fecha:** 15-11-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple	
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME	
Elaboración: Propia	

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME

	PREGUNTAS	NIVEL DE CUMPLIMIENTO 3	2	1	OBSERVACIONES	COMENTARIOS
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?	X				
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?	X				
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?	X				
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?	X				
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?	X				
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?	X				
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?	X				
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?	X				
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?	X				
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?		X			
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?	X				
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?	X				
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?		X			
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?		X			
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?	X				
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?	X				
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?		X			
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?	X				
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?	X				
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?	X				
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?	X				
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?	X				
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?	X				
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?	X				
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?		X			
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?		X			

P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?	X				
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?	X				
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?	X				
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?	X				
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?	X				
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?	X				
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?	X				
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?	X				
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?	X				
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?		X			
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?	X				
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?	X				
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?	X				
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?	X				
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?		X			
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?		X			
P.2.12	¿El área cumple en guardar los documentos en la red?	X				
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?	X				
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?	X				
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?	X				
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?	X				
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?		X			
	Incidentes en la disponibilidad de la información					
P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?	X				

P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?	X				
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?	X				
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?	X				
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?	X				
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?		X			
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?	X				
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?	X				

UNIVERSIDAD CÉSAR VALLEJO

COMERCIAL (POST TEST)

Área: COMERCIAL	**Fecha:** 15-11-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple	
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME	
Elaboración: Propia	

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME

	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?	X				
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?	X				
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?	X				
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?	X				
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?	X				
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?		X			
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?	X				
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?	X				
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?	X				
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?		X			
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?	X				
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?	X				
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?	X				
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?		X			
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?	X				
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?	X				
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?		X			
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?	X				
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?	X				
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?	X				
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?	X				
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?	X				
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?	X				
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?	X				
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?		X			
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?	X				

P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?	X				
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?	X				
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?	X				
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?	X				
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?	X				
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?	X				
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?	X				
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?	X				
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?	X				
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?		X			
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?	X				
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?	X				
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?	X				
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?	X				
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?	X				
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?	X				
P.2.12	¿El área cumple en guardar los documentos en la red?	X				
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?	X				

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?	X				
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?	X				
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?	X				
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?	X				
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?		X			
	Incidentes en la disponibilidad de la información					

P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?	X				
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?	X				
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?	X				
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?	X				
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?	X				
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?		X			
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?	X				
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?	X				

UNIVERSIDAD CÉSAR VALLEJO

FINANZAS (POST TEST)

Área: FINANZAS	Fecha:	15-11-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME		
Elaboración: Propia		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?	X				
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?	X				
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?	X				
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?	X				
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?	X				
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?	X				
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?	X				
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?	X				
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?	X				
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?		X			
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?	X				
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?	X				
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?	X				
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?		X			
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?	X				
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?	X				
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?		X			
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?	X				
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?	X				
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?	X				
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?	X				
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?	X				
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?	X				
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?	X				
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?		X			
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?	X				

P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?	X				
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?	X				
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?	X				
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?	X				
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?	X				
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?	X				
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?	X				
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?	X				
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?	X				
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?		X			
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?	X				
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?	X				
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?	X				
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?	X				
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?	X				
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?	X				
P.2.12	¿El área cumple en guardar los documentos en la red?	X				
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?	X				

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME							
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	**2**	**1**		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?	X				
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?	X				
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?	X				
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?	X				
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?		X			
	Incidentes en la disponibilidad de la información					
P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?	X				
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?	X				

P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?	X				
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?	X				
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?	X				
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?	X				
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?	X				
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?	X				

UNIVERSIDAD CÉSAR VALLEJO

PRODUCCIÒN (POST TEST)

Área: PRODUCCIÓN	Fecha:	15-11-22
Instrucciones: Marque con un aspa (X) la alternativa correcta. Nivel de Cumplimiento: (3) Si cumple (2) Cumple Parcialmente (1) No cumple		
Objetivo: Determinar los indicadores de seguridad de Confidencialidad, Integridad y Disponibilidad de la PYME		
Elaboración: Propia		

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME

	PREGUNTAS	NIVEL DE CUMPLIMIENTO			OBSERVACIONES	COMENTARIOS
		3	2	1		
1	**CONFIDENCIALIDAD**					
	Gestión de los incidentes de la seguridad de la información.					
P.1.1	¿El área cuenta con un lugar especializado, para mantener la seguridad de sus activos de información?	X				
P.1.2	¿El área cuenta con políticas de seguridad en el servidor?	X				
P.1.3	¿El área establece controles de acceso a la información de los datos?	X				
P.1.4	¿El área tiene conocimiento sobre las restricciones de acceso al servidor?	X				
P.1.5	¿El área cuenta con políticas de restricción de acceso a los distintos documentos en red?	X				
P.1.6	¿La empresa cuenta con licencias originales de los sistemas operativos?		X			
P.1.7	¿El área cuenta políticas de acceso a la red desde los equipos móviles de la organización?		X			
P.1.8	¿El área cuenta con políticas en seguridad de información, aprobada por la administración y comunica a todos los empleados de la organización?	X				
P.1.9	¿El área tiene conocimiento de no dejar material confidencial en forma impresa en sus oficinas de trabajo?	X				
P.1.10	¿El área cuenta con políticas o acuerdos de confidencialidad sobre la seguridad de la información?	X				
	Control de Documentos					
P.1.11	¿El área cumple con subir los documentos a la red?		X			
P.1.12	¿El área revisa y actualiza los documentos publicados en el file server?	X				
P.1.13	¿El área cuenta con versiones actualizadas de los documentos del sistema?	X				
P.1.14	¿El área asegura que la documentación sea legible y fácil de entender?	X				
P.1.15	¿El área asegura que la distribución de los documentos sea segura?		X			
	Gestión de Contraseñas					
P.1.16	¿El área asegura que sus claves son complejas y confidenciales?		X			
P.1.17	¿El área establece políticas de contraseña sobre la renovación de claves mensualmente?	X				
P.1.18	¿Los usuarios del área saben la importancia de no exponer las claves que usan para conectarse al sistema de la organización?	X				
P.1.19	¿Los usuarios cuentan con el conocimiento de que las claves no pueden contener: nombre, apellido y fecha de nacimiento?		X			
	Gestión de seguridad de datos					
P.1.20	¿El área tiene conocimiento del lugar donde se almacenan sus datos y quienes pueden acceder al contenido de estos?	X				
P.1.21	¿El área asegura que cada usuario solo tiene acceso a la carpeta de su área específica?	X				
P.1.22	¿El área realiza copias de seguridad de sus datos almacenados en el sistema?	X				
P.1.23	¿El área cuenta con equipos físicos que puedan resguardar la información de los datos almacenados en el servidor?	X				
P.1.24	¿El área cuenta con políticas de restricción sobre el borrado de los datos del sistema?	X				
	Gestión de Fugas de Información					
P.1.25	¿Los datos de información del área se encuentran vulnerados ante cualquier conexión no autorizada?	X				
P.1.26	¿Solo el personal autorizado tiene permiso de acceder a los equipos físicos del área?	X				
P.1.27	¿El área tiene conocimiento de que los proveedores contratados no deberían tener acceso al sistema?		X			
P.1.28	¿El área cuenta con un flujo eléctrico estabilizado que permite mantener los datos del sistema estables?		X			

P.1.29	¿El área de T.I limita el acceso de uso del USB a los empleados de la organización?	X				
	Soporte de los Datos de Información					
P.1.30	¿El área cuenta con un soporte especializado para proteger los activos de la información?	X				
P.1.31	¿El área de soporte realiza la copia de seguridad de los datos semanalmente?	X				
P.1.32	¿El área de soporte cuenta con una guía de clasificación de cómo se debe manejar la protección de los datos?	X				
P.1.33	¿El área cuenta con un sistema de control de acceso que ayuden a resguardar la información de los datos del sistema?	X				
P.1.34	¿La empresa cuenta con un sistema de control de temperatura, detección de humo y detección de humedad para prever cualquier daño físico de los activos de la organización?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	2	1		
2	**INTEGRIDAD**					
	Incidentes en la integridad de los documentos					
P.2.1	¿El área cuenta con el compromiso de preservar los datos de forma completa, confiable y consistente?	X				
P.2.2	¿El área tiene conocimiento de prever la integridad de los datos?	X				
P.2.3	¿El área garantiza que los datos almacenados se puedan encontrar y vincular con otros datos del sistema?	X				
P.2.4	¿El área garantiza que, ante una pérdida de información, se pueda recuperar todos los documentos?	X				
P.2.5	¿El área cuenta con una planificación de seguridad empresarial?		X			
	Frecuencia de incidentes en la integridad de los datos de información					
P.2.6	¿El área cuenta con un nivel de incidencia que está monitoreado por un especialista en la integridad de los datos?	X				
P.2.7	¿El área de T.I realiza un monitoreo constante de las incidencias de impacto en la integridad de los datos?	X				
P.2.8	¿El área cuenta con políticas de procedimientos de gestión de incidencias en la integridad de los datos?	X				
P.2.9	¿El área toma medidas preventivas ante cualquier eventualidad que pudiera ocurrir sobre la seguridad de la información?	X				
	Integridad de documentos y control.					
P.2.10	¿El área cuenta con políticas y procedimientos ante algún incidente generado con los datos de la empresa?		X			
P.2.11	¿El área cuenta con un método de seguridad ante algún incidente generado contra la integridad de la información?		X			
P.2.12	¿El área cumple en guardar los documentos en la red?	X				
P.2.13	¿Los usuarios del área son conscientes del procedimiento a seguir ante cualquier mal acto en contra de la integridad de los datos?		X			

ANEXO 1 - LISTA DE COTEJO PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME						
	PREGUNTAS	**NIVEL DE CUMPLIMIENTO**			**OBSERVACIONES**	**COMENTARIOS**
		3	2	1		
3	**DISPONIBILIDAD**					
	Seguridad física y del entorno.					
P.3.1	¿El área cuenta con la disponibilidad de información que asegura la fiabilidad y acceso oportuno de los datos de la organización?	X				
P.3.2	¿La empresa cuenta con controles de acceso a los diferentes activos de la organización?	X				
P.3.3	¿La seguridad de los datos se encuentra protegido ante un desastre natural o daño físico ocasionado por algún usuario?	X				
P.3.4	¿Las condiciones ambientales del área se encuentran monitoreadas para un buen funcionamiento de los datos almacenados en los servidores?	X				
P.3.5	¿El área de T.I realiza mantenimiento preventivo de los equipos físicos de las diferentes áreas de la empresa?		X			
	Incidentes en la disponibilidad de la información					

P.3.6	¿El área cuenta con un nivel aceptable de disponibilidad de la información?	X				
P.3.7	¿El área de T.I realiza seguimiento de cómo se maneja la disponibilidad de la información de las diferentes áreas de la empresa?	X				
P.3.8	¿El área cuenta con procedimientos que ayuden a mantener la disponibilidad de la información en buen estado?	X				
P.3.9	¿El área cuenta con un registro de incidentes que se presentan con la disponibilidad de la información y se toma medidas antes estos casos?	X				
	Disponibilidad de servicios de información					
P.3.10	¿El área cuenta con copias de seguridad que respaldan la disponibilidad de los datos de la organización?	X				
P.3.11	¿El área de T.I cuenta con UPS con bancos de baterías que permitan mantener la disponibilidad de la información en la empresa?		X			
P.3.12	¿El área cuenta con una buen orden de sus documentos que se almacenan en sus servidores?	X				
P.3.13	¿El área cuenta con mecanismos y metodologías que ayudan a mantener estable la disponibilidad de la información?	X				

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, SABOYA RIOS NEMIAS, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Método de Seguridad de Información basado en tecnología de Servidores Espejos en la nube con herramientas open source para PyMES", cuyos autores son OCAMPO GUTIERREZ JHONATTAN WALTER, LAYMITO LOZANO JESUS MARTIN, constato que la investigación tiene un índice de similitud de 22.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 20 de Diciembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
SABOYA RIOS NEMIAS **DNI:** 42001721 **ORCID:** 0000-0002-7166-2197	Firmado electrónicamente por: NSABOYARI el 20-12-2022 20:45:17

Código documento Trilce: TRI - 0497360

INVESTIGA UCV