UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de un VPN basado en la metodología top-Down para mejorar la seguridad de la información en el consorcio Andia

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

AUTOR:

Valero Andia, Billy Scott (orcid.org/0000-0002-9133-9557)

ASESOR:

Dr. Sánchez Atuncar, Giancarlo (orcid.org/0000-0001-9842-7317)

LÍNEA DE INVESTIGACIÓN:

Infraestructura y servicios de redes y comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2023

DEDICATORIA

A mi familia, esta tesis es para ustedes.
A mi madre, por su amor incondicional,
su paciencia infinita y su fe inquebrantable en mí.
A mis abuelos, por su cariño y comprensión,
que siempre me han hecho sentir amado y apoyado.
A mi padrino, por su apoyo incondicional,
su amistad sincera y su aliento constante
Sin ustedes, no habría llegado hasta aquí.
Este logro es de ustedes también.

AGRADECIMIENTOS

A mi asesor, Dr. Giancarlo Atuncar, por su invaluable apoyo, consejos y recomendaciones. Su tiempo y dedicación fue de mucha ayuda en mi preparación.

Al Consorcio, por apoyarme con la información en un ambiente de aprendizaje y crecimiento.

A la Universidad Cesar Vallejo, por la preparación académica y las herramientas necesarias para alcanzar este logro.

A mi compañero Pepes, por su compañía y apoyo incondicional. Siempre estuvo ahí para mí, incluso cuando los días eran difíciles.

Y, sobre todo un agradecimiento perse, por la perseverancia, el compromiso y la dedicación que me permitieron superar los desafíos y completar esta tesis.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, SANCHEZ ATUNCAR GIANCARLO, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, asesor de Tesis titulada: "Implementación de un VPN basado en la metodología top-Down para mejorar la seguridad de la información en el consorcio Andia", cuyo autor es VALERO ANDIA BILLY SCOTT, constato que la investigación tiene un índice de similitud de 14.00%, 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, 19 de Diciembre del 2023

Apellidos y Nombres del Asesor:	**Firma**
SANCHEZ ATUNCAR GIANCARLO **DNI:** 41488834 **ORCID:** 0000-0001-9842-7317	Firmado electrónicamente por: GSANCHEZAT el 19-12-2023 20:37:54

Código documento Trilce: TRI - 0700798

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Originalidad del Autor

Yo, VALERO ANDIA BILLY SCOTT estudiante de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Implementación de un VPN basado en la metodología top-Down para mejorar la seguridad de la información en el consorcio Andia", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

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

Nombres y Apellidos	**Firma**
VALERO ANDIA BILLY SCOTT **DNI:** 74732818 **ORCID:** 0000-0002-9133-9557	Firmado electrónicamente por: VALEROANDIA el 15-01-2024 14:22:47

Código documento Trilce: INV - 1526376

Índice de contenidos

Carátula……i
Dedicatoria……ii
Agradecimiento……iii
Declaratoria de Autenticidad del Asesor……iv
Declaratoria de Originalidad del Autor……v
Índice de Contenidos……vi
Índice de tablas……vii
Índice de figuras……ix
Resumen……xi
Abstract……xii
I. INTRODUCCIÓN ……1
II. MARCO TEÓRICO……7
III. METODOLOGÍA……19
3.1. Tipo y diseño de investigación ……19
3.2. Variables y Operacionalización……20
3.3. Población, muestra y muestreo……21
3.4. Técnicas e instrumentos de recolección de datos……22
3.5. Procedimiento……26
3.6. Método de análisis de datos……27
3.7. Aspectos éticos……28
IV. RESULTADOS ……29
V. DISCUSIÓN……43
VI. CONCLUSIONES……46
VII. RECOMENDACIONES……48
REFERENCIAS……50
ANEXOS……62

Índice de Tablas

Tabla N° 1 Comparativa de Metodologías……..……..19

Tabla N° 2: Población de la muestra. ……..21

Tabla N°3: Instrumento de recolección de datos……22

Tabla N° 4: Nivel de Confiabilidad…….……24

Tabla 5: Medidas descriptivas para nuestra variable general Seguridad de la Información..,…….29

Tabla 6: Medidas descriptivas del Indicador de Protección de datos antes y después de implementar el VPN.……30

Tabla 7: Tabla comparativa entre las opciones marcadas para la variable Autenticación en el Pre-test y el Post-test.……31

Tabla 8: Medidas descriptivas del Indicador de Protección de datos para el pre-test y post-test de la implementar del VPN.……31

Tabla 9: Tabla comparativa entre las opciones marcadas para la variable Protección de datos en el Pre-test y el Post-test.……32

Tabla 10 Medidas descriptivas del Indicador Accesos para el pre-test y post-test de la implementación del VPN……32

Tabla 11: Tabla comparativa entre las opciones marcadas para la variable Acceso en el Pre-test y el Post-test.……33

Tabla 12: Medidas descriptivas del Indicador Autorización para el pre-test y post-test de la implementación del VPN…….…..33

Tabla 13: Tabla comparativa entre las opciones marcadas para la variable Accesos en el Pre-test y el Post-test.……...34

Tabla 14: Medidas descriptivas del Indicador Accesibilidad para el pre-test y post-test de la implementación del VPN……..35

Tabla 15: Tabla comparativa entre las opciones marcadas para la variable Accesibilidad en el Pre-test y el Post-test.……35

Tabla 16 Pruebas de normalidad Hipótesis General ……36

Tabla 17 Prueba Estadística Wilcoxon Hipótesis General……36
Tabla 18 Pruebas de normalidad Autenticación……37
Tabla 19 Prueba Estadística Wilcoxon Autenticación……38
Tabla 20 Pruebas de normalidad Protección……38
Tabla 21 Prueba Estadística Wilcoxon Protección de datos……39
Tabla 22 Pruebas de normalidad Accesos……39
Tabla 23 Prueba Estadística Wilcoxon Accesos……40
Tabla 24 Pruebas de normalidad Autorización……40
Tabla 25 Prueba Estadística Wilcoxon Autorización ……41
Tabla 26 Pruebas de normalidad Accesibilidad……41
Tabla 27 Prueba Estadística Wilcoxon Accesibilidad……42

Índice de Figuras

Figura 1: Cyber Incidents by industry……..…3

Figura 2: Formula de la muestra……22

Figura 3: Obtención de muestra…….……22

Figura 4: Ecuación de Cronbach……25

Figura 5: Estadística de fiabilidad de Seguridad de Información……..25

Figura 6: Estadística de fiabilidad de confidencialidad……..26

Figura 7: Estadística de fiabilidad de integridad……..26

Figura 8 Estadístico de fiabilidad de disponibilidad……..……..26

Figura 9 Grafico de barras pre-test por opción marcada en cada indicador……..30

Figura 10 Grafico de barras Post-Test por opción marcada en cada indicador….30

Figura 11 Indicador de autenticación del pre-test y post-test del VPN……31

Figura 12 Indicador de protección del pre-test y post-test del VPN……32

Figura 13 Indicador de accesos para pre-test y post-test ……33

Figura 14 Indicador de autorización para pre-test y post-test …….……34

Figura 15 Indicador de accesibilidad para el pre-test y post-test.……35

Figura 16 Fases metodologia Top-Down.....71

Figura 17 Topologia Estrella.....75

Figura 18 Software definido para redes……77

Figura 19 Login de software definido para redes……78

Figura 20 Creación del proyecto……79

Figura 21 Configuración del proyecto……79

Figura 22 Escogiendo el tipo de dispositivo añadir……79

Figura 23 Activación de nuestro dispositivo……..…80

Figura 24 Los 3 proyectos creados para nuestras oficinas……..…80

Figura 25 Túnel IPSec.……80
Figura 26 Configuración del router……81
Figura 27 Políticas del VPN……82
Figura 28 VPN conectada y sincronizada……82
Figura 29 IPSec túnel encriptado……...82
Figura 30 Configuración del servidor VPN……...83
Figura 31 Configurar de la seguridad……83
Figura 32 Configuración de la conexión……84
Figura 33 Marco del IPSec protocolo…….....……..84
Figura 34 Detalles del router……..84
Figura 35 Lista de políticas VPN……85
Figura 36 Ipsec Estado de conexión……85
Figura 37 Prueba de ping entre subnet……86
Figura 38 IPSec estados de conexión……..86
Figura 39 IPSec lista de seguridad……87
Figura 40 Prueba de pineo del servidor……87
Figura 41 Funcionamiento del IPSec……89
Figura 42 Ruta del servidor storage……..89
Figura 43 Ubicación de red de nuestro storage……..90
Figura 44 Agregando la ubicación……90
Figura 45 Asignando ruta y letra……91
Figura 46 Ruta agregada correctamente……91

Resumen

Esta investigación presenta los resultados de un estudio llevado a cabo en el Consorcio Andia, una firma de bienes raíces reconocida por su experiencia en transacciones inmobiliarias. El estudio se enfocó en desafíos de seguridad de la información y la comunicación entre las sedes, identificando problemas como falta de confidencialidad, cifrado inseguro, control de acceso deficiente, integridad y limitaciones en la disponibilidad de datos. El objetivo principal fue evaluar el impacto de una VPN basada en la metodología top-down en la seguridad. Se establecieron objetivos específicos para medir su influencia en áreas como el cifrado, control de acceso, integridad y disponibilidad. La metodología empleada fue cuantitativa y experimental, incorporando mediciones tanto en el pretest como en el post-test para analizar cambios. Los resultados revelaron un impacto positivo considerable en la seguridad de la información, mejorando aspectos como Autenticación, Protección de datos, control de acceso y, especialmente, se observó una mejora significativa en el post-test tras la implementación de la VPN. Estos hallazgos poseen relevancia no solo para el consorcio, sino también para otras empresas del rubro inmobiliario, ya que una VPN con esta metodología puede disminuir los riesgos de violaciones de datos y accesos no autorizados. En resumen, este estudio enfatiza la importancia de soluciones como la VPN top-down para abordar los desafíos de seguridad en el sector inmobiliario, demostrando su efectividad en mejorar la seguridad de la información en organizaciones similares.

Palabras Clave: *VPN, top-down, disponibilidad*

Abstract

This research presents the results of a study carried out at the Andia Consortium; a real estate firm recognized for its experience in real estate transactions. The study focused on information security challenges and communication between sites, identifying issues such as lack of confidentiality, insecure encryption, poor access control, integrity, and limitations in data availability. The main objective was to evaluate the impact of a VPN based on the top-down methodology on security. Specific objectives were established to measure its influence in areas such as encryption, access control, integrity and availability. The methodology used was quantitative and experimental, incorporating measurements in both the pretest and the post-test to analyze changes. The results revealed a considerable positive impact on information security, improving aspects such as Authentication, Data Protection, access control and, especially, a significant improvement was observed in the post-test after the implementation of the VPN. These findings are relevant not only for the consortium, but also for other companies in the real estate sector, since a VPN with this methodology can reduce the risks of data breaches and unauthorized access. In summary, this study emphasizes the importance of solutions such as top-down VPN to address security challenges in the real estate sector, demonstrating its effectiveness in improving information security in similar organizations.

Keywords: *VPN, top-down, availability*

I. INTRODUCCIÓN

Según Cisco (2021) nos comenta que hoy en día tener seguridad en la información es muy importante para sobrellevarlo en nuestra época actual, donde la tecnología y la información se han vuelto cada vez más omnipresentes. La protección de nuestra información vendría siendo lo mismo que cuidar nuestros datos de cualquier forma o medio de acceso no autorizado, divulgación o destrucción, con el fin de garantizar nuestra accesibilidad, fiabilidad y utilizabilidad de nuestros datos. La seguridad de la información se aplica en cualquier tipo de datos, ya sea un correo en formato virtual o físico, y se aplica todos tipos de empresas. (p.1). También Imperva (2021) nos comenta:

Resalta que la protección de nuestros datos es un tema extenso que incluye la protección contra amenazas internas y externas, como hackers, virus informáticos, desastres naturales y fallas en los servidores. La estabilidad de nuestros datos también da a entender que nuestra intimidad estará protegida de los terceros, la información robada es un gran motivo, la financiera también puede ser robada y utilizada de manera fraudulenta. La seguridad de la información es esencial para asegurar una secuencia de elementos y la reputación de las organizaciones en el mundo actual. (p.1)

Cid-Fuentes, et al., 2020, comento:

En la actualidad, el aumento de las “TIC” ocasiono un crecimiento en, la medida de datos que se dirige a través de internet, lo que a su vez ha aumentado la preocupación por la seguridad de esta información. Aseguramos de manera efectiva la protección de datos online a través del método (VPN) que se lleva a cabo mediante ordenadores permitiendo la extensión del área local de manera segura, que permiten el cifrado de los datos y la conexión a internet a través de servidores seguros. (p.3)

En línea con esta necesidad, las empresas y organizaciones gubernamentales han comenzado a implementar soluciones de VPN con el fin de asegurar en line la seguridad de los datos. Por ejemplo, en un estudio de investigación reciente realizado por Cid-Fuentes et al. (2020), se encontró que el uso de VPN es una estrategia efectiva para proteger la información en línea en empresas españolas de

diversas áreas del sector, como educación, también el área de salud, y las finanzas. El diseño de un VPN puede ser un proceso complejo que requiere la consideración de múltiples factores, como la elección de protocolos de cifrado y la configuración de servidores. En este sentido, la metodología Top Down se ha propuesto como una forma efectiva de abordar el diseño de redes de seguridad, al permitir detectar e identificar los riesgos y necesidades de esta seguridad antes de la implementación de la solución.

Para Perdigón, Rubidel (2021),

> En nuestro país, la seguridad de información se volvió un tema muy reciente y de preocupación. La tecnología avanza a pasos muy rápidos, volviéndose así más importante para nuestro entorno, siendo mucho más difícil encontrar maneras correctas para defendernos y a su vez la información del consorcio. Dado que nuestra red es cada vez más grande y compleja, y con la aparición de la Internet de las cosas, es necesario buscar alternativas innovadoras y protegeré nuestros datos de información. Por lo tanto, el uso de una VPN podría proporcionar una solución efectiva para asegurarnos de brindarnos un servicio confidencial e integro en la empresa.

De acuerdo con el informe del (MTPE) Ministerio de Trabajo y Promoción del Empleo se registraron 226 mil empleados formales que estaban trabajando en modalidad de teletrabajo o trabajo remoto, lo que equivale al 6,7% de los empleados formales en el sector privado, esto aumenta el factor vulnerabilidad para seguridad. Además, con la creciente cantidad de dispositivos conectados a la red, es difícil controlar quienes acceden a la información confidencial. Por lo tanto, una VPN podría permitir a los empleados de la empresa acceder a la red interna de forma más protegida de cualquier punto de interne, garantizando al mismo tiempo la información privada junto a la seguridad de información.

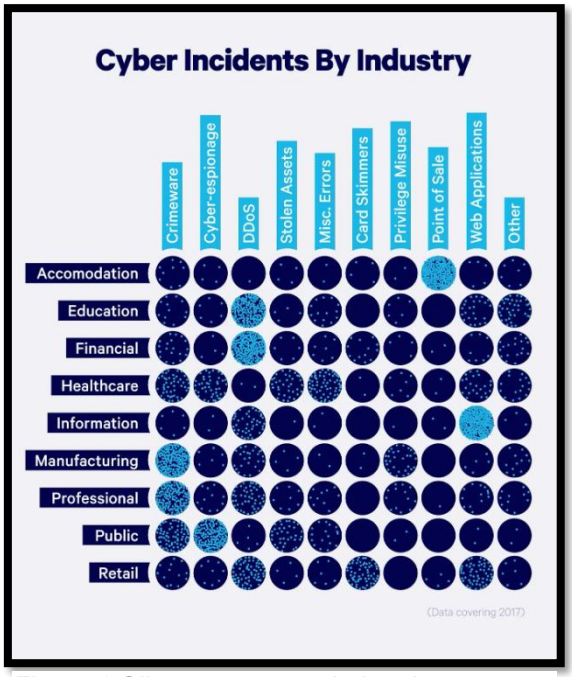


Figura 1 Ciberataques por industria

La Figura 1 describe los riesgos que enfrentan estas industrias y destaca la importancia de la ciberseguridad para proteger nuestra información más preciada y confidencial. El análisis destaca la necesidad de implementar medidas de seguridad adecuadas para prevenir y mitigar los ataques cibernéticos y proteger la integridad de los datos en estas industrias.

Por otro lado, existe la preocupación en nuestra ciudad por la creciente cantidad de ataques cibernéticos a empresas y organizaciones gubernamentales. Con la aparición de nuevas tecnologías, también han aparecido nuevas formas de ciberataques, por lo que es necesario buscar medidas efectivas para proteger la información confidencial de la organización. Una VPN puede proporcionar una solución más asegurar para la confidencialidad e integridad de nuestros datos la empresa frente a posibles amenazas externas.

La investigación se realizó en el Consorcio Andia SAC, consorcio dedicado al rubro inmobiliaria. Es reconocida por su experiencia en la adquisición y comercialización de propiedades inmobiliarias., lotes y propiedades, así como por sus servicios de alquiler de pisos y departamentos.

En el consorcio actual, nos encontramos ante una situación que plantea diversos desafíos de la S.I. y la comunicación efectiva entre las sedes. La definición del

problema nos podrá delimitar con claridad los aspectos clave que requieren atención. Los desafíos incluyen la falta de información confidencial, la información insegura por falta de cifrado, el control de acceso deficiente, la necesidad de integridad y la disponibilidad limitada con los datos. Estas problemáticas se derivan de la utilización de una nube pública con una cuenta gratuita para el intercambio de información, así como de la falta de una conexión adecuada y segura entre las sedes del consorcio. Estas deficiencias ponen en riesgo la confidencialidad de datos importantes y pueden resultar en la posible divulgación de información confidencial.

En particular, la falta de confidencialidad de la información expone al consorcio a posibles violaciones de datos y a la pérdida de información estratégica y sensible. La insuficiente protección de datos deja al consorcio vulnerable a ataques cibernéticos y filtraciones de datos confidenciales, lo que puede tener graves consecuencias tanto para la organización como para los individuos involucrados. Además, el control de acceso deficiente dificulta la correcta gestión de los permisos y la protección nuestra información sensible, lo que aumenta el riesgo de accesos no autorizados y uso indebido de los datos. A falta de la integridad en nuestra información se puede generar inconsistencias y alteraciones en los datos, lo que afecta negativamente la toma de decisiones y la confianza en la información disponible. Por último, la disponibilidad limitada de los datos dificulta la el intercambio y colaborar de manera eficiente entre las diferentes sedes del consorcio.

Teniendo en cuenta la realidad problemática o la realidad expuesta, surge alguna interrogante de esta investigación, como Problema general: ¿Cómo el diseño de una VPN basada en la metodología top-Down mejora la seguridad de la información en un consorcio? De igual manera para los Problemas Específicos**:** ¿Cómo la VPN basada en la metodología top-Down mejora la Autenticación en el consorcio Andia?, ¿Cómo la VPN basada en la metodología top-Down mejora la protección de datos de información en el consorcio Andia?, ¿Cómo la VPN basada en la metodología top-Down mejora el control de acceso en el consorcio Andia?, ¿Cómo la VPN basada en la metodología top-Down mejora la control de Autorizacion en el

consorcio Andia?, ¿Cómo la VPN basada en la metodología top-Down mejora la Accesibilidad en el consorcio Andia?

Teniendo en cuenta la relevancia de respaldar nuestras afirmaciones con fundamentos sólidos y fuentes confiables, es necesario presentar la justificación teórica de nuestro estudio, nos basamos en la definición proporcionada por la RAE (2020), una prueba es “señalar una causa, motivo o justificación para probar determinados hechos”; tanto para Sabaj y Landea (2017), esto será considerado como algo decidido por el investigador que busca construir sobre los cimientos de su conducta, creencias y conocimientos. Para Bernal (2010 – Citado de Sabaj y Landea,2017), la legitimidad de un campo científico implica abordar el vacío científico o quizá los problemas que deben ser llenado completa o parcial, y amerita ser desarrollado a través de argumentos fuertes.

En este punto cuando hablamos del aporte de la empresa podemos decir que implementar medidas efectivas de seguridad de la información constituye un aporte fundamental para las empresas en la era digital. El diseño y desarrollo de una VPN con la metodología top-down mejorará la seguridad en el consorcio, garantizando todos los principios de la Seguridad como la confidencialidad, también la integridad y por ultimo disponibilidad de los datos. Esto permitirá prevenir vulnerabilidades, evitar la pérdida o filtración de información sensible, y proteger los intereses de la organización. Además, la VPN facilitará el acceso y la transferencia segura de información entre las diferentes sedes del consorcio, promoviendo la colaboración y eficiencia en los procesos empresariales. Con este aporte, se fortalecerá la confianza de los clientes, se protegerá la reputación de la empresa y se cumplirán los requerimientos legales para el área de la información y seguridad

En términos sociales este proyecto tiene relevancia para todas las empresas y organizaciones que manejan información sensible en un entorno digitalizado, ya que les brindará pautas y soluciones prácticas para fortalecer la seguridad de sus datos. Asimismo, para tratar el valor teórico de este proyecto podemos ver el desarrollo de un marco sólido que profundizará en las características para mejorarla compresión de la seguridad de la información, lo que beneficiará tanto a la comunidad académica como a otros profesionales interesados en el tema.

En cuanto a la utilidad metodológica, el uso de entrevistas y cuestionarios como herramientas de recopilación de datos permitirá obtener información cualitativa y percepciones expertas para el área de seguridad de información. Esto enriquecerá el análisis y las conclusiones del estudio, aportando una perspectiva práctica y fundamentada al momento de implementar las mejoras de seguridad propuestas**.**

Para abordar los objetivos de nuestra investigación, podemos decir que como Objetivo general tenemos Determinar el impacto del diseño de una VPN basada en la metodología top-Down en la mejora de la seguridad de la información en un consorcio, y para los objetivos específicos tenemos primero: Determinar la influencia del diseño de una VPN basada en la metodología top-Down en el cifrado de información en el consorcio, segundo: Determinar la influencia del diseño de una VPN basada en la metodología top-Down en el cifrado de información en el consorcio, tercero: Determinar el impacto del diseño de una VPN basada en la metodología top-Down en el control de acceso a la información en el consorcio, cuarto: Determinar el efecto la implementación de una VPN basada en la metodología top-Down en la integridad de la información en el consorcio, y por ultimo quinto: Determinar el impacto la implementación de una VPN basada en la metodología top-Down en la disponibilidad de la información en el consorcio.

En el estudio se explora diversas explicaciones o suposiciones, conocidas como hipótesis, que nos ayudaran a establecer las bases teóricas. A continuación, se presenta la hipótesis general “La implementación de una VPN basada en la metodología top-Down mejora la seguridad de la información en un consorcio” de igual manera se presenta las hipótesis específicas: La implementación de una VPN basada en la metodología top-Down contribuye a mejorar el cifrado de información en el consorcio. La implementación de una VPN basada en la metodología top-Down contribuye a mejorar el cifrado de información en el consorcio. La implementación de una VPN basada en la metodología top-Down incide positivamente en el control de acceso a la información en el consorcio. Verificar el efecto de la implementación de una VPN basada en la metodología top-Down en la integridad de la información en el consorcio. La implementación de una VPN basada en la metodología top-Down favorece la disponibilidad de la información en el consorcio.

II MARCO TEÓRICO

En la búsqueda de la información, se encontró unas investigaciones similares al título, en el ambiente nacional la investigación de Lazarte y Silva, (2022):

En su propuesta Creación de una VPN utilizando software de código abierto este informe proporciona información valiosa sobre cómo implementar una VPN bajo software libre y asi lograr mejorar la S.I. en un área específica. La metodología que se llegó a usar fue la metodología Top-Down Network Design para La implementación del proyecto de despliegue de una VPN usando soluciones de libre software. Esta metodología consta de cuatro fases: Llevar a cabo un análisis exhaustivo de los requisitos, elaborar un diseño lógico detallado, desarrollar un diseño físico acorde y realizar pruebas rigurosas, optimización efectiva y documentación completa la implementación (p.15).

También se encontró en el trabajo de Morales, J. et al (2021)

En su título VPN y su implementación con PPDIOO el ciclo de vida, y a su vez mejorar la seguridad informática, se propone la implementación de una VPN con el objetivo de hacer mejoras, seguridad la información en la red corporativa. La estudio se define en una muestra de 30 procesos relacionados con la seguridad informática, utilizando fichas de observación para recopilar datos. Se aplicó un enfoque cuantitativo junto con un diseño experimental puro, utilizando pruebas estadísticas para contrastar las hipótesis planteadas. Los resultados obtenidos indicaron una reducción significativa reportada por los usuarios en el número de incidencias, una disminución en la cantidad los endpoints conectados, una baja en el tiempo dedicado al acceso compartido y un incremento para los usuarios y su nivel de satisfacción.

De igual forma para Huanca, Pablo (2022)

El desarrollo de su labor, que implica implementar una Red Privada Virtual para elevar la seguridad de los datos, se estableció como objetivo principal mejorar la red y sus servicios mediante la incorporación de una Red Privada Virtual en la institución educativa. Este estudio se utilizó un enfoque cuantitativo, con un diseño preexperimental. La muestra consistió en 30 participantes, y se recopiló la información mediante cuestionarios relacionados con la VPN y también la

seguridad de información. Tras obtener los resultados estos indicaron que la VPN se encontraba en un nivel medio, mientras que la variable dependiente exhibía una tendencia hacia un nivel alto, con una considerable proporción en el nivel medio. Al contrastar la Red Privada Virtual implementada con la seguridad de la información, se evidenció una conexión significativa entre ambas variables. En resumen, al aumentar la Red Privada Virtual implementada en la Institución Educativa Militar Francisco Bolognesi, se observó una relación directa en la Seguridad de la información y su mejoría. Por el contrario, una disminución en la adopción de la VPN resultó en una disminución de la seguridad de los datos. Estos hallazgos resaltan la importancia del uso de una VPN como un factor clave e importante hacia la seguridad de la información.

Asimismo, Valverde (2022) en su tesis Implementación de gestión TI, donde el propósito principal consistió en implementar un sistema de riesgo en el área de TI a un plan de manera estratégico, con el fin de que la S.I. mejore en la empresa de publicidad. El enfoque se centró en la habilidad de la organización para manejar los riesgos y prevenir posibles ataques informáticos y manipulaciones inapropiadas de la información. Se establecieron niveles adecuados de la integridad, la privacidad y la accesibilidad a la continuidad de la información. Cuando este proceso se llevó a cabo, se optó por utilizar Magerit como metodología, lo que permitió la evaluación de análisis de los riesgos presentes en la organización y obtener respuestas concretas a dichos riesgos. Estas respuestas se utilizaron para implementar algunas soluciones y administrara la S.I. empresarial. (p.10)

De igual forma (Cruz, 2017) en su tesis de investigación Implementación de un Sistema de Gestión De S.I para proteger los activos de Información La Clínica investigación, demuestra que el propósito de implementar SGSI tiene como objetivo salvaguardar la información crítica del negocio que son fundamentales para los objetivos de la empresa. Al lograr esto, se decidió utilizar el enfoque El enfoque de Deming, o el enfoque PDCA (Planificar-Hacer-Verificar-Actuar), es altamente recomendado por la norma ISO 27001 para los SGSI. El resultado obtenido es la minimización de los riesgos asociados a Los riesgos y debilidades que afectan datos, documentos, sistemas, infraestructura tecnológica de MEDCAM Perú S.A.C., así como la garantía de la privacidad, accesibilidad y consistencia de esa

información. Entonces podemos decir que la seguridad es lo más importante de los recursos de la información para alcanzar los objetivos empresariales (p.8).

En otro estudio realizado por (Bueno, 2021), en su investigación de tesis Marco de trabajo en software libre, se propone crear un framework para utilizar un Protocolo virtual de red y con software libre y aumentar la banda ancha de internet. Usó la metodología Cisco PPDIOO, la arquitectura de la plataforma V2RAY está implementada sobre nubes AWS y ORACLE. Los resultados de las evaluaciones antes y después del uso de la solución mostraron mejoras significativas en varias métricas. En particular, la velocidad de descarga aumentó un 26,4 %, la velocidad de carga aumentó un 79,5 % y el tiempo de respuesta aumentó un Cien por ciento. Además, se registró una tasa de deserción del Cien por ciento, que también se consideró significativa con un valor de p value< 0,05 para sus indicadores (p.12).

También (Luna y Zeta, 2021) su objetivo es desarrollar una herramienta, con una base sólida de rentabilidad y utilidad, para establecer una conexión o enlace VPN de acceso remoto utilizando equipos MIKROTIK que priorice la confidencialidad de la transferencia de información de un punto A al punto B, esquivando que los Puntos de internet y así violar o tomar los paquetes en el tráfico y robar todo lo enviado y recibido mediante esta VPN, mejorando ventajosamente el rendimiento de la infraestructura de red, aumentando el rendimiento de los paquetes enviados, además de demostrar que los recursos se usan menos y las cargas de trabajo de MIKOTRIK VPN de RAM, no como otros agentes remotos con mayor consumo de memoria(p.8).

También para la búsqueda de información encontramos los antecedentes internacionales Según (Cabrera y Cordero, 2021), quien se enfoca en dos tecnologías vanguardistas como las VPN y los MLPS, siendo su valor más preciado la escalabilidad, integridad e interoperabilidad, como parte de la metodología y las actividades propuestas de la investigación, también se realizó una búsqueda minuciosa y completa de las tecnologías y hardware para su implementación en la red, logrando así la implementación telemática de la red que asegure la comunicación confiable y de velocidad alta para las diferentes sucursales de la empresa(p7).

Tambien (Madigral y Pedrigon,2021):

Con su objetivo principal del proyecto fue crear una solución utilizando herramientas de software libre para establecer el teletrabajo en línea. Se usaron diferentes maneras científicas, como el análisis el método experimental, la triangulación teórica, el histórico lógico y sintético. Los resultados obtenidos confirmaron que la solución propuesta permite a los teletrabajadores ingresar de manera más segura aplicaciones digitales de la empresa, logrando un rendimiento aceptable a pesar de los recursos tecnológicos limitados disponibles.

De igual manera (Peñafiel Cristian, 2019):

Se aborda el tema de la información protegida en el ámbito del Cloud Computing. El objetivo central de este estudio, realizado por el autor Vidal, S., consiste en desarrollar un marco para establecer un SGSI en un entorno de Cloud Computing, empleando como referencia la norma ISO 27001:2013. En dicho documento, se detallan los requisitos necesarios para la implementación de este modelo, teniendo en consideración las ventajas y desventajas asociadas al Cloud Computing, así como los riesgos, amenazas y vulnerabilidades inherentes a dicho entorno. La norma ISO 27001:2013 se examina en relación al Cloud Computing con el fin de adaptarla y aplicarla de manera efectiva en dicho contexto. El propósito de esta investigación es proporcionar a las organizaciones una guía que les permita salvaguardar la seguridad de su información al llevar a cabo la migración hacia la nube.

También en Ecuador (Mora, Jaime,2021):

En su trabajo de Gestión de Seguridad alienada a la norma 27001, comenta que el mayor objetivo es diseñar una metodología que permita gestionar de forma eficiente y adecuada la SI, basada en la norma ISO 27001 y también los marcos de ciberseguridad establecidos en ISO/IEC 27032. Esta metodología se enfoca en analizar las brechas de seguridad en los SI, con el fin de garantizar su protección de manera efectiva. Es importante resaltar la estrecha relación de marcos establecidos a normas I.S.O. 27001 e ISO 27032, los cuales se centran en la SGSI y la ciberseguridad. Lo que se propone es que la metodológica desarrollada tenga la capacidad de identificar los procesos, las normas y los protocolos que están involucrados en la SI en diferentes niveles de gestión.

También (Párraga, Rene,2018):

En su trabajo donde diseño el protocolo de seguridad post evento, siguiendo las normas ISO 17799, donde se lleva a cabo una investigación centrada en la creación de un protocolo de seguridad para abordar los eventos informáticos posteriores en dicha facultad. El objetivo principal es resolver las vulnerabilidades presentes para los S.O., databases, y app's y hardware utilizados, a fin de prevenir la pérdida o alteración de información. El estudio se divide en tres capítulos que abordan la problemática, la metodología propuesta y los análisis para la seguridad implementada. Se ha diseñado un protocolo siguiendo las nomas de la ISO/IEC-17799 con el fin de establecer prácticas efectivas para la gestión de seguridad y garantizar la protección para la facultad de ingeniería industrial siendo los datos lo principal a proteger.

Para describir la variable independiente: VPN, se considerarán las siguientes definiciones

Comenta Jota, Yuly, (2018)

La vpn es un protocolo de capa 3 que extiende la red sea pública o privada no controlada. Es probablemente el modelo el software que más se utiliza hoy en día y consiste en que un usuario o proveedor se conecta a una empresa desde un sitio remoto (oficina comercial, domicilio, hotel, avión en servicio, etc.) utilizando la red pública como puntos de red. Luego de autenticarse, los usuarios dentro del negocio tendrían que tener el acceso a la red igual. Esta tecnología ha llevado a muchas empresas a reemplazar su infraestructura dial-up.

Tambien para William J. Tolley and Beau Kujath (2021):

El propósito de una VPN es evitar que cualquier persona en la dirección entre la vpn cliente y la vpn servidor vea el contenido del tráfico del usuario y, en general, se supone que esta parte del túnel está protegida. Incluso si un atacante pudiera ver los paquetes enviados entre el servidor VPN y el servidor terminal, no podría determinar el cliente VPN en el otro lado del servidor VPN simplemente analizando los paquetes)

Es una red privada que simula su estructura dentro de la red pública por donde viaja normalmente los datos, esta tecnología viaja en las capas del modelo OSI, más exacto en la capa 2 y en la capa 3, facilitando que las sedes y distintas

localidades disfruten de la interconexión facilitada por un proveedor de servicios, siendo esta vpn muy segura porque se crea en un túnel de encriptación que viaja por la red pública pero de manera muy segura, pudiendo ofrecer servicios de seguridad, privacidad y funciones adicionales, las redes virtuales privadas (VPN) brindan beneficios que las redes internas convencionales no poseen. (Cabrera y Cordero, 2021)

Por lo mismo, Skendzic, S. et al (2017):

Comenta que la Internet, como plataforma de comunicación, desempeña un papel fundamental en la sociedad actual. Entre los diferentes servicios que ofrece, las redes privadas virtuales destacan como un método altamente eficiente y rentable de comunicación, especialmente para la interconexión de oficinas remotas. Estas tecnologías permiten transmitir información sensible, clasificada como secreta o confidencial, a través de redes inseguras al establecer túneles de comunicación protegidos mediante métodos criptográficos.

De acuerdo con la investigación realizada por Rama Bansode (2021):

Se ha identificado que la seguridad de las VPN sigue siendo un tema de preocupación. Aunque existen instrucciones comunes para configurar las VPN, los administradores aún tienen dudas sobre la seguridad de sus sistemas. Existe una falta de investigación que aborde adecuadamente las vulnerabilidades y las políticas de mitigación en las infraestructuras ya configuradas. No obstante, es importante destacar que siempre habrá oportunidades para fortalecer los sistemas mientras existan vulnerabilidades. Para mejorar la seguridad de las VPN, se requiere un enfoque más exhaustivo para adaptarse a las necesidades de la organización.

Durante la investigación realizada, Al-Fayum (2022)

Se ha observado que el aumento del uso de dispositivos tecnológicos durante la pandemia se ha generado un gran volumen de datos en Internet. El uso de VPNs y el encriptado de datos se han vuelto comunes para preservar la privacidad. Sin embargo, esto presenta desafíos para los términos de calidad, monitoreo de tráfico y seguridad en la red para los ISP (Internet Service Provider). Este estudio propone modelos de aprendizaje automático para clasificar el tráfico

encriptado y no encriptado con alta precisión. Es crucial comprender y abordar las vulnerabilidades de seguridad en las VPNs y buscar enfoques más avanzados para mejorar la gestión y seguridad de la red.

Así mismo Zhou, Z. (2021):

Aborda cómo las agencias de prevención y control del COVID-19 expanden sus redes internas utilizando la tecnología de VPN abierta. Se propone un diseño que utiliza el acceso de la VPN a través de una puerta de enlace abierta para solucionar el problema de informar directamente a los usuarios que acceden al sistema desde la red externa. Además, se emplea el análisis de big data basado en el diseño del panel de control ArcGIS para implementar en tiempo real un sistema de monitoreo y visual de la situación epidémica global. Este sistema permite obtener de manera efectiva y oportuna el desarrollo de la epidemia del coronavirus 2019. El enfoque principal del sistema es la visualización en línea rápida y conveniente de la distribución global de la epidemia, el análisis estadístico en tiempo real de la distribución espacial de la epidemia y la visualización dinámica de la gravedad de la epidemia en diferentes países y regiones, así como la tendencia de desarrollo de la epidemia global. Este enfoque contribuye al desarrollo del trabajo de monitoreo de la epidemia.

El autor también añade que los beneficios adicionales brindados es que este será de más fácil acceso y un acceso más rápido a través del software libre. Por consiguiente, Zhou, Z. (2021) en su artículo se centra en el uso de OpenVPN, una tecnología de código abierto basada en el protocolo SSL, para establecer un sistema de acceso de usuarios en la plataforma de operación LINUX en instituciones educativas. Esto permite acceder más rápidamente a los recursos de red desde los usuarios del campus a través del programa cliente de OpenVPN, garantizando la confidencialidad de los datos sin requerir inversiones adicionales. Además, permite a los usuarios superar las limitaciones de tiempo y espacio, mejorando la comodidad de los recursos de información para dentro de la red del campus.

Para describir la variable dependiente: Seguridad de la información**,** se consideró tomar los conceptos:

Según, Verdejo (2019):

Define un ataque de la seguridad de información viene siendo DoS a una red IP siendo el cese total o parcial (temporal o total) del servicio a las computadoras conectadas a Internet. Verdejo [2] explica que existen dos tipos de DoS: a) Denegación de servicio simple, donde el ataque se origina desde una única fuente de denegación, y b) Denegación de servicio distribuida, donde existen múltiples fuentes de coordinación donde se produce un ataque gradual, estilo giratorio o ataque a gran escala.

Para INICTEL:

Una VPN es una red privada de conexión segura establecida a dentro o través de la red pública no confiable. En este estudio, se utilizó el protocolo PPTP, que permite encapsular diferentes protocolos LAN en paquetes IP sin que el usuario lo perciba. Según la explicación proporcionada por INICTEL, el protocolo PPTP utiliza dos canales de comunicación: uno para el control y otro para transportar el tráfico de la red privada. El canal de control se establece mediante una conexión TCP al puerto 1723 del servidor de acceso, mientras que el canal de datos lleva el tráfico de la red privada utilizando el protocolo IP.

Según la investigación realizada, Jeong, C. Y (2019),

Se examinó el impacto de las brechas de seguridad y las inversiones en seguridad de TI en los competidores de una empresa. Se recopilaron datos sobre incidentes de brechas de seguridad y anuncios de inversiones en seguridad de TI, y se encontraron pruebas sustanciales que respaldan la hipótesis de que las brechas de seguridad tienen un efecto de competencia. Cuando una empresa sufre una brecha, sus competidores tienen la oportunidad de adquirir poder de mercado. En cuanto a las inversiones en seguridad de TI, se observó un efecto de contagio positivo, donde los inversores consideran que las inversiones en seguridad de una empresa aumentan el nivel de la empresa a través de la seguridad, beneficiando también a los competidores. Además, se encontró que el efecto de competencia era mayor cuando las brechas ocurrieron después de las inversiones en seguridad previas. Estos hallazgos demuestran la interdependencia entre las brechas de seguridad y las inversiones en el mercado.

Para Ahmad, Z(2019), el propósito de su investigación es explicar cómo la monitorización de la S.I. y otros efectos del aprendizaje social influyen en el

comportamiento de seguridad de los empleados. Se identificaron seis constructos significativos, como la norma subjetiva, la expectativa de resultados y la autoeficacia, que determinan este comportamiento. Mediante el uso de una encuesta en línea, se recopilaron datos para evaluar estos constructos y se utilizó la teoría cognitiva social como marco teórico. Este estudio proporciona información valiosa sobre cómo ayudar con las prácticas de la S.I. al abordar el comportamiento humano al proteger los S.I.

Comenta Ng, K. C. (2021):

Examina cómo la supervisión de la seguridad de la información y diferentes características que afectan el aprendizaje social determinan el comportamiento de aseguramiento de la seguridad de los empleados. Se utilizó la (PMT)Teoría de la Motivación de Protección como inicio teorico y se recopiló información a través de cuestionarios en línea de 1,383 individuos que se enfrentaban a posibles ciberataques en sus correos electrónicos. Los resultados revelaron que la ambivalencia actitudinal, generada por la contradicción entre recompensas inadecuadas y normas sociales, afecta las evaluaciones de afrontamiento y motivación de protección de los empleados, lo cual impacta en su comportamiento de protección. Este estudio contribuye al campo de la S.I. al aceptar la ambivalencia actitudinal como un factor relevante en el comportamiento de aseguramiento de la seguridad. Además, proporciona recursos prácticos y teóricos en el diseño de estrategias de seguridad más efectivas y para evitar la ambivalencia actitudinal.

Para describir la Metodología Top-Down, el marco de este proyecto, se empleará la metodología top-down como enfoque principal. La metodología top-down se ha reconocido por su enfoque estructurado y sistemático, y se considera apropiada para guiar el este proceso de manera eficiente. se llega considerar las siguientes definiciones:

Según Heart, T. (2019):

Nos define la metodología de su estudio, la metodología top-down empleada consta de seis pasos consecutivos que se enfocan en la implementación de sistemas de registros. En primer lugar, la etapa de Preparación se centra en identificar los requisitos clave y establecer el objetivo del proyecto. A continuación, en la fase primera se establecen los requisitos generales de la red y se eligen las

tecnologías adecuadas para la solución propuesta. El siguiente paso, la etapa de Diseño, se dedica a desarrollar un diseño detallado de la solución, abordando ambos aspectos, siendo físico como el lógico de infraestructura de la red. Posteriormente, en la etapa de Implementación se lleva a cabo la instalación y configuración del sistema de acuerdo con el diseño previo. La etapa de Operación se encarga de poner en marcha el sistema y supervisar su funcionamiento, realizando ajustes y solucionando problemas identificados. Por último, la etapa de Optimización busca mejorar continuamente el sistema, corrigiendo errores y actualizando características según sea necesario.

Para Sánchez, Saul:

En su trabajo sobre la implementando la VPN Zero trust en la gestión del servidor de archivos a una empresa, Sánchez, S. (2022) aborda la necesidad de darle mejora para que acceda a los diferentes recursos el contexto del laborar virtualmente durante la pandemia de COVID-19. Para ello, propone el uso VPN basada en la metodología top-down y la herramienta Zero Tier One. La implementación exitosa de esta VPN ha permitido que el personal acceda desde cualquier momento y cualquier lugar hacia la información compartida, lo que ha aumentado la productividad y ha brindado a la dirección de la empresa un acceso conveniente a la información de toma de decisión.

Para Araujo, J.(2017):

Donde nos habla de la mejora de la gestión a través de la implementación, el control sobre el uso de la red pública de internet para la empresa Consorcio Río Mantaro a través del método Top-Down examina la problemática relacionada con el consumo de datos en la empresa y el servicio de internet ofrecido, el cual se ve afectado debido al acceso abierto a internet, generando que los usuarios enfrenten dificultades en sus labores diarias. A través de la aplicación de la metodología top-down, compuesta por cuatro etapas: primero es analizar, luego diseñar la red lógica, y por tercer paso diseñar la red física y pruebas de optimización, se identifican los objetivos tanto empresariales como técnicos, se seleccionan los equipos adecuados y se implementan estrategias de seguridad con el fin de aumentar la calidad de la transmisión del del servicio de red. Mediante el uso de la herramienta MikroTik, se definen políticas que permiten reducir el consumo

individual de datos y optimizar los sistemas utilizados en la empresa Consorcio Río Mantaro.

"Desarrollo de un modelo paramétrico-asociativo de un radiador automovilístico utilizando la metodología top-down en la modelación CAD avanzada" describe una metodología que se basa en la estructura top-down para abordar el modelado de productos complejos, con un enfoque específico en el desarrollo de un modelo de radiador automovilístico. La metodología propuesta utiliza una estructura fundamental o esqueleto que contiene los criterios y elementos clave del proyecto, como las posiciones de montaje y los espacios ocupados por los subsistemas y las partes del radiador. Esta estructura optimizada permite una gestión completa y paramétrica del modelo durante su desarrollo, independientemente de la complejidad geométrica y las variaciones que puedan surgir en diferentes etapas del proyecto. Este estudio tiene como objetivo mostrar cómo la metodología top-down en la modelación CAD avanzada puede facilitar el proceso de diseño y optimizar el marco de construcción un radiador automovilístico, permitiendo una mayor flexibilidad y eficiencia en el desarrollo del producto.

Siguiendo con la metodología top-down, nos cuenta Camas, D. (2020) en su estudio de investigador, donde el obtiene principal fue aumentar en los servicios de comunicación y su calidad ofrecida el entorno universitario, garantizando un acceso fluido a los S.I. Luego es necesario para esta investigación, que se emplearon diversas metodologías, incluyendo técnicas como encuestas, evaluar y revisar los documentos. Además, se aplicó el método Top-down para el diseño de red para analizar y rediseñar la infraestructura existente. También se hizo una prueba de “T-Student” para validar la hipótesis general, y los resultados respaldaron la hipótesis alterna. Esta investigación pudo demostrar que la metodología Top-down ayuda positivamente creando un impacto significativo en calidad de comunicación en la Universidad. Como resultado de esta mejora, se logró optimizar los servicios de comunicación, y se generó la documentación necesaria para que el personal a cargo pueda administrar la red de manera eficiente y satisfacer futuras necesidades.

En el libro de Banoth, R., Gugulothu, N., & Godishala, A. K. (2023). A Comprehensive Guide to Information Security Management and Audit. Boca Raton,

FL: CRC Press, Nos hablade la confidencialidad donde se refiere a los ataques pasivos son atacados para transmitir datos y la divulgación no autorizada. Implica asegurar que la información solo sea accesible para personas o sistemas autorizados, así como proteger el flujo de tráfico de análisis no autorizados. Un ejemplo ilustrativo es el caso de Frodo en su viaje para destruir el anillo, donde se mantuvo en secreto su posesión para asegurar su confidencialidad. De manera similar, en una transacción en línea, es crucial proteger la confidencialidad del número de tarjeta de crédito para evitar su exposición a terceros no autorizados.

También para el autor cuando hablamos de Integridad de la información, comenta: La integridad de los datos implica que no pueden ser alterados sin autorización. Esto se aplica tanto a flujos de mensajes, mensajes individuales o campos específicos dentro de un mensaje. Existen servicios de integridad orientados a la conexión y sin conexión, los cuales garantizan que los mensajes se reciban sin modificaciones no autorizadas, duplicaciones, inserciones, reordenamientos o reproducciones. La integridad se encarga de proteger los datos contra manipulaciones no autorizadas, asegurando que los mensajes lleguen sin cambios no deseados. Un ejemplo es cuando Frodo y su grupo recibieron una carta sellada de Gandalf en Bree, donde romper el sello era una forma de verificar la integridad del mensaje. Sin embargo, es importante destacar que los métodos actuales para garantizar la integridad son más avanzados que los sellos de cera utilizados en el pasado.

La disponibilidad se refiere a la característica del sistema abordando la capacidad de recuperarse o quizás un recurso para ser utilizable y accesible cuando lo solicita una entidad autorizada. Puede verse comprometida por diversos ataques, algunos de los cuales pueden contrarrestarse con medidas automatizadas como la autenticación y el cifrado, mientras que otros necesitan tomar medidas de control físico para recuperar o evitar la pérdida de disponibilidad en un sistema distribuido. En términos más sencillos, la disponibilidad implica que los datos estén disponibles cuando el usuario los necesite. Un ejemplo ilustrativo es cuando Frodo contaba con la protección de su camisa de mithril durante sus viajes, aunque no siempre era conocida por sus compañeros. Sin embargo, cuando la necesitaba (por ejemplo, para protegerse de una lanza), estaba disponible para él.

Tabla N° 1 *Comparativa de Metodologías*

Criterios	Top-Down	Bottom-Up	Cisco
Enfoque Principal	Comienza desde lo general hasta lo específico.	Inicia desde lo específico y se expande a lo general.	Proporciona un marco estructurado para diseñar, implementar y mantener redes.
Diseño	Centrado en la visión global y la planificación estratégica.	Se enfoca en la implementación práctica y la optimización de detalles.	Ofrece un enfoque detallado para diseñar soluciones adaptadas a las necesidades.
Implementación	La implementación sigue la estructura y el diseño planificados.	La implementación puede variar según los elementos individuales y luego se integra.	Proporciona fases detalladas para la implementación, prueba y despliegue de soluciones.
Ventajas	Mejor para una visión estratégica inicial y decisiones de alto nivel.	Permite adaptación y flexibilidad a cambios y ajustes durante el proceso.	Ofrece un enfoque completo y estructurado, asegurando coherencia y eficiencia.
Desafíos	Puede ser menos flexible ante cambios imprevistos o emergentes.	Podría carecer de una visión global, provocando inconsistencias.	Requiere un tiempo y recursos considerables para seguir todos los pasos.
Documentación	Requiere documentación extensa para el diseño completo y sus objetivos.	La documentación puede ser más específica y orientada a detalles técnicos.	Proporciona documentación detallada por cada fase del ciclo la red.
Puntaje	9	5	7

Fuente: elaboración propia

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Para la investigación se usó un enfoque cuantitativo, donde Babativa, Carlos. (2017), nos dice, que la este tipo de investigaciones busca ver las relaciones

producidas en la casusa y efecto de problemas sociales, basándose en hallazgos comunes y utilizando la estadística para relacionar variables en diferentes realidades. Otros investigadores sociales pueden utilizar estos fundamentos para futuros estudios.

De otra manera, para el tipo de investigación se considera descriptiva, por lo que Bruce, A.(2017) comenta, "La investigación descriptiva es un diseño de investigación que tiene como objetivo describir las características de una población o fenómeno. La investigación descriptiva se puede utilizar para describir el estado actual de un fenómeno, para identificar tendencias o para comparar diferentes grupos de personas o cosas. Uno de los métodos más comunes de investigación descriptiva es la encuesta."

También este estudio se encuentra con un diseño experimental, por ello Galarza, Ramos (2021). la investigación experimental implica la manipulación intencional de una V.I. y el analizar de su efecto en una V.D. Este enfoque implica manipular la V.I. en diferentes niveles y la medición de la variable dependiente antes y después del experimento

Formula:

$$G = O1 \ X \ O2$$

Dónde:

- G = Grupo experimental del consorcio.
- O1= Medición del grupo G antes del diseño de un VPN para mejorar la seguridad en el consorcio.
- X = VPN para mejorar la seguridad en el consorcio
- O2 = Medición del grupo G después del diseño de un VPN para mejorar la seguridad en el consorcio.

3.2. Variables y Operacionalización

Variables a trabajar son las siguientes: VPN, variable independiente cuantitativa y seguridad de la información variable dependiente cuantitativa. Se identifico 3 dimensiones siendo La Integridad, también la confidencialidad y la disponibilidad. En el tema de indicadores la primera dimensión cuenta con dos indicadores: Gestión de accesos y protección de datos En cuanto a la segunda dimensión su indicador es: Accesos y Autorización y para la tercera dimensión: Accesibilidad. Para encontrar la operacionalización de las variables diríjase al Anexo 1.

3.3 Población, muestra y muestreo

Nos dice Condori, Porfirio (2020), Los elementos que son accesibles o forman parte de la unidad de análisis están relacionados con el contexto específico en el cual se lleva a cabo la investigación. (p3).

Para la investigación se usó como población a 10 empleados del consorcio.

Tabla N° 2 *Población de la muestra*.

INDICADORES	CANTIDAD	UNIDAD
1. Autenticación 2. Protección de datos 3. Acceso 4. Autorización 5. Accesibilidad	10	EMPLEADO
TOTAL	10	EMPLEADOS.

Fuente: Creación Propia

También Condori, Porfirio (2020), comenta acerca de la muestra, La muestra se selecciona de manera que sea representativa de la población, compartiendo las mismas características generales que se encuentran en la población en su conjunto.

$$n = \frac{Nz^2 p\, q}{(N-1)e^2 + z^2 p\, q}$$

Figura 2 Formula de la muestra (GUBEA – Academia Gubernamental)

Dónde:

n = Tamaño de la muestra.

N = Población.

Z = Nivel de confianza.

p = Probabilidad de éxito, o proporción esperada.

q = Probabilidad de fracaso.

e = Error muestral (Error máximo admisible en términos de proporción).

$$n = \frac{10 * (1.96)^2 * 0.5 * 0.5}{(10-1) * (0.5)^2 + (1.96)^2 * 0.5 * 0.5} = 10$$

Figura 3 Obtención de Muestra

Para nuestras dimensiones ya mencionadas, se usará el tamaño de muestra de 10 empleados.

Para el tema del muestreo se va usar en esta investigación es de probabilístico aleatorio simple y para esto Tamara Otzen (2017), asegura que todos los individuos que componen el objetivo poblacional tengan igual puedan ser seleccionados para la muestra. Esto implica que la probabilidad de selección de un sujeto específico en estudio "x" sea independiente de la probabilidad de selección de los demás individuos que formaran parte de esta población. (p.2)

3.4 Técnicas e instrumentos de recolección de datos

Para llevar a cabo el estudio mencionado, se empleó un cuestionario como método principal para recopilar la información necesaria., En este sentido, Según Sierra Bravo (1998:305 – citado de Conejero, Manuel,2017) se menciona que la encuesta por observación es el método sociológico de investigación más relevante y ampliamente utilizado. Esta técnica proporciona una forma de recopilar datos al interrogar a los miembros de una comunidad con el objetivo de obtener información.

Nos comenta Useche M. et al, (2019), Sobre el instrumento que cuando se elige como técnica de recolección de datos el cuestionario viene siendo el instrumento clave es el cuestionario estandarizado, que consta en una lista de enunciados estandarizadas que se leen de forma literal y siguen el mismo orden con cada encuestado (Cea, 2001- citado en Useche M. et al, 2019). El cuestionario puede adoptar diferentes formatos, utilizando preguntas abiertas o cerradas, afirmaciones o instrucciones, para recopilar información sobre aspectos específicos. Aunque presenta ventajas y desventajas, el cuestionario se usa sobre un tema o problea peculiar y de esa manera obtener los datos e información necesaria, ya que es un instrumento rigurosamente estandarizado que traduce y opera de manera precisa los problemas objeto de investigación (Hurtado, 1998; Ander-Egg, 2003- Useche M. et al, 2019).

Sobre la recolección de datos nos comenta, Useche M. et al, (2019), la etapa de recolección de datos implica la recopilación y organización de información relevante sobre variables, hechos, contextos, categorías y comunidades relacionadas con la investigación. Estos datos se obtienen mediante la utilización de instrumentos que deben ser precisos, fiables y previamente validados. Para las ciencias, es fundamental comprender el proceso, el lugar y el contexto en el que la recolección de datos se llevara a cabo, ya que constituye una fase operativa crucial en el diseño de investigación para alcanzar los objetivos planteados.

Tabla N°3 Instrumento de recolección de datos

DIMENSION	INDICADORES	TECNICA	INSTRUMENTO
Confidencialidad	Autenticación	Encuesta	Cuestionario

	Protección de datos	Encuesta	Cuestionario
Integridad	Acceso	Encuesta	Cuestionario
	Autorización	Encuesta	Cuestionario
Disponibilidad	Accesibilidad	Encuesta	Cuestionario

Fuente Elaboración Propia

La investigación es de tipo Confiable, y dice Campo & Oviedo, (2008 – Citado de Tuapanta, Jorge,2017), para hablar de la confiabilidad de tipo consistencia interna debemos decir que se relaciona con el nivel de correlación existente entre los ítems de una escala. Para evaluar la consistencia interna, se utilizan diferentes métodos según el tipo de escala. Para escalas politómicas se utiliza el coeficiente de alfa de Cronbach. Esto permitira estimar la confiabilidad de la escala de manera interna y son ampliamente utilizados en la investigación.

Tabla N° 4 Nivel de Confiabilidad

ESCALA	CONSISTENCIA
0.80 ≤ X < 1.00	Elevado
0.60 ≤ X < 0.80	Aceptable
0.40 ≤ X < 0.60	Regular
0.20 ≤ X < 0.40	Bajo
0.00 < X < 0.20	Muy Bajo

Fuente Elaboración Propia

Continuando con la confiabilidad, se aplicará una medición por el coeficiente de Cronbach, donde Rodríguez, J. (2019La confianza en una medición se refiere al grado de certeza de que la medición es precisa. Está determinado por la consistencia de las mediciones cuando se repite el proceso de medición. Una

medición con alta confianza es aquella que produce los mismos resultados cada vez que se toma. (p.5)

$$\propto = \frac{K}{K-1}\left[1 - \frac{\sum S_i^2}{S_T^2}\right]$$

Figura 4 Ecuación de Cronbach (GUBEA - Academia Gubernamental)

Dónde:

α = Coeficiente de Cronbach

K = Número de ítems

S_i^2 = Suma de varianzas de cada item

S_T^2 = Varianza del total de filas

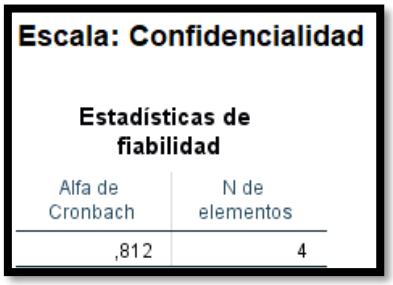
Para la siguiente Figura podemos observar el resultado de nuestro cuestionario de confiabilidad de la variable S.I teniendo como valor de Alfa de Cronbach de 0,849 analizado en el SPSS25, este resultado indica que nuestro instrumento de recolección de datos es aceptable y muestra consistencia interna en la medición de dicha variable.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,849	11

Figura 5 Estadístico de Fiabilidad de Seguridad de la Información (Elaboración propia)

También como se puede observar en la siguiente figura, nuestro resultado de confiabilidad tiene un valor de Alfa de Cronbach de 0.812 en el SPSS25, entonces esto significa que nuestro instrumento de Confidencialidad tiene un aceptable grado de confiabilidad, validando su uso para la recolección de datos.



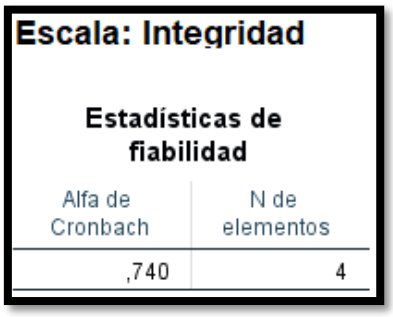
Escala: Confidencialidad

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,812	4

Figura 6 Estadístico de Fiabilidad de Confidencialidad (Elaboración propia)

De igual manera para nuestra dimensión Integridad, el resultado de la confiabilidad en el SPSS25, para el valor de Alfa de Cronbach fue de 0.812. Lo que significa que el instrumento es confiable, y de esta manera validando su uso para la recolección de datos.



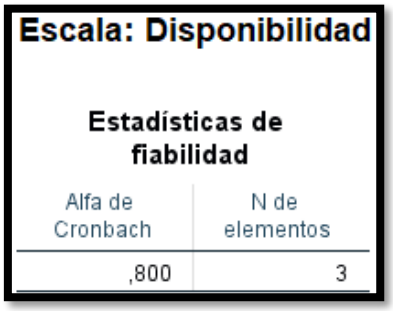
Escala: Integridad

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,740	4

Figura 7 Estadístico de Fiabilidad de Integridad (Elaboración propia)

Tambien para nuestra dimensión Disponibilidad, el resultado de la confiabilidad en el SPSS25, para el valor de Alfa de Cronbach fue de 0,800. Lo que nos garantiza que el instrumento es confiable.



Escala: Disponibilidad

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,800	3

Figura 8 Estadístico de Fiabilidad de Disponibilidad

3.5 Procedimiento

Para nuestra tesis, se lleva a cabo una evaluación exhaustiva de los aspectos relacionados con la S.I. en nuestro consorcio. Durante la etapa de elaboración de la investigación, se llevó a cabo un minucioso procedimiento que involucró la

revisión e inspección de los datos recopilados. Estos datos fueron registrados en una base de datos en formato Excel, asegurando su correcta organización y almacenamiento. Posteriormente, se procedió al diseño de los instrumentos de recolección de datos, siendo el cuestionario la herramienta principal en esta investigación. Para garantizar su confiabilidad, se sometió al cuestionario a una prueba de confiabilidad mediante el pretest, y se evaluó su consistencia interna con el alfa de Cronbach mediante una prueba piloto. Una vez completada esta fase, se procedió a la codificación de la información utilizando el software SPSS26, que permitió realizar un análisis detallado y preciso de los datos recopilados.

En relación al análisis de la normalidad de los datos, se realizarán distintas pruebas en función de la población de muestra. En primer lugar, se consideró la cantidad de la población, y al ser menor a 35, se utilizará el test de Shapiro-Wilk para evaluar la normalidad de los datos. Esta prueba será utilizada específicamente por la naturaleza de la muestra, que presentaba un tamaño reducido. De esta manera, se asegurará un análisis adecuado de la normalidad de los datos y se obtuvieron resultados confiables para el estudio en cuestión.

3.6 Método de análisis de datos

Para analizar detalladamente se optó por usar el software SPSS 26, entonces Rivadeneira, J. (2020) comenta, que se utiliza para analizar cualitativamente los datos, aplicándose a muchas ramas de esta Ciencia, resaltando por su comprensión fácil, su utilidad, y manejo adecuado, teniendo dentro de manera nativa una variedad muy amplia variedad de temas estadísticos orientados en su mayoría a las ciencias sociales, llegando cubrir las diferentes necesidades de operaciones y cálculos estadísticos para profesionales e investigadores en el campo al cual se aplique.(p.18)

Para esta investigación se observaron mediante un análisis aplicativo para las dos variables, vpn (V. Independiente), el cual mejorará la Seguridad de Información (V. Dependiente). Para obtener dichos resultados se usará el cuestionario como instrumento de recolección de datos.

3.7 Aspectos éticos

La presente investigación se adhiere estrictamente a las normativas vigentes a nivel mundial, asegurando un riguroso de la propiedad intelectual y de las fuentes citadas en este trabajo. Se realiza una adecuada referencia a los autores, lo cual garantiza la solidez y calidad de la estructura informativa del proyecto. De esta manera, se busca generar un estudio de alta calidad y utilidad para investigadores futuros que deseen obtener información relevante.

IV. RESULTADOS

La investigación se llevó a cabo en el Consorcio Andia, para obtener una mejora en la Seguridad de la información. El objetivo de nuestro estudio fue las 10 preguntas obtenidas de la CISA (Cibersecurity & Infraestructure Security Agency), y realizadas a nuestros 10 colaboradores para la variable Seguridad de la información.

4.1 Análisis Descriptivo

Para nuestro estudio se utilizó una Red Privada Virtual para mejorar la S.I. en el Consorcio Andia. Para esto se usó un Pretest el cual tenía la intención de registrar en qué estado se encontraba la actual estructura que manejaba el Consorcio, luego tras implementar la VPN se volvió a registrar un Post-Test para ver la variación y mejora en nuestra implementación, de esta manera, se presenta de manera descriptiva los resultados en las tablas:

Variable Seguridad de la información:

Se observa que la Media de la S.I. en el pre-test fue de 26,5, mientras que en el post-test se ve un aumento en 40. Esto demuestra que hubo un aumento del pre hacia el post-test demostrando la hipótesis general.

Tabla 5 Medidas descriptivas para nuestra variable general Seguridad de la Información.

	PRE - TEST						POST - TEST					
Muestra	S.I.	Autenticación	Protección de datos	Accesos	Autorización	Accesibilidad	S.I	Autenticación	Protección de datos	Accesos	Autorización	Accesibilidad
1	40	7	7	7	7	12	52	10	9	9	9	15
2	21	3	3	2	4	9	49	8	10	9	9	9
3	33	6	6	4	8	8	47	9	8	10	8	12
4	23	3	3	4	4	8	45	9	9	8	6	9
5	39	10	10	7	5	8	41	7	7	9	6	12
6	34	7	7	10	7	7	39	7	8	8	6	10
7	29	7	7	5	7	6	36	6	6	8	8	8
8	23	5	5	4	4	5	37	8	8	6	6	9
9	24	4	4	5	4	6	34	8	6	7	5	8
10	17	4	4	2	4	3	29	8	9	5	2	5
Media	**26,5**	5,5	5,5	4,5	4,5	7,5	**40**	8	8	8	6	9

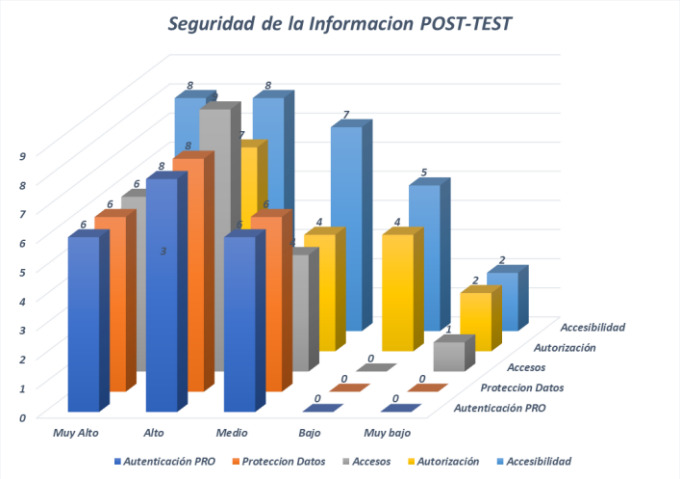


Figura 9 Grafico de barras Pre-test por opción marcada en cada indicador

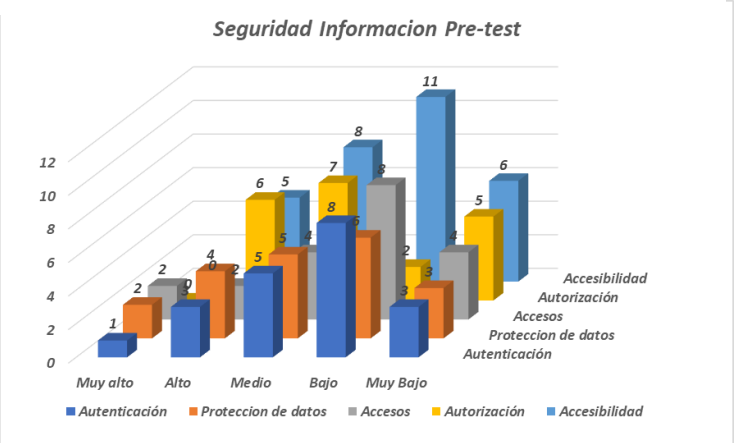


Figura 10 Grafico de barras Post-Test por opción marcada en cada indicador

Indicador: Autenticación

Se observa en la siguiente tabla los resultados descriptivos que se obtuvieron del indicador de Autenticación

Tabla 6 Medidas descriptivas del Indicador Autenticación antes y después de implementar el VPN.

Muestra	Autenticación Pre-test	Autenticación Post-test
1	7	10
2	3	8
3	6	9
4	3	9
5	10	7
6	7	7
7	7	6
8	5	8
9	4	8
10	4	8
Media	5,5	8

Tabla 7 Tabla comparativa entre las opciones marcadas para la variable Autenticación en el Pre-test y el Post-test

Leyenda	Autenticación Pre-test	Autenticación Post-test
Muy Alto	1	6
Alto	3	8
Medio	5	6
Bajo	8	0
Muy bajo	3	0

Para la Autenticación se obtuvo un valor de 5.5 en el Pretest, mientras que en el Post-test se obtuvo un valor de 8, Tambien observamos en el grafico que el pretest Bajo obtuvo 8 puntos y que el post-test el más puntaje fue Alto con 8 puntos.

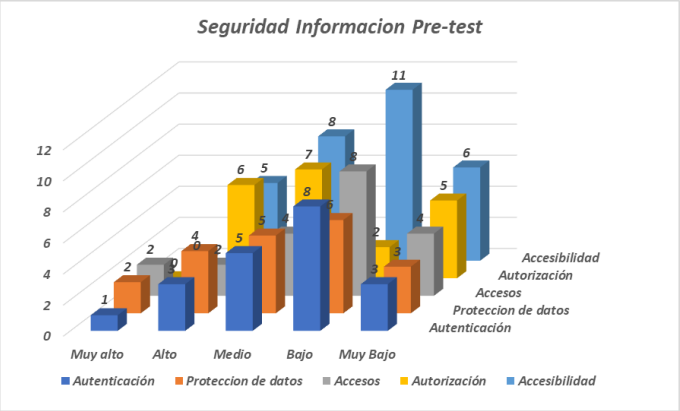


Figura 11 Indicador de Autenticación del pre-test y post-test del VPN

Indicador: Protección de datos

Se puede observa en la taba X los resultados descriptivos que se obtuvieron del indicador Protección de datos.

Tabla 8 Medidas descriptivas del Indicador de Protección de datos antes y después de implementar el VPN.

Muestra	Protección de datos Pre	Protección de datos Post
1	7	9
2	3	10
3	6	8
4	3	9
5	10	7
6	7	8
7	7	6
8	5	8
9	4	6
10	4	9
Media	5,5	8

Tabla 9 Tabla comparativa entre las opciones marcadas para la variable Protección de datos en el Pre-test y el Post-test

Leyenda	Proteccion de datos PRE	Proteccion de Datos PRO
Muy Alto	2	6
Alto	4	8
Medio	5	6
Bajo	6	0
Muy bajo	3	0

Para el indicador Protección de Datos, se consiguió un valor de 5,5 en el pretest, mientras que en el Posttest tuvo un valor de 8, esto de igual manera ratifica que existe una diferencia entre el antes y después de la implementación VPN, asi mismo se obtuvo que la votacion en el pre-test fue de BAJO con 6 puntos y en el post-test fue ALTO con 8 puntos

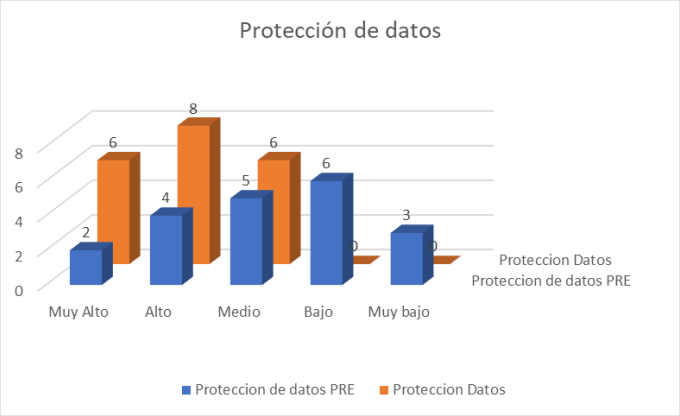


Figura 12 Indicador de Protección de pre-test y post-test del VPN

Indicador Acceso:

Se observa que en la siguiente tabla los resultados descriptivos que se obtuvieron del indicador Accesos

Tabla 10 Medidas descriptivas del Indicador Accesos para el pre-test y post-test de la implementación del VPN.

Muestra	Accesos Pre-test	Accesos Post-test
1	7	9
2	2	9
3	4	10
4	4	8
5	7	9
6	10	8
7	5	8
8	4	6
9	5	7
10	2	5
Media	4,5	8

Tabla 11 Tabla comparativa entre las opciones marcadas para la variable Acceso en el Pre-test y el Post-test

Leyenda	*Accesos Pre-test*	*Accesos Post-test*
Muy Alto	2	6
Alto	2	9
Medio	4	4
Bajo	8	0
Muy bajo	4	1

Para el indicador acceso se obtuvo un valor de 4,5 en el Pretest, mientras que en el Post-test se obtuvo un valor de 8 y esto a su Vez ratifica que existe una diferencia antes y el después de haber implementado la VPN. Tambien Podemos ver que la opción mas elegida en el PRE-TEST fue bajo con 8 puntos, mientras que en el POST-TEST es de ALTO con 9 puntos

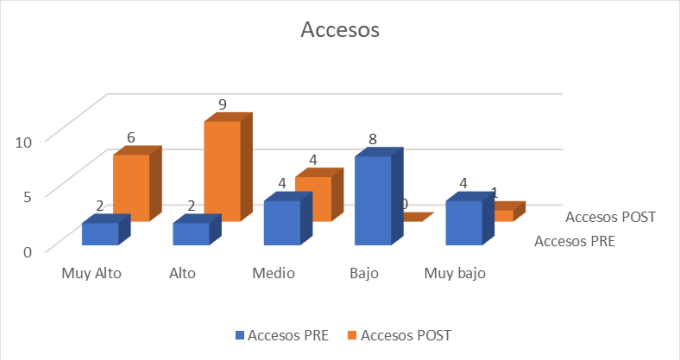


Figura 13 Indicador de Accesos para el pre-test y post-test

Indicador: Autorización

Se observa que en la siguiente tabla los resultados descriptivos que se obtuvieron del indicador Autorización .

Tabla 12 Medidas descriptivas del Indicador Autorización pre-test y post-test de la implementación del VPN.

Muestra	Autorización Pre-test	Autorización Post-test
1	7	9
2	4	9
3	8	8
4	4	6
5	5	6
6	7	6
7	7	8

8	4	6
9	4	5
10	4	2
Media	4,5	6

Tabla 13 Tabla comparativa entre las opciones marcadas para la variable Autorización de datos en el Pre-test y el Post-test

Leyenda	*Autorización Pre-test*	*Autorización Post-test*
Muy Alto	0	3
Alto	6	7
Medio	7	4
Bajo	2	4
Muy bajo	5	2

Para el indicador Autorización se obtuvo un valor de 4,5 en el Pretest, mientras que en el Post-test se obtuvo un valor de 6, y esto a su vez ratifica que existe una diferencia antes y el después de haber implementado la VPN. En el grafico se observa que la opción más escogida en el Pre-test fue Medio con 7 puntos, y en el post-test Alto con 7 puntos.

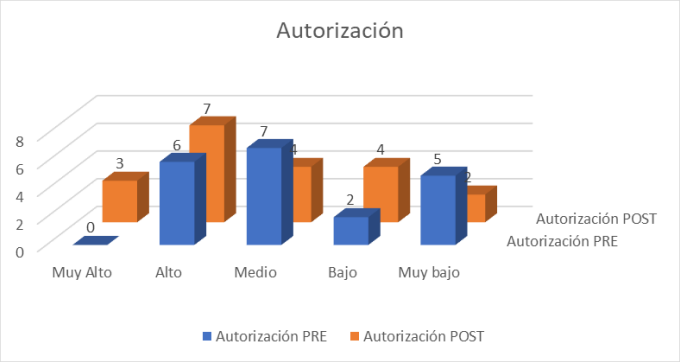


Figura 14 Indicador de Autorización para el pre-test y post-test

Indicador: Accesibilidad

Se observa que en la siguiente tabla los resultados descriptivos que se obtuvieron del indicador Accesibilidad.

Medidas descriptivas del Indicador Accesibilidad antes y después de implementar el VPN.

Tabla 14 Medidas descriptivas del Indicador Accesibilidad para el pre-test y post-test de la implementación del VPN

Muestra	Accesibilidad Pre-test	Accesibilidad Post-test
1	12	15
2	9	9
3	8	12
4	8	9
5	8	12
6	7	10
7	6	8
8	5	9
9	6	8
10	3	5
Media	7,5	9

Tabla 15 Tabla comparativa entre las opciones marcadas para la variable Accesibilidad de datos en el Pre-test y el Post-test

Leyenda	*Accesibilidad Pre-test*	*Accesibilidad Post-test*
Muy Alto	0	8
Alto	5	8
Medio	8	7
Bajo	11	5
Muy bajo	6	2

Para el Valor de Accesibilidad se obtuvo un valor de 7,5 en el Pretest, mientras que en el Post-test se obtuvo un valor de 9, de igual manera para el grafico se observa que en el pre-test Bajo obtuvo 11 puntos mientras que para el Post-test Muy alto y Alto obtuvieron 8 puntos.

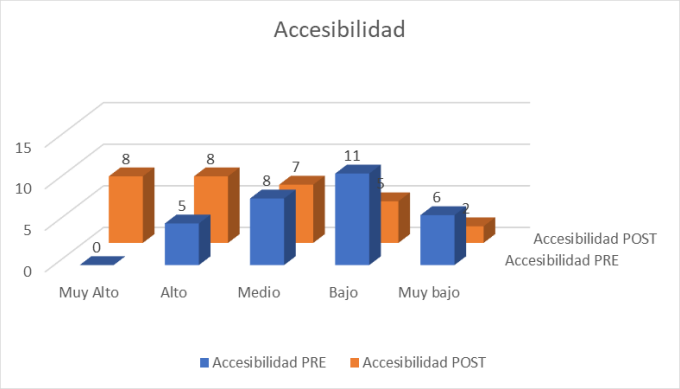


Figura 15 Indicador de Accesibilidad para pre-test y post-test

4.2 Análisis Inferencial

Para nuestras pruebas de normalidad de nuestra variable general, se utilizó Shapiro-Wilk debido a que el numero de la muestra es inferior a 50.

H0: Las variables tienen una distribución normal.

H1: Las variables no tienen una distribución normal.

Tabla 16 Pruebas de normalidad Seguridad Información

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
SeguridadInformacion_Pre	,207	10	,200*	,933	10	,480
SeguridadInformacion_Post	,114	10	,200*	,978	10	,953
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Debido a que el Sig. es mayor al nivel 0.05, por lo tanto, aceptamos la hipótesis Nula y rechazamos la hipótesis alterna. Se utilizara la prueba de Wilcoxon para nuestras pruebas de hipótesis, debido a su variable cuantitativa discontinuas se incluyen las pruebas estadísticas no paramétricas.

A continuación, se demuestran las validaciones de las hipótesis

Hipótesis General de la Investigación

H0: La implementación de una VPN basada en la metodología top-Down no mejora la seguridad de la información en un consorcio.

Ha: La implementación de una VPN basada en la metodología top-Down mejora la seguridad de la información en un consorcio

Tabla 17 Prueba Estadística Wilcoxon Hipotesis General

	SeguridadInformacion_Post - SeguridadInformacion_Pre
Z	-2,807[b]
Sig. asintótica(bilateral)	,005
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

El análisis de rangos con signo de Wilcoxon para muestras independientes mostró una predominancia de rangos positivos ($p \leq 0,05$). Por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alterna de que las puntuaciones del posttest son significativamente mayores que las puntuaciones del pretest. Se rechaza la hipótesis nula y se acepta la hipótesis alterna, la implementación de una VPN basada en la metodología top-Down mejora la seguridad de la información en un consorcio.

Hipótesis Específica 1

De igual manera para nuestra indicador Autenticación, las pruebas de normalidad

H0: Las variables tienen una distribución normal.

H1: Las variables no tienen una distribución normal.

Tabla 18 *Pruebas de normalidad Autenticación*

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Autenticacion_Pre	,164	10	,200*	,918	10	,338
Autenticacion_Post	,200	10	,200*	,953	10	,703
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Debido a que el Sig. es mayor al nivel 0.05, por lo tanto, aceptamos la hipótesis Nula y rechazamos la hipótesis alterna. Se utilizara la prueba de Wilcoxon para nuestras pruebas de hipótesis, debido a su variable cuantitativa discontinuas se incluyen las pruebas estadísticas no paramétricas.

A continuación, se demuestran las validaciones de las hipótesis

H_0 La implementación de una VPN basada en la metodología top-Down no contribuye a mejorar la gestión de autenticación en el consorcio.

H_1 La implementación de una VPN basada en la metodología top-Down contribuye a mejorar la gestión de autenticación en el consorcio.

Tabla 19 *Prueba Estadística Wilcoxon Autenticación*

	Autenticacion_Post - Autenticacion_Pre
Z	-2,153[b]
Sig. asintótica(bilateral)	,031
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

La prueba de Wilcoxon para comparar un grupo antes y después, hablamos de muestras relacionadas. Dado que el valor de p es 0,035 menor a $p < 0.05$. Entonces se rechaza la H_0 y se acepta la H_a., Por lo tanto, La implementación de una VPN basada en la metodología top-Down contribuye a mejorar la autenticación en el consorcio.

Hipótesis Específica 2

De igual manera para nuestro indicador Autenticación, las pruebas de normalidad

H0: Las variables tienen una distribución normal.

H1: Las variables no tienen una distribución normal.

Tabla 20 *Pruebas de normalidad Protección*

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
ProteccionDatos_Pretest	,164	10	,200*	,918	10	,338
ProteccionDatos_Posttest	,200	10	,200*	,918	10	,344
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Debido a que el Sig. Es 0,3 mayor al nivel 0.05, por lo tanto, aceptamos la hipótesis Nula y rechazamos la hipótesis alterna. Se utilizara la prueba de Wilcoxon para nuestras pruebas de hipótesis, debido a su variable cuantitativa discontinuas se incluyen las pruebas estadísticas no paramétricas.

A continuación, se demuestran las validaciones de las hipótesis

H_0 La implementación de una VPN basada en la metodología top-Down no contribuye a mejorar la protección de datos en el consorcio.

H_a La implementación de una VPN basada en la metodología top-Down contribuye a mejorar la protección de datos en el consorcio

Tabla 21 *Prueba Estadística Wilcoxon Protección de datos*

	ProteccionDatos_Posttest - ProteccionDatos_Pretest
Z	-1,995[b]
Sig. asintótica(bilateral)	,046
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

La prueba de Wilcoxon para comparar un grupo antes y después, hablamos de muestras relacionadas. Dado que el valor de p es 0,046 menor a $p < 0.05$. Entonces se rechaza la H_0 y se acepta la H_a., Por lo tanto, La implementación de una VPN basada en la metodología top-Down contribuye a mejorar la protección de datos en el consorcio.

Hipótesis Específica 3

De igual manera para nuestra indicador Autenticación, las pruebas de normalidad

H0: Las variables tienen una distribución normal.

H1: Las variables no tienen una distribución normal.

Tabla 22 Pruebas de normalidad Accesos

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Accesos_Pretest	,200	10	,200*	,918	10	,340
Accesos_Posttest	,226	10	,158	,929	10	,441
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Debido a que el Sig. es mayor al nivel 0.05, por lo tanto, aceptamos la hipótesis Nula y rechazamos la hipótesis alterna. Se utilizara la prueba de Wilcoxon para nuestras pruebas de hipótesis, debido a su variable cuantitativa discontinuas se incluyen las pruebas estadísticas no paramétricas.

A continuación, se demuestran las validaciones de las hipótesis

H_0 La implementación de una VPN basada en la metodología top-Down no contribuye a mejorar el control de acceso en el consorcio.

H_a La implementación de una VPN basada en la metodología top-Down contribuye a mejorar el control de acceso en el consorcio.

Tabla 23 *Prueba Estadística Wilcoxon Accesos*

	Accesos_Posttest - Accesos_Pretest
Z	-2,532[b]
Sig. asintótica(bilateral)	,011
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

Se observa que existe predominancia de rangos positivos que indica que las puntuaciones del posttest son mayores que las puntuaciones del pretest. Dado que el valor de p es 0,011siendo menor a 0.05. Entonces se rechaza la H_0 y se acepta la H_a., Entonces, La implementación de una VPN basada en la metodología top-Down contribuye a mejorar la gestión de acceso en el consorcio.

Hipótesis Específica 4

De igual manera para nuestra indicador Autenticación, las pruebas de normalidad

H0: Las variables tienen una distribución normal.

H1: Las variables no tienen una distribución normal.

Tabla 24 *Pruebas de normalidad Autorización*

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Autorizacion_Pretest	,302	10	,010	,770	10	,006
Autorizacion_Posttest	,207	10	,200*	,891	10	,173
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Debido a que el Sig. es mayor al nivel 0.05, por lo tanto, aceptamos la hipótesis Nula y rechazamos la hipótesis alterna. Se utilizará la prueba de Wilcoxon para

nuestras pruebas de hipótesis, debido a su variable cuantitativa discontinuas se incluyen las pruebas estadísticas no paramétricas.

A continuación, se demuestran las validaciones de las hipótesis

H_0 La implementación de una VPN basada en la metodología top-Down no contribuye a mejorar la Autorización el consorcio.

H_1 La implementación de una VPN basada en la metodología top-Down contribuye a mejorar la Autorización en el consorcio.

Tabla 25 *Prueba Estadística Wilcoxon Autorización*

	Autorizacion_Posttest - Autorizacion_Pretest
Z	-1,628[b]
Sig. asintótica(bilateral)	,103
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

La prueba de Wilcoxon para comparar un grupo antes y después, hablamos de muestras relacionadas. Dado que el valor de p es 0,103 mayor a p < 0.05. Entonces se acepta la H_0 y se rechaza la H_a., Entonces, La implementación de una VPN basada en la metodología top-Down no contribuye a mejorar la Autorización el consorcio.

Hipótesis Específica 5

De igual manera para nuestra indicador Autenticación, las pruebas de normalidad

H0: Las variables tienen una distribución normal.

H1: Las variables no tienen una distribución normal.

Tabla 26 *Pruebas de normalidad Accesibilidad*

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Accesibilidad_Pretest	,172	10	,200*	,965	10	,846
Accesibilidad_Posttest	,200	10	,200*	,948	10	,640
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Debido a que el Sig. es mayor al nivel 0.05, por lo tanto, aceptamos la hipótesis Nula y rechazamos la hipótesis alterna. Se utilizará la prueba de Wilcoxon para nuestras pruebas de hipótesis, debido a su variable cuantitativa discontinuas se incluyen las pruebas estadísticas no paramétricas.

A continuación, se demuestran las validaciones de las hipótesis

H_0 La implementación de una VPN basada en la metodología top-Down no contribuye a mejorar la Accesibilidad en el consorcio.

H_a La implementación de una VPN basada en la metodología top-Down contribuye a mejorar la Accesibilidad en el consorcio.

Tabla 27 *Prueba Estadística Wilcoxon Accesibilidad*

	Accesibilidad_Posttest - Accesibilidad_Pretest
Z	-2,687[b]
Sig. asintótica(bilateral)	,007
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

La prueba de Wilcoxon para comparar un grupo antes y después, hablamos de muestras relacionadas. Dado que el valor de p es 0,007 menor a $p < 0.05$. Entonces se rechaza la H_0 y se acepta la H_a., Por lo tanto, La implementación de una VPN basada en la metodología top-Down contribuye a mejorar la accesibilidad en el consorcio.

V. DISCUSIÓN

En esta sección, se visualizaran los resultados alcanzados tras la evaluación después de la implementación de la solución de VPN en la organización Consorcio Andia, con el propósito de determinar si satisfacen los objetivos previamente establecidos al inicio de nuestra investigación. Este es el punto en el que se examina el grado de conformidad entre nuestros resultados y las investigaciones previas que consideramos pertinentes como antecedentes para nuestro estudio. Los resultados se presentan a continuación:

En la presente investigación mediante la estadística descriptiva se demostró que con tras implementar la Red Privada Virtual basada en la metodología top-Down mejora la seguridad de la información en el Consorcio se logró un valor aceptable que demuestra nuestra hipótesis alterna, Para Pablo Huanca, en su investigación 'Implementando de una Red Privada Virtual para la S.I de los servicios de red de la IEPM CMFB – Arequipa' (2022), al analizar los resultados estadísticos, tanto descriptivos como inferenciales, se confirma el logro del objetivo general. Siendo hipótesis alterna que sostiene que la implementación de una VPN tiene un impacto significativo en la seguridad de la información de los servicios de red de la IEPM CMFB – Arequipa.

En su tesis 'Implementación de una Red Privada Virtual en una red corporativa para mejorar la G.I. de los servicios en la empresa Técnica Plástica SRL' en 2018, Alvarado Sánchez abordó implementar una Red Privada Virtual en la red corporativa y su impacto en la gestión de la información. Su investigación reveló un índice inicial de insatisfacción del 60% en el pretest con la protección de datos e los usuarios con respecto al manejo de la información. Sin embargo, tras la implementación de la VPN en nuestro contexto, hemos alcanzado un notable aumento, elevando la aprobación de los usuarios al 90% en el post-test con respecto a la protección de datos del manejo de la información. Este contraste con nuestra investigación demuestra que la protección de datos en la VPN obtuvo una media de 56% en el pretest y un 80% en el Post-test, demostrando de esta manera que la implementación de una VPN mejora la protección de datos en el Consorcio.

Por otro lado, también se demostró que, con la implementación del VPN para mejorar la integridad de la información, se obtuvo una media de 65% siendo el mayor obtenido un 90% y el menor obtenido un 20%, demostrando de esta manera que la implementación de una VPN para mejorar la Integridad de la información mejora sustancialmente las redes del Consorcio.

También para Pablo Huanca en relación a su dimensión de Integridad los resultados respaldan la hipótesis alterna, que afirma que una VPN tiene un impacto notoria en la integridad de la seguridad de la información, donde según los resultados obtenidos, teniendo como media 43.3%, siendo el mayor 40% y en el menor obtenido un 16.7%, Esto quiere decir que la aceptación de integridad de la información varía entre los niveles medio y alto preferentemente subrayando la importancia de la integridad en la seguridad de la información.

Según los resultados presentados por Julio Morales en 2021, en su estudio sobre el indicador de disponibilidad a las carpetas compartidas, se destacó que antes de la aplicación de la VPN, el tiempo requerido era un de 45% más, mientras que con la VPN se incrementó a 23%. Esto representa una disminución significativa equivalente a una reducción del 56.7%. En ese sentido guarda relación con la presente investigación ya que para nuestra solución tecnología Implementación de una VPN para mejorar la disponibilidad de información, se vio mejorada en un 72% a un 97% teniendo una mejora obtenida del 15%, demostrando así que la VPN mejora la accesbilidad de la información para el Consorcio.

VI. CONCLUSIONES

1. Con los resultados que se mostraron en este informe se concluye que la implementación de la VPN mejora la seguridad de la información en el Consorcio Andia de un 26,5% de la variable a una mejora del 40% para la seguridad de la información.

2. Se puede concluir que, a través la Red Privada Virtual implementada, el indicador Autenticación mejoro de un pretest con 56% a un 80% en el post test, logrando cumplir con los requisitos de la empresa y demostrando que la implementación de una VPN basada en la metodología top-Down contribuye a mejorar la gestión de autenticación en el consorcio.

3. Se puede concluir que la implementación de una VPN, mejoro la protección de datos mejoro de un 56% a un 80% luego de la implementación del VPN logrando cumplir con los requisitos de la empresa y demostrando que Red Privada Virtual implementada basada en la metodología Top-Down contribuye a mejorar la protección de datos en el consorcio.

4. Se puede concluir también que a través de la implementación del VPN se mejoró la control de acceso desde un pretest con 50% a un post test con 79% y de esta manera asegurando el control de accesos para mejorar la S.I. en el Consorcio Andia

5. Se concluyo también que tras la implementación del VPN el indicador Autorización se vio mejorado desde el pretest con un 54% y en su posttest con un 65%, llegando a demostrar que la implementación de la VPN si mejora la Autorización.

6. También se concluye que para el indicador Accesibilidad, este se vio mejorado del pretest con un 72% en el pretest, y terminando con un 97% en el posttest y de esta manera asegurando que la Accesibilidad a través de la implementación VPN se ve mejorada significativamente.

VII. RECOMENDACIONES

1. Además de su implementación en el ámbito inmobiliario, se recomienda explorar la viabilidad de utilizar la solución VPN basada en el protocolo IPSEC y gestionada a través de la nube o SDN en otros sectores, como la industria financiera, educativa o de atención médica. Esta extensión hacia diferentes rubros permitiría adaptar y optimizar la seguridad de la red para proteger datos sensibles y garantizar la conectividad segura y confiable en diversas áreas de aplicación empresarial
2. Se sugiere investigar y evaluar diferentes opciones de software libre para implementar en el desarrollo de futuras VPN. Esta estrategia permitiría reducir los costos asociados y optimizar el rendimiento, lo que podría resultar en un uso más eficiente de los recursos financieros y una maximización de beneficios para la organización
3. Se recomienda llevar a cabo la migración a la nube con un enfoque constante en la seguridad por parte de la empresa. Es fundamental implementar medidas robustas para proteger los datos y sistemas en la nube, monitoreando de manera continua los posibles vectores de ataque y manteniendo un alto nivel de preparación ante desastres. Esto garantizará que la organización pueda aprovechar los beneficios de la nube mientras mantiene la integridad y la disponibilidad de sus recursos críticos,
4. Se recomienda profundizar en la evaluación de diversas tecnologías VPN además del protocolo IPSEC, tales como OpenVPN, SSL/TLS VPN, entre otras. Realizar un análisis comparativo detallado de sus características de seguridad, escalabilidad, facilidad de implementación y administración en entornos de nube o SDN
5. Para investigaciones futuras, se sugiere explorar la integración de tecnologías emergentes, como la inteligencia artificial y el blockchain, con las infraestructuras VPN. Esto podría incluir el estudio de cómo la IA puede mejorar las autorización y la adaptabilidad de la seguridad en las VPN, así como el uso de blockchain para fortalecer la autenticación y el registro de acceso en entornos de VPN gestionados en la nube o SDN.

REFERENCIAS

AHMAD, Zauwiyah., et al. Security monitoring and information security assurance behaviour among employees: An empirical analysis. *Information and Computer Security* **[En línea]**. Malaysia .Vol. 27 No. 2, pp. 165-188, 25 febrero 2019 **[Consulta: 13 junio 2023]** Disponible en: https://doi.org/10.1108/ICS-10-2017-0073 ISSN: 2056-4961

ASHISH Garg Ph.D.,JEFFREY Curtis & HILARY Halper, **The Financial Impact of IT Security Breaches: What Do Investors Think? 201 6[En línea] States [Consulta: 11 mayo 2023].**

Disponible en: https://doi.org/10.1201/1086/43325.12.1.20030301/41478.5

AL-FAYOUMI, Mustafa., AL-FAWA'REH, Mohammad., & NASHWAN, Shadi. (2022). VPN and Non-VPN Network Traffic Classification Using Time-Related Features. *Computers, Materials & Continua* **[En línea]**. Arabia Saudita, 72(2), 3091–3111, 29 Marzo 2022 **[Consulta: 10 junio 2023]**. Disponible en: https://doi.org/10.32604/cmc.2022.025103

ANDERSSON, Annika., HEDSTRÖM, Karin., & KARLSSON, Fredrik. Standardizing information security – *a structurational analysis. Information & Management* **[En línea]**. Suecia ,59(3), 10362, 3 abril 2022 **[Consulta: 10 mayo 2023]** Disponible en: https://doi.org/10.1016/j.im.2022.103623

BANOTH, Rajkummar., GUGULOTHU, Narsimha., & GODISHALA, Aruna. Kranthi. (2023). *A Comprehensive Guide to Information Security Management and Audit* (1st ed.) **[En línea]**. Florida Boca Raton, **[Consulta: 04 mayo 2023]**.

ISBN 9781003322191

Disponible en: https://www.routledge.com/A-Comprehensive-Guide-to-Information-

Security-Management-and-Audit/Banoth-Narsimha-Godishala/p/book/9781032344430

BANSODE, Rama., & GIRDHAR, Anup. (2021). Common Vulnerabilities Exposed in VPN - A Survey. *Journal of Physics. Conference Series*, **[En línea]**. India, 1714(1), 12045 ,24 – 25 octubre 2020 **[Consulta: 02 abril 2023]**.

Disponible en: https://doi.org/10.1088/1742-6596/1714/1/012045

BUENO, Carlos. y MEJÍA, José. (2021) Marco de trabajo usando VPN con software libre para mejorar la velocidad de internet en dispositivos móviles con Android. *Universidad Cesar Vallejo* **[En línea]**., Lima, Perú. 21 Octubre 2021**[Consulta: 02 mayo 2023]**.

Disponible en: https://hdl.handle.net/20.500.12692/83406

BABATIVA Carlos, *Investigación Cuantitativa,* Fondo editorial Areandino **[En línea]**. Colombia, 1(7)7-8, 12 noviembre 2017**[Consulta: 11 mayo 2023]**.

Disponible en: https://digitk.areandina.edu.co/handle/areandina/3544

CABRERA, O. CORDERO, R(2021) Diseño De Una Red Para La Empresa Arabito Con Solución En La Nube En Su Sede Principal Interconectando Sus Sucursales Mediante Vpn Mpls. Universidad Católica Andrés Bello, Venezuela [En línea]., Caracas, Venezuela. D Space. [Consulta: 16 mayo 2023].

Disponible en: https://repository.ucc.edu.co/items/3b4e3d8b-0366-437d-8ead-94998b553bc7

CARLOS Ramos. (2021) *Diseño de investigación Experimental.Vol.* 10 (1) I Revista CienciAmérica **[En línea]**. Ecuador,10(1),5-6. Enero – Junio 2021 **[Consulta: 19 mayo 2023]**.

Disponible en: https://doi.org/10.33210/ca.v10i1.356

CAROL Hsu, JAE-NAM Lee, DETMAR W. Straub, (2022) Institutional Influences on Information Systems Security Innovations. Information Systems Research **[En línea]** Vol 23 (3-part-2):918-939. **[Consulta: 11 mayo 2023]**

Disponible en: https://doi.org/10.1287/isre.1110.0393

CISCO, 2023. What Is Information Security?. [En línea]. San José, CA, Estados Unidos, 29 Marzo 2022 [Consultado: 30 Mayo 2023].

Disponible en: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

CONDORI Ojeda, Porfirio (2020). Universo, población y muestra**.** Curso Taller. **[En línea]**. Perú, Sesión 4, mayo 2020 **[Consulta: 19 abril 2023]**

Disponible en: https://www.aacademica.org/cporfirio/18

CONEJERO Suárez, Manuel., et al. *Diseño y validación de un instrumento de observación para valorar la toma de decisiones en la acción de recepción en voleibol*. Cultura, Ciencia y Deporte, 12(34),67-75. **[En línea] España, octubre 2016 [Consulta: 24 mayo 2023]**

ISSN:1696-5043
Disponible en: https://www.redalyc.org/articulo.oa?id=163049997008

CID-FUENTES, R. et al(2020) Implementation of a Large-Scale Platform for

Cyber-Physical System Real-Time Monitoring. Global IoT and Eleven Paths & Telefónica Investigación y Desarrollo [En línea]., Madrid, España. 21 Octubre 2021[Consulta: 20 mayo 2023].

Disponible en: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8693711

CRUZ, M. et al (2017) Diseño E Implementación De Un Sistema De Gestión De Seguridad De La Información Para Proteger los activos de Información De La Clínica Medcam Perú. (Tesis de Ingeniería). Universidad San Martin de Porres, Lima, Perú.

ESTRADA Esponda, Royer. David., UNÁS-GÓMEZ, Jose. Luis., & FLÓREZ-RINCÓN, Oleskyenio. Enrique. *Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá*. Revista Logos Ciencia & Tecnología, 13(3), 98-110. **[En línea] Colombia, 01 diciembre 2021 [Consulta: 22 mayo 2023]**

Disponible en: https://doi.org/10.22335/rlct.v13i3.1446

FERNÁNDEZ Bedoya, VÍCTOR. Hugo. (2020). *Tipos de justificación en la investigación científica*. Espí ritu Emprendedor TES, 4(3), 65–76. **[En línea] Perú 17 julio 2020 [Consulta: 02 mayo 2023]**
Disponible en: https://doi.org/10.33970/eetes.v4.n3.2020.207.

HEART, Tsipi., O'REILLY, Philip., SAMMON, David., & O'DONOGHUE, John. (2009). *Bottomup or topdown*. Journal of Systems and Information Technology, 11(3), 244–268. **[En línea] Irlanda, Israel 14 agosto 2009 [Consulta: 17 mayo 2023]**
Disponible en: https://doi.org/10.1108/13287260910983623

ISSN: 1328-7265

HUANCA Pablo (2022) Implementación de una VPN para la seguridad de la información de los servicios de red de la IEPM CMFB – Arequipa Universidad Tecnologica del Perú [En línea]. Lima, Perú. 21 Octubre 2022[Consulta: 12 mayo 2023].

Disponible en: https://repositorio.utp.edu.pe/handle/20.500.12867/6751

IMPERVA, 2022. Information Security: The Ultimate Guide.[En línea]. San Mateo, EEUU, 29 Marzo 2022 [Consultado: 25 Mayo 2023].

Disponible en: https://www.imperva.com/learn/data-security/information-security-infosec/

INT. J. MORPHOL., *Técnicas de Muestreo sobre una Población a Estudio,* International Journal of Morphology 35(1):227-232, 2017. **[En línea] Chile, marzo 2017** Disponible **[Consulta: 27 mayo 2023]**

Disponible en: http://dx.doi.org/10.4067/S0717-95022017000100037

JEONG, Christina. LEE, Sang. -YONG. Tom., & LIM, Jee.-Hae. *Information security breaches and IT security investments: Impacts on competitors*. Information & Management, 56(5), 681–695. **[En línea] USA, Corea , 10 noviembre 2018 [Consulta: 29 mayo 2023]**
Disponible en: https://doi.org/10.1016/j.im.2018.11.003

JIANYUN, Chen.; CHUNYAN, Li. *Research On Meteorological Information Network Security System Based On Vpn Technology*. En: 2nd International Conference On Electronic Information Technology And Computer Engineering (Eitce), 2018. **[En línea] China, 19 noviembre 2018 [Consulta: 29 junio 2023]**

Disponible en: https://Doi.Org/10.1051/Matecconf/201823201001

JOTA, Y. y RAMIREZ, D.(2018) Diseño de una red privada virtual (vpn) con seguridad l2pt para la empresa Laoratoros Expofarma S.A.(Tesis de ingeniería). Universidad Cooperativa De Colombia, Bogotá, Colombia.

KARAYMEH, Ashraf.; ABABNEH, Mohammad.; QASAIMEH, Malik.; AL-FAYOUMI, Mustafa. *Enhancing Data Protection Provided By Vpn Connections Over Open Wifi Networks.* En: 2nd International Conference On New Trends In Computing Sciences (Ictcs). Amman: Ieee, 2019, P. 1-6. **[En línea] Jordania 9 – 11 octubre 2019**

[Consulta: 19 junio 2023]

Disponible en: https://Doi.Org/10.1109/Ictcs.2019.8923104

Karaymeh, R. Secure Protocols And Virtual Private Networks: An Evaluation. Issues In Information Systems, 2019, 20(3): P. 37-46. Https://Doi.Org/10.48009/3_Iis_2019_37-46

KOSSINGOU, Ghislain. MERVYL. Saint; DÉGBOÉ, Bessan. Melckior.; OUYA, Samuel.; MENDY, Gervias. *Mutualisation Of Ict Laboratory Resources Between West And Central African Universities In Post-Crisis Situations: The Case Of Senegal And The Central African Republic*. En: Sixth International Conference On E-Learning (Econf). Sakheer: Ieee, 2020, P. 1-5. **[En línea] Senegal y Republica Africana , 06 - 07 diciembre 2020 [Consulta: 05 Abril 2023]**

Disponible en: https://Doi.Org/10.1109/Econf51404.2020.9385470

KURODA, Toshikazu. *A Combination Of Raspberry Pi And Softether Vpn For Controlling Research Devices Via The Internet*. Jrnl Exper Analysis Behavior, 2017, 108, P. 468-484. **[En línea] [Consulta: 03 mayo 2023]**

Disponible en: https://Doi.Org/10.1002/Jeab.289

LACKOVIĆ, D.; TOMIĆ, M. Performance Analysis Of Virtualized Vpn Endpoints. En: 40th International Convention On Information And Communication Technology, Electronics And Microelectronics (Mipro). Opatija: Ieee, 2017, P. 466-471. **[En línea] [Consulta: 16 junio 2023]**

Disponible en: https://Doi.Org/10.23919/Mipro.2017.7973470

LAZARTe, D. y SILVA,G. 2022 *Diseño de una red privada virtual (VPN) basada en software libre para la mejora de la seguridad de la información de la jurisdicción de la dirección de redes integradas de salud Lima Centro* **[en línea]** (Tesis de Ingeniería). Universidad Cesar Vallejo, Lima, Perú. **[consulta:** 16 de junio 2023**].**

Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/92270

LAWRENCE Gordon & LOEB Martin, **Budgeting process for information security expenditures** , **Communications of the ACM, Volume 49Issue, [En línea] 2006, pp 121–125 [Consulta: 11 mayo 2023]**

Disponible en: https://dl.acm.org/doi/10.1145/1107458.1107465

LUNA, A. y ZETA, C. (2021) Implementación de redes VPN MIKROTIK para los servidores entre ciudades de Lima y Pisco.**[en línea]** (Tesis de Ingenieria) Universidad Cesar Vallejo, Lima, Perú. **[consulta:** 21 de junio 2023**].**

Disponible: https://repositorio.ucv.edu.pe/handle/20.500.12692/82658?show=full

MENDIETA, J. y VALENCIA, J y CAMACHO, H. (2020). Diseño y prototipado de Red P2P Definida por Software para Pymes y Trabajo Remoto (Proyecto de Ingenieria) Universidad Del Norte, Barranquilla, Colombia. **[En línea] [Consulta: 23 mayo 2023]**

Disponible en: https://manglar.uninorte.edu.co/handle/10584/9312#page=1

MICHAIL, H. E., KAKAROUNTAS, A. P., MILIDONIS, A. S., & GOUTIS, C. E. (2009). A Top-Down Design Methodology for Ultrahigh-Performance Hashing Cores. IEEE Transactions on Dependable and Secure Computing, 6(4), 255–268]. **[En línea] [Consulta: 18 mayo 2023]**

Disponible en: https://doi.org/10.1109/TDSC.2008.15

MORA. J.(2021) *Propuesta metodológica para la gestión de la seguridad de la información alineada a la norma ISO 27001 y ciberseguridad (*Tesis de ingeniería) Pontificia universidad católica del ecuador, Quito, Ecuador.].. **[En línea] [Consulta: 12 junio 2023].**

Diponible en: https://core.ac.uk/download/pdf/235988174.pdf

MORALES, J. et al.(2021) Implementación de una Red Privada Virtual basada en la metodología PPDIOO para mejorar la seguridad informática en la red de Lima Traylers S.A.C. Universidad Cesar Vallejo [En línea]., Trujillo, Perú. 21 Octubre 2021[Consulta: 22 mayo 2023].

Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/74675

NADKARNI, S. (2020). *Fundamentals of Information Security: A Complete Go-to Guide for Beginners to Understand All the Aspects of Information Security*.. Karnataka, India, New Delhi, India: BPB Publications. **[Consulta: 12 junio 2023].**

ISBN 9789389328400

Disponible en: https://www.amazon.com/Fundamentals-Information-Security-Go-Understand/dp/9389328403

NG, Ka. Chung., ZHANG, Xiaojun., THONG, James., & TAM, Kar. Yan. *Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective*. Journal of Management Information Systems, 38(3), 732–764. **[En línea] Hong Kong, 07 diciembre 2021 [Consulta: 12 mayo 2023]**

Disponible en: https://doi.org/10.1080/07421222.2021.1962601

PÁRRAGA, René(2018).D*iseño de protocolo de seguridad postevento informático basado en la norma iso/iec-17799 para la facultad de ingeníeria industrial*,(Tesis de Ingenieria) Universidad de Guayaquil, Guayaquil, Ecuador. **[En línea] [Consulta: 12 junio 2023].**

Diponible en: http://repositorio.ug.edu.ec/handle/redug/36275

PERDIGON Llanes, Rudibel y RAMIREZ Alonso, Rosangel. Plataformas de software libre para la virtualización de servidores en pequeñas y medianas empresas cubanas. *Rev cuba cienc informat* [online]. 2020, vol.14, n.1 [citado 2023-07-05], pp.40-57.

ISSN 2227-1899.

Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992020000100040&lng=es&nrm=iso

PERALTA, Alvaro. Raúl.; BILOUS, Allá.; FLORES, Carlos. Roberto.; BOMBÓN, Carlos. Fernando. El Impacto Del Teletrabajo Y La Administración De Empresas. *Recimundo, 2020,* **[En línea]** 4(1): P. 326-335. Ecuador, 16 febrero 2020 **[Consulta: 11 junio 2023]** Disponible en: https://Doi.Org/10.26820/Recimundo/4.(1).Enero.2020.326-335

PERDIGÓN, Pérez, Maria. Teresa. Análisis Holístico Del Impacto Social De Los Negocios Electrónicos En América Latina, Paakat: *Revista De Tecnología Y Sociedad* 2020, **[En línea]** 10(18). México 2014 – 2019 **[Consulta: 11 mayo 2023]**

Disponible en: http://dx.doi.org/10.32870/Pk.a10n18.459

PINZÓN, Sonia. Alexandra.; MARTÍNEZ, Angelica. Maria.; ÁVILA, Edwin. Alejandro. State Of Art On Telematic Infrastructure For Telework. *Visión Electrónica*, **[En línea]** 2017, 11(2): P. 261-278. Colombia, 29 diciembre 2017 **[Consulta: 07 mayo 2023]**

Disponible en: https://Doi.Org/10.14483/22484728.12114

MARTEL, Víctor. Diseño de una red de comunicación VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764. (Tesis de Ingeniería) *Universidad Peruana De Ciencias Aplicadas* **[En línea]** Lima, Perú , 3 abril 2019

[Consulta: 16 mayo 2023]

Disponible en: https://Doi.Org/10.19083/tesis/625693

RIVAS, W. y RODRIGUEZ, J. (2015) Esquemas de seguridad basados en vpn para una red corporativa enfocada al control de acceso utilizando los servicios de

seguridad AAA. (Tesis de ingenieria) Universidad Don Bosco, El Salvador El Salvador, Centroamérica.

Disponible en: http://hdl.handle.net/11715/1650

SANCHEZ, S.(2022) Diseño de plataforma de seguridad en centro de datos La Colina, caso Corporación Digitel. Universidad Centra de Venezuela [En línea]. Caracas, Venezuela. 21 Octubre 2028[Consulta: 30 mayo 2023].

Disponible en: http://hdl.handle.net/10872/18009

SANJAY Goel, HANY A. Shawky. Estimating the market impact of security breach announcements on firm values, *Scopus* , **[En línea]** University at Albany, United States **[Consulta: 11 mayo 2023].**

Disponible en: https://doi.org/10.1016/j.im.2009.06.005

SHAOFENG, L.; CHAOPING, G.; WEIFENG, S. Design And Implementation Of An Enhanced Vpn Isolation Gateway. En: 2017 International Conference On Robots & Intelligent System (Icris). Huai An City: Ieee, 2017, P. 82-85. **[Consulta: 02 junio 2023].**

DOI: 10.1109/ICRIS.2017.27

Disponible en: https://Doi.Org/10.1109/Icris.2017.27

SKENDZIC, S.; KOVACIC, B. Open Source System Openvpn In A Function Of Virtual Private Network. *Iop Conf. Ser.: Mater. Sci. Eng.* **[En línea] Romania** 2017, 200, 012065.11 noviembre 2016 **[Consulta: 14 mayo 2023]** Disponible en: https://Doi.Org/10.1088/1757-899x/200/1/012065

TOLLEY, J. Beau, KUJATH.(2021) Blind In/On-Path Attacks and Applications to VPNs.30 Usenix Security Syposum [En línea]., Arizona State University.[Consulta: 23 mayo 2023].

Disponible en: https://www.usenix.org/system/files/sec21fall-tolley.pdf

VALVERDE, Diego. Implementación de una gestión de riesgos de TI para mejorar la seguridad de la información de una empresa de agencia publicitaria (Tesis de ingeniería*). Universidad Tecnológica del Perú*, **[En línea]** Lima, Perú. Febrero 2019 **[Consulta: 18 abril 2023] Disponible en: https://repositorio.utp.edu.pe/handle/20.500.12867/5529**

VERDEJO, et al. Defensas frente a ataques DoS a baja tasa contra servidores basadas en políticas de gestión de colas. Rev VIII Jornadas de Ingeniería Telemática [online]. 2019, vol.16, n.1 **[Consulta: 19 de Mayo 2023]**

Disponible en: http://scielo.sld.cu/scielo.php?pid=S2227-18992022000100092&script=sci_arttext&tlng=pt

World Economic Forum (2021) The Global Risks 2021. World Economic Forum,1(16),11-14. **[Consulta: 22 junio 2023].**

Disponible en: https://www.weforum.org/reports/the-global-risks-report-2021/

YULY, J. et al.(2018) Diseño De Una Red Privada Virtual (Vpn) Con Seguridad L2pt Para La Empresa Laboratorios Expofarma S.A.. Universidad Cooperativa de Colombia [En línea]., Bogota, Colombia. Octubre 2018 [Consulta: 16 mayo 2023].

Disponible en: https://repository.ucc.edu.co/items/3b4e3d8b-0366-437d-8ead-94998b553bc7

ZAIN Ul Abideen, MUHAMMAD., Saleem, Shahzad., & EJAZ, Madiha. VPN Traffic Detection in SSL-Protected Channel. *Security and Communication Networks*, **[En línea] Pakistan** 2019, 1–17. 29 Octubre 2019 **[Consulta: 18 mayo 2023]** Disponible en: https://doi.org/10.1155/2019/7924690

ZHOU, Zhengchun., & HUANG, Tongcheng . Open VPN Application in COVID-19 Pandemic. *Journal of Physics. Conference Series*, **[En línea] Canada** 1865(4), 42015–.23 enero 2021**[Consulta: 02 mayo 2023]** Disponible en: https://doi.org/10.1088/1742-6596/1865/4/042015

ZHOU, Zhengchun., & HUANG, Tongcheng . Open VPN Application Under Campus Network. *Journal of Physics. Conference Series*, **[En línea]**. Canada 1865(4), 42014–. 23 enero 2021 **[Consulta: 01 mayo 2023]** Disponible en: https://doi.org/10.1088/1742-6596/1865/4/042014

ANEXOS

Anexo 1 Tabla operacionalización

Variable (Dependiente)	Definición Conceptual	Definición Operacional	Dimensión	Indicador	ÍTEMS	Escala de Medición
Seguridad de la información	"Una variedad de ataques a los activos informáticos pueden resultar en una pérdida de disponibilidad y confidencialidad de la información; estos son efectos peligrosos para las organizaciones y muchas personas y la oportunidad de causar un daño irreparable" (Diego, valverde, 2022.p27).	Esta variable se medirá por medio de una encuesta.	Confidencialidad	Autenticación	1. 2.	Escala Ordinal
				Protección de datos	3. 4	
			Integridad	Acceso	5. 6.	
				Autorización	7. 8.	
			Disponibilidad	Accesibilidad	9. 10. 11.	

Anexo 2 Instrumento de recolección de datos

Este cuestionario tiene como objetivo comprobar el nivel de la seguridad de información

Marca con una (X)

1. ¿Ha establecido la organización un proceso de autenticación y autorización (es decir, prueba de identidad, registro, gestión de roles) para limitar el acceso a los Servicios críticos solo a las personas autorizadas?

( ) Muy Alto
( ) Alto
( ) Medio
( ) Bajo
( ) Muy Bajo

2. ¿La organización practica el concepto de privilegios mínimos (es decir, los usuarios solo tienen acceso a la información, los archivos y las aplicaciones necesarios para cumplir con sus roles y responsabilidades) dentro de los Servicios críticos para todas las cuentas?

( ) Muy Alto
( ) Alto
( ) Medio
( ) Bajo
( ) Muy Bajo

3. ¿La organización identifica y categoría la informacion sensible para proteger los datos confidenciales utilizados en los Servicios Críticos?

( ) Muy Alto
( ) Alto
( ) Medio
( ) Bajo
( ) Muy Bajo

4. ¿La organización implementa una revisión de seguridad para el tránsito de informacion y que esta se publique fuera de las operaciones?

( ) Muy Alto
( ) Alto
( ) Medio
( ) Bajo
( ) Muy Bajo

5.¿La organización implementa controles de seguridad sólidos para limitar el acceso físico y lógico a los Servicios Críticos?

( ) Muy Alto
( ) Alto
( ) Medio
( ) Bajo
( ) Muy Bajo

6. ¿La organización emplea medidas para garantizar la integridad de los sistemas y asi prevenir y evitar la explotación de rutas de acceso en los Servicios Críticos?

( ) Muy Alto
( ) Alto
( ) Medio
( ) Bajo
( ) Muy Bajo

7. ¿La organización permite el acceso remoto a los activos de Servicios Críticos?

( ) Muy Alto
( ) Alto
( ) Medio
( ) Bajo
( ) Muy Bajo

8.¿La organización emplea estrategias o defensas en capas específicas adicionales para compensar la pérdida de controles primarios?

( ) Muy Alto
( ) Alto
( ) Medio
( ) Bajo
( ) Muy Bajo

9 ¿La organización tiene un plan de respaldo y recuperación de datos para garantizar la continuidad?

( ) Muy Alto
( ) Alto
( ) Medio
( ) Bajo
( ) Muy Bajo

10. ¿Con que medida la organización realiza pruebas periódicas de los procedimientos de respaldo y recuperación?

( ) Muy Alto
( ) Alto
( ) Medio

( ) Bajo
( ) Muy Bajo

11. ¿ Tiene la organización capacidades de almacenamiento alternativas o de respaldo que puedan usarse en caso de pérdida del almacenamiento principal?

( ) Muy Alto
( ) Alto
( ) Medio
( ) Bajo
( ) Muy Bajo

Leyenda:

Muy Bajo	1
Bajo	2
Medio	3
Alto	4
Muy Alta	5

Anexo 3: Matriz de Consistencia

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	MÉTODO
P.G.1: ¿Cómo el implementación de una VPN basada en la metodología top-Down mejora la seguridad de la información en un consorcio?	O.G.1: Determinar el efecto de la implementación de una VPN basada en la metodología top-Down en la mejora de la seguridad de la información en un consorcio.	H.G.1: La implementación de una VPN basada en la metodología top-Down mejora la seguridad de la información en un consorcio.	**Variable Dependiente:** Seguridad de la información	D.1.: Confidencialidad	I.1.: Autenticación	**Tipo de investigación** Aplicada **Enfoque de investigación** Cuantitativo **Diseño de Investigación** Experimental – Pre experimental **Técnica e instrumento de Recolección de datos:** Encuesta Cuestionario
P.E.1: Cómo la VPN basada en la metodología top-Down mejora la gestión de autenticación en el consorcio?	O.E.1: Determinar el efecto de la implementación de una VPN basada en la metodología top-Down en la gestión de autenticación en el consorcio.	H.E.1: La implementación de una VPN basada en la metodología top-Down contribuye a mejorar la gestión de autenticación en el consorcio.				
P.E.2: ¿Cómo la VPN basada en la metodología top-Down mejora	O.E.2: Determinar el efecto de la implementación de una VPN basada en la	H.E.2: La implementación de una VPN basada en la metodología top-Down contribuye a mejorar la			I.2.: Protección de datos	

protección de datos en el consorcio?	metodología top-Down en la protección de datos en el consorcio	protección de datos en el consorcio.				**Población:** 10 colaboradores **Muestra:** 10 colaboradores **Análisis de datos:** Análisis Aplicativo
P.E.3: ¿Cómo la VPN basada en la metodología top-Down mejora la gestión de acceso en el consorcio?	O.E.3: Determinar el efecto de la implementación de una VPN basada en la metodología top-Down en la gestión de acceso en el consorcio.	H.E.3: La implementación de una VPN basada en la metodología top-Down contribuye a mejorar la gestión de acceso en el consorcio.		D.2.: Integridad	I.3.: Acceso	
P.E.4: ¿Cómo la VPN basada en la metodología top-Down mejora la Autorizacion en el consorcio?	O.E.4: Determinar el efecto de la implementación de una VPN basada en la metodología top-Down en la Autorización el en el consorcio.	H.E.4: La implementación de una VPN basada en la metodología top-Down contribuye a mejorar la Autorización el consorcio.			I.4.: Autorización	
P.E.5: ¿Cómo la VPN basada en la metodología top-Down mejora la Accesibilidad en el consorcio?	O.E.5: Determinar el efecto de la implementación de una VPN basada en la metodología top-Down en la Accesibilidad en el consorcio.	H.E.5: La implementación de una VPN basada en la metodología top-Down ayuda a mejorar la Accesibilidad en el consorcio		D.3.: Disponibilidad	I.5 Accesibilidad	

Anexo 4 Autorización de a la empresa para realizar la investigación

CONSORCIO ANDIA E HIJOS S.A.C.
R.U.C. 20523956826

CARTA DE ACEPTACIÓN

Lima, 19 de junio 2023

Estimada Universidad Cesar Vallejo,

Tengo el agrado de dirigirme a usted con el propósito de informarle que el Sr. Billy Scott Valero Andia con DNI N° 74732818, estudiante de la carrera de Ingeniería de Sistemas de la Universidad Cesar Vallejo, ha sido aceptado por el Consorcio Andia e Hijos S.A.C. para realizar su Proyecto de Investigación titulado "Implementación de un VPN bajo la metodología Top-Down para mejorar la seguridad de la información en el Consorcio Andia". Este proyecto se llevará a cabo desde el 3 de abril de 2023 hasta el 20 de diciembre de 2023.

En el marco de esta colaboración, el consorcio se compromete a proporcionar la información necesaria, de acuerdo con los aspectos éticos mencionados en la investigación. Asimismo, se garantiza que la información será tratada de manera transparente y que el estudiante se compromete a no divulgarla ni utilizarla más allá de los fines acordados con la empresa. Es importante destacar que la información proporcionada está destinada únicamente con fines académicos.

Sin otro particular, se expide este documento de acuerdo a los requisitos solicitados por el interesado para los fines que requiera.

Atentamente.

CONSORCIO ANDIA E HIJOS S.A.C.
RUC: 20523956826

Av. Naranjal N° 1195 2do Piso - Los Olivos
Telf.: 521-5751

Anexo 6 Desarrollo

Para llevar a cabo la investigación actual, se utilizará la metodología conocida como Top-Down Network Design, la cual ha demostrado su eficacia en diversos campos de la Ingeniería. La metodología top-down es importante en la industria porque permite a los diseñadores comprender el sistema en su conjunto antes de comenzar a diseñar los detalles. Esto ayuda a garantizar que el sistema sea coherente y funcione correctamente.

Es crucial resaltar que la metodología Top-Down Network Design aporta valiosos beneficios a las organizaciones que la adoptan. Estos beneficios engloban la mejora de la comunicación entre diseñadores, tanto actuales como futuros; un mayor control de calidad al permitir la identificación temprana de defectos en las etapas iniciales del diseño, cuando su corrección resulta más sencilla y económica; el incremento de la eficiencia de los diseñadores mediante la reorganización de las tareas de diseño y la ejecución en paralelo, en lugar de depender de secuencias lineales; así como la reducción de la necesidad de una verificación exhaustiva del estado final del diseño

4.1 Fases de la Metodología Top-Down Network Design

La metodología cuenta con 4 fases que ayudan a la creación e implementación del
Fase 1: Analizar requerimientos

Fase 2: Desarrollar diseño Lógico

Fase 3: Desarrollar diseño Físico

Fase 4: Probar, optimizar y documentar diseño

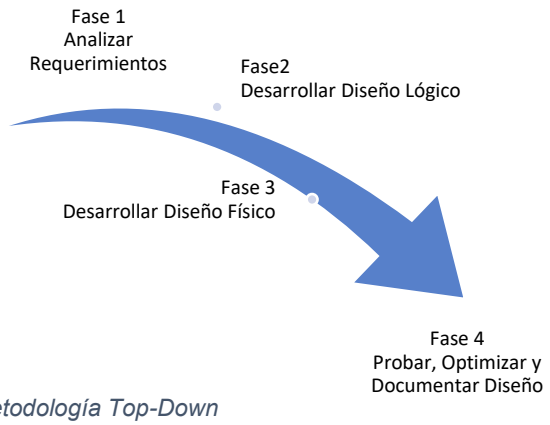
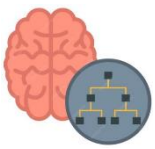


Figura 16 Fases Metodología Top-Down

4.2 Fases y actividades de la metodología Top-down Network Design

Fases	***Procesos***	***Actividades***
Fase 1 Analizar Requerimientos 	*Analizar los Objetivos y limitaciones de la empresa*	*- Definición de Metas* *-Puntualizar Objetivos* *-Situación Actual de la empresa*
	Analizar los objetivos y limitaciones técnicas	
	Caracterizar la red existente	
	Caracterizar el tráfico de la red	
Fase 2 Diseño Lógico de la red 	*Diseñar una topología de red*	*-Diseñar una Topología de red* *-Diseñar modelos de direccionamiento* *-Seleccionar protocolos de conmutación y enrutamiento* *-Diseñar estrategias de seguridad de la red* *-Diseñar estrategias de gestión de la red*
	Diseñar modelos de direccionamiento y nombres	
	Seleccionar protocolos de Conmutación y Erutación	

	Desarrollar estrategias de seguridad	
	Desarrollar estrategias para el manteamiento de la red	
FASE 3 DISEÑO FISICO DE LA RED 	*Seleccionar tecnologías y dispositivos para las redes*	*-Detalles técnicos del hardware.* *-Detalles técnicos de conexión* *-Configuración equipo y su Nube Ruijie*
FASE 4 PROBAR, OPTIMIOZAR Y DOCUMENTAR 	*Probar el diseño de red*	*-Configurar las políticas de la VPN* *-Probar el diseño entre las sedes* *-Configurar las carpetas compartidas en la red VPN*
	Optimizar el diseño de red	
	Documentar el diseño de red	

Fase 01 Analizar Requerimientos

a) Actividad 1: Definición de Metas

Atraves de las conversaciones y reuniones con los lideres de cada departamento dentro de la empresa, se ha conseguido identificar los factores que contribuyen a las metas obtenidas a continuación:

- El Consorcio Andia quiere expandir su presencia en el mercado inmobiliario, tanto en el ámbito nacional como internacional. Para ello, planea abrir nuevas oficinas en otros países y ampliar su cartera de productos y servicios. También vela por ofrecer a sus clientes una amplia gama de productos y servicios inmobiliarios, desde la compra y venta de propiedades hasta la gestión de alquileres y la construcción de viviendas. De la misma manera quiere ser reconocido como una empresa líder en el sector inmobiliario. Para

ello, se compromete a ofrecer un servicio de alta calidad y a estar a la vanguardia de las últimas tendencias del mercado.

- El consorcio Andia actualmente necesita herramientas tecnologías como las facturas electrónicas, acceso a intranet segura, compartir información para poder completar las actividades del negocio dentro de la empresa. Esta necesidad viene del avance de la tecnología, es inevitable no trabajar con la tecnología actual y en el caso del consorcio teniendo 3 oficinas aisladas es necesario una red que integre a las sucursales, por tal motivo se desea implementar una red segura cumpliendo la regla de la triada CIA (Confidencialidad, Integridad y Disponibilidad)

b) Actividad 2: Puntualización de objetivos

Después de establecer los problemas esenciales que aquejan al Consorcio Andia, se inicia establecer el enfoque que se pretende con la ejecución del proyecto:

- Mejorar la seguridad de la información: el consorcio quiere proteger sus datos de la pérdida, la divulgación o el acceso no autorizado. Para ello, implementará un sistema de control de acceso basado en roles, un sistema de auditoría y una infraestructura de red segura y eficiente.
- Mejorar la eficiencia de las operaciones: el consorcio quiere agilizar sus procesos y procedimientos para reducir costes y mejorar la productividad. Para ello, centralizará sus datos en un único repositorio, estandarizará sus procesos y procedimientos y automatizará las tareas repetitivas.
- Mejorar la experiencia del cliente: el consorcio quiere ofrecer un servicio de alta calidad y personalizado a sus clientes. Para ello, implementará un sistema definido para redes o nube centralizada, donde monitoreara a los clientes teniendo una solución especfica para cada cliente.

c) Actividad 3: Situación Actual de la empresa

El Consorcio Andia es una empresa inmobiliaria que cuenta con varias sucursales en Lima. La empresa utiliza una red cableada interna para conectar sus oficinas y un servicio de internet para acceder a recursos externos

- Situación actual de la red del Consorcio Andia está compuesta por los siguientes elementos: Routers, switch, tarjetas inalámbricas PCI, Routers inalámbricos, computadoras y laptops. Una red interna que se encarga de todo el trafico del Consorcio en cada sede independientemente, también se cuenta con Servicio de internet que por donde acceden a los recursos externos y se comunican entre sucursales.
- Los problemas actuales del Consorcio son la falta de confidencialidad al no tener políticas seguras, los datos viajando de manera libre sin ningún tipo de seguridad, también no se encuentra protegida ante alteraciones ya que no cuenta con un sistema de auditoria o registros log, y la disponibilidad por si llega a fallar la red y no se cuenta con un backup.

Fase 02 Propuesta de diseño lógico de la red

En esta parte se establece la topología de red que será empelada por el Consorcio

a) Actividad 1 Diseñar una topología de red

- Para el diseño de la VPN la topología usar será estrella, debido a que todas los dispositivos se interconectan entre si como una red local.

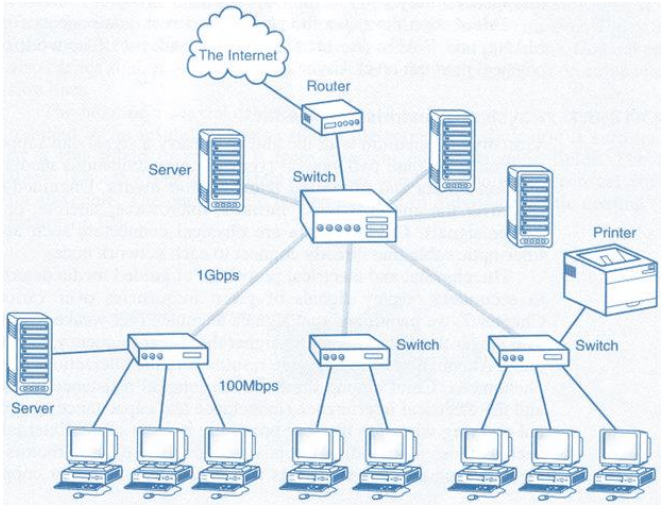


Figura 16 Topologia estrella

b) Actividad 2 Diseñar modelos de direccionamiento y denominación

El modelo de direccionamiento se establece a través del Router Ruijie Network R105G.

- El direccionamiento será un enrutamiento estatico establecido a manualmente en las configuraciones de la nube para adminsitrar el Router Ruijie.

c) Actividad 3 Seleccionar protocolos de conmutación y enrutamiento.

Posteriormente , se procede a seleccionar los protocolos de conmutación y enrutamiento apoyados por el Router Ruijie.

- Los protocolos y enrutamientos serán decididos por el Router Ruijie Network, tenia como enrutamiento una ruta estática entre sucursales.

d) Actividad 4 Desarrollar estrategias de seguridad de la red.

Luego, se procede a diseñar estrategias de seguridad apoyados por el Router Ruijie.

- La seguridad e la red VPN es propia de Ruijie, teniendo algunas características como Análisis de trafico, Control de acceso , Cifrado, Protección de aplicaciones, control de flujo.

e) Actividad 5 Desarrollar estrategias de gestión de la red.

También se procede con el desarrollo de las estrategas de gestión de red apoyadas por el Router Ruijie

- En el panel Ruijie Cloud se puede administrar todas las opciones disponibles para la configuración de Routers, así como la VPN, algunos ejemplo incluyen gestión de policitas, gestión de dispositivos, gestión de usuarios, gestión de aplicaciones, gestión de seguridad.

Fase 03: Propuesta diseño físico de la red.

a) Actividad 1 Detalles técnicos del Hardware

- Seguidamente se detalles las características técnicas del Hardware a usar:

Característica	**Descripción**
Interfaz de red	5 puertos Base-T 10/100/1000

Certificaciones	CE, ROHS
RAM	DDRIII de 128 MB
Máx. puertos WAN	2 puertos Base-T 10/100/1000
Ancho de banda recomendado	600Mbps
Almacenamiento	Flash de 16 MB
Salida PoE	802.3af/at en LAN1-4
Usuarios concurrentes recomendados	100
Dimensión	206,5 mm × 108,5 mm × 28 mm
Temperatura de funcionamiento	0°C ~ 40°C
Alimentación	100～240 V CA, 50/60 Hz
Consumo de energía	< 60 W (con carga PoE)

- Se presenta la pantalla del hardware Ruijie a usar, en este dispositivo se configurar y administrara el VPN para mejorar la seguridad de información.

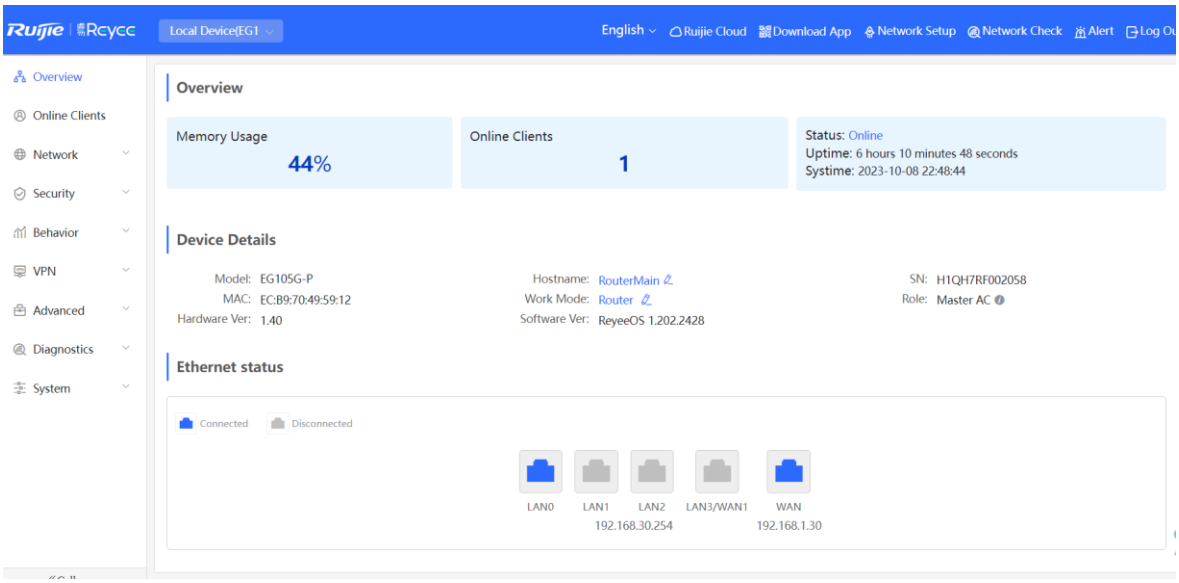


Figura 18 Software Definido para Redes

b) Entregable 2 Detalles técnicos de conexión.

Seguidamente se realizan los detalles técnicos de conexión:

- El consorcio cuenta con 100Mbps, el cual es proporcionadoa través de Fibra HFC, llegando a través de un equipo UBEE, para luego llegar hacia el Router Ruijie quien estará cargo la distribución del internet y la adminsitraciond e la red.

- A continuación se detalla la lista de equipos con los que cuenta la empresa actualmente

TIPO	MARCA	MODELO	CANTIDAD
Router	Ubee	Docsis 3.0	1
Router	Ruijie	RG105 P	3
Switch	TPLink	TL SG1016D	1
Access Point	Ruijie	RAP2260G	1
Computadoras	Intel	I3 8000	1
Computadora	Intel	Core duo	12

c) Configuracion del equipo y su Nube Ruijie

Luego se procede a realizar la configuración de Ruijie Cloud.

- Ingresar al siguiente link: https://cloud-la.ruijienetworks.com/
- Luego crear una cuenta y acceder al controlador Ruijie.

En la siguiente figura se muestra la pantalla inicial

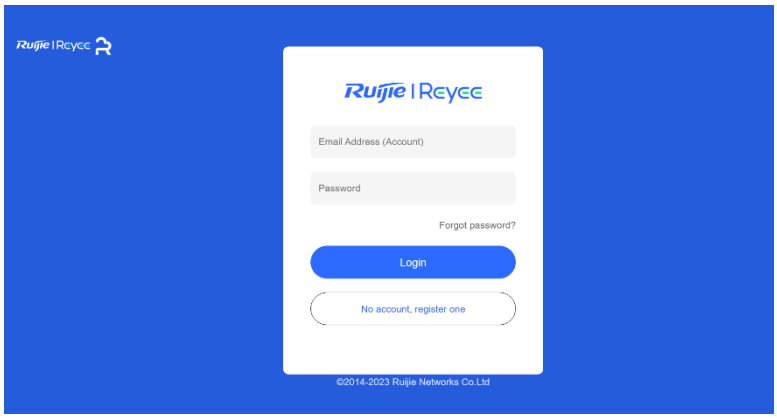


Figura 19 Login de Software Definido para redes

Luego se de ingresar, en la pantalla principal debemos crear los 3 proyectos que representaran a las surcursales del consorcio, a continuación se muestra la secuencia de pasos y pantallas hasta terminar la creación del proyecto.

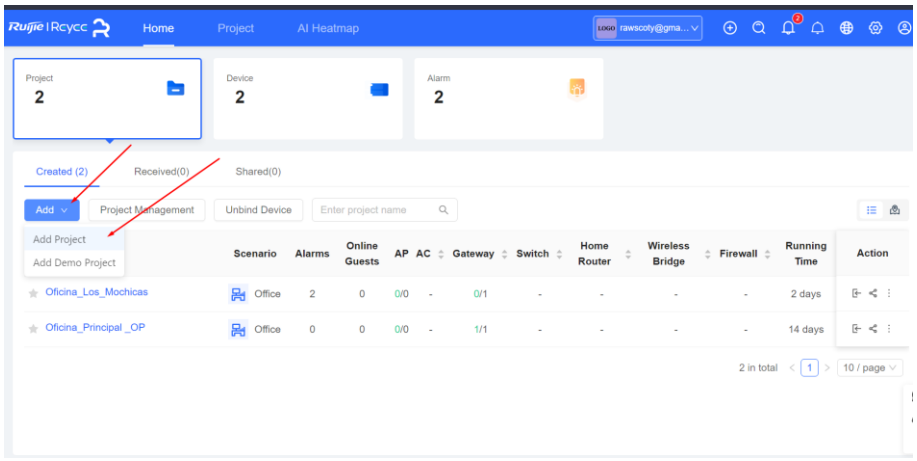


Figura 20 Creación del proyecto

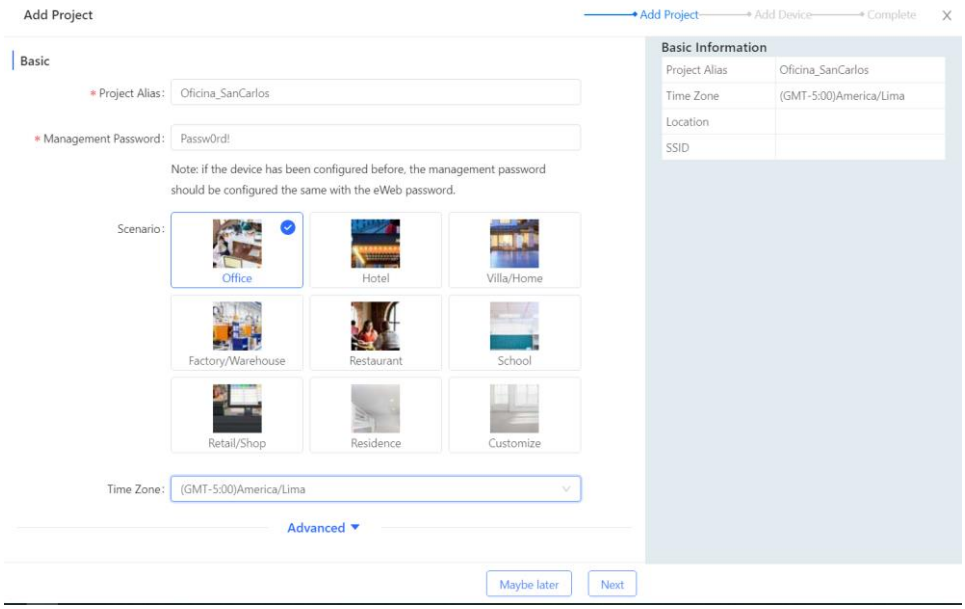


Figura 21 Configuración del proyecto

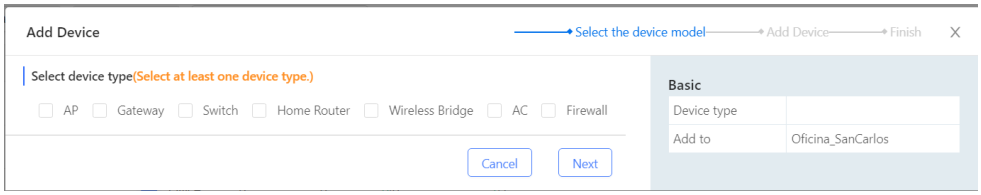


Figura 22 Escogiendo el tipo de dispositivo añadir

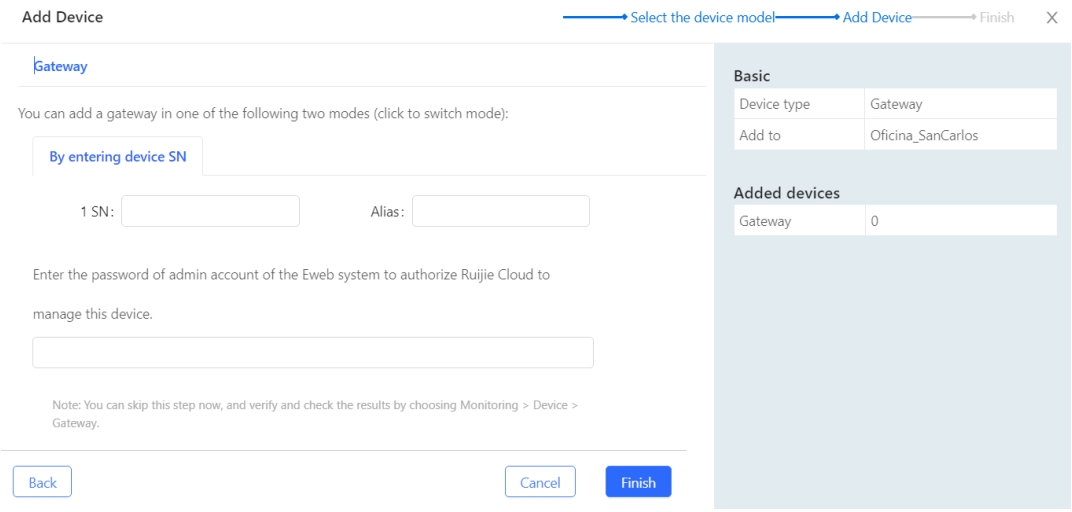


Figura 23 Activación de nuestro dispositivo

Una vez tengamos los 3 proyectos preparados y listo para configurar, procederemos a configurar las ip y rutas estáticas, asi como las vlan y la VPN para mejorar la seguridad de información.

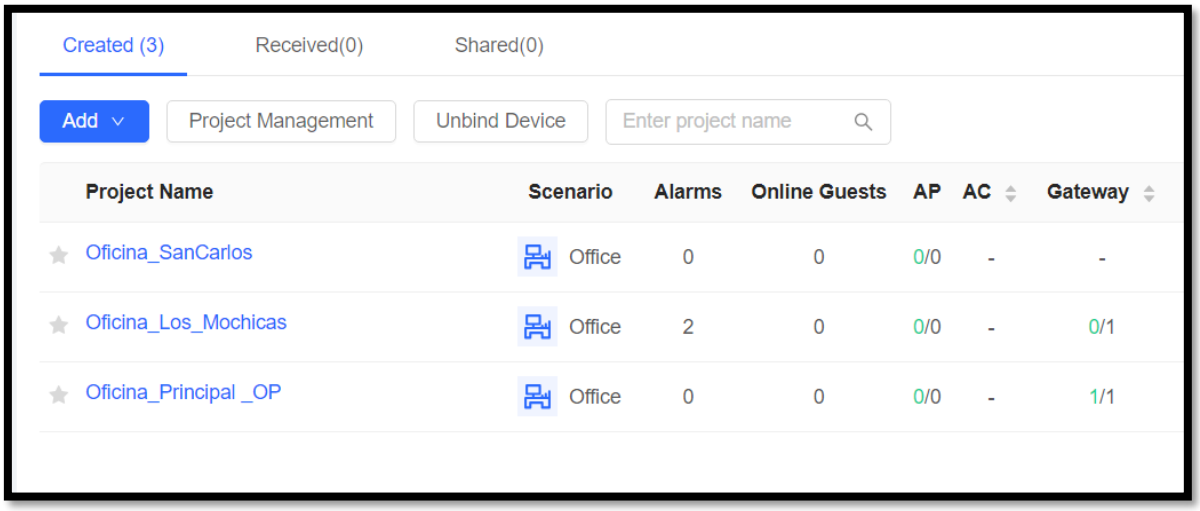


Figura 24 Los 3 proyectos creados para nuestra oficinas

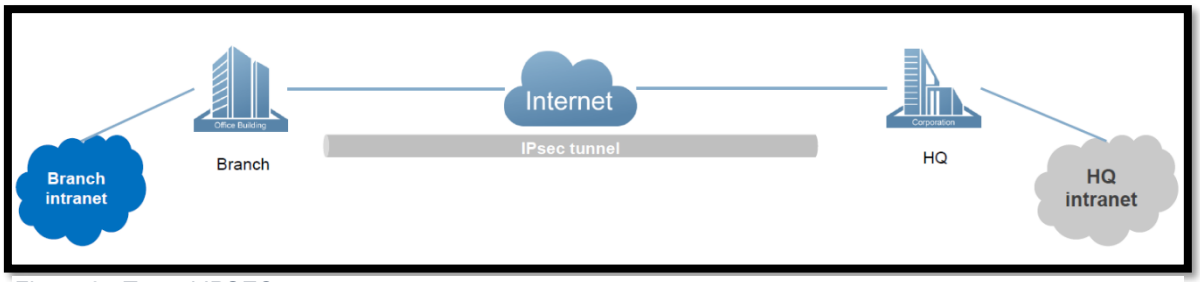


Figura 25 Tunnel IPSEC

Previamente a la gestión de Cloud Ruijie, se debe configurar desde el mismo router las interfaces WAN y LAN para la correcta administración.

Configuracion WAN *Configuracion LAN*

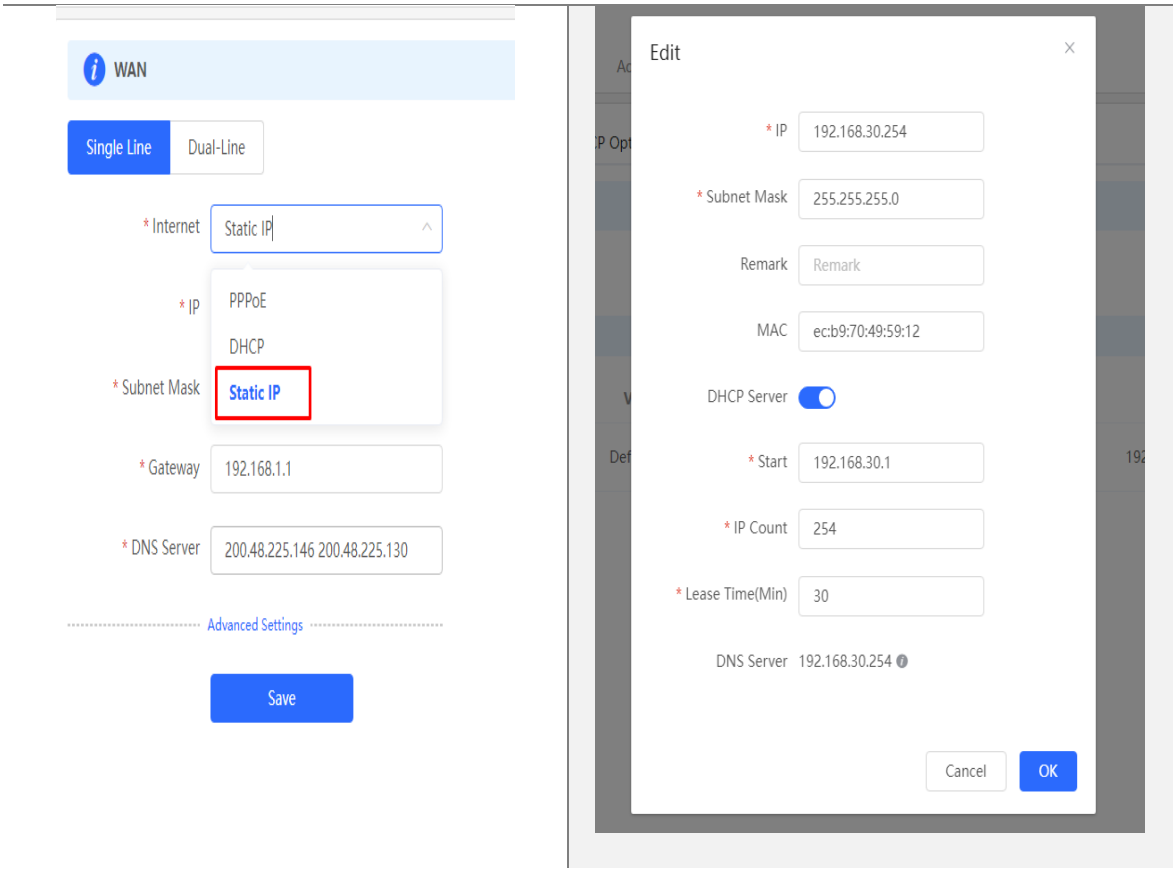


Figura 26 Configuraciones del Router

Una vez configurado y preparado el Router para recibir la VPN, se procede a crear la política de VPN a través de Cloud Ruijie.

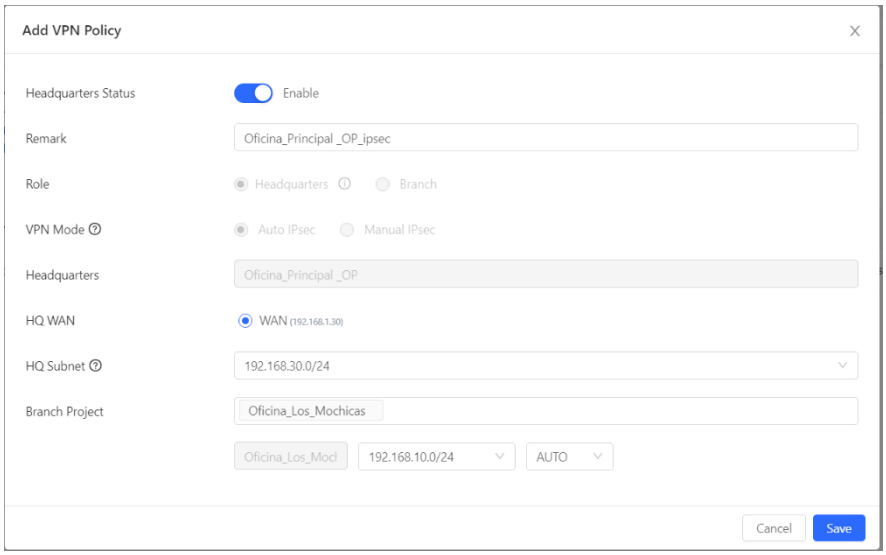


Figura 27 Politicas del VPN

Quedando de la siguiente manera para el servidor VPN como para los Clientes

Figura 28 VPN Conectada y sincronizada

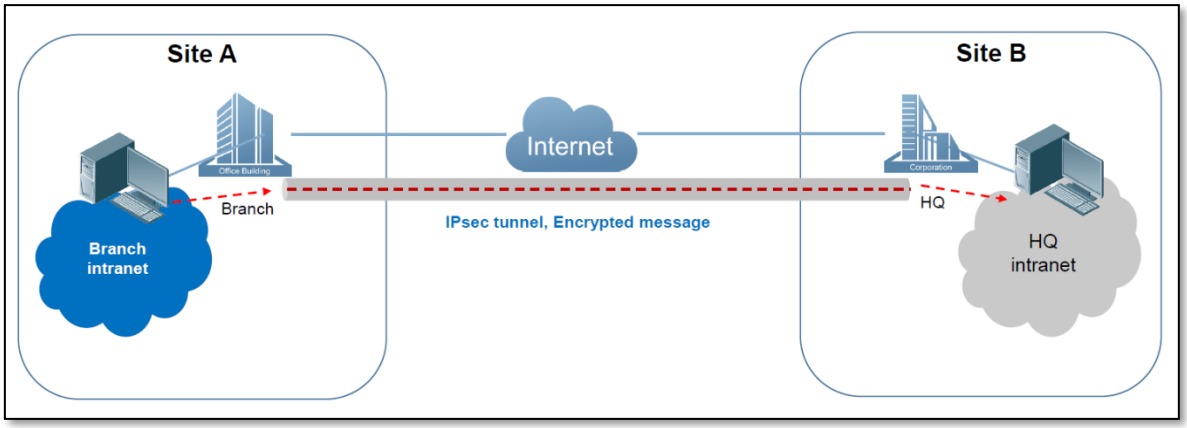


Figura 29 IPSEC tunnel encriptado

Fase 04: Probar, optimizar y documentar el diseño de la red.

a) Actividad 1 Configurar las políticas de la VPN

- Configurando el tipo de política

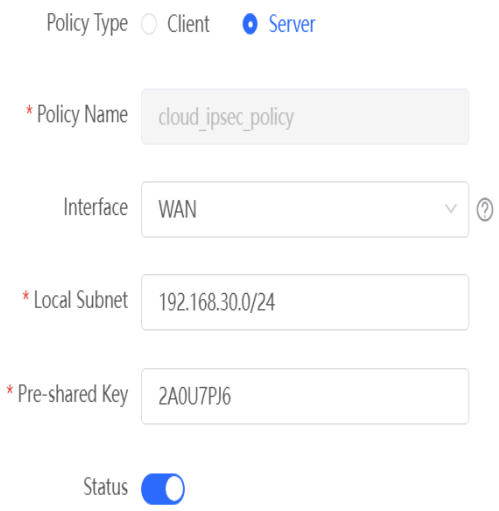


Figura 30 Configurando el Servidor VPN

- Configurando el intercambio de llaves por internet, IKE Policiy

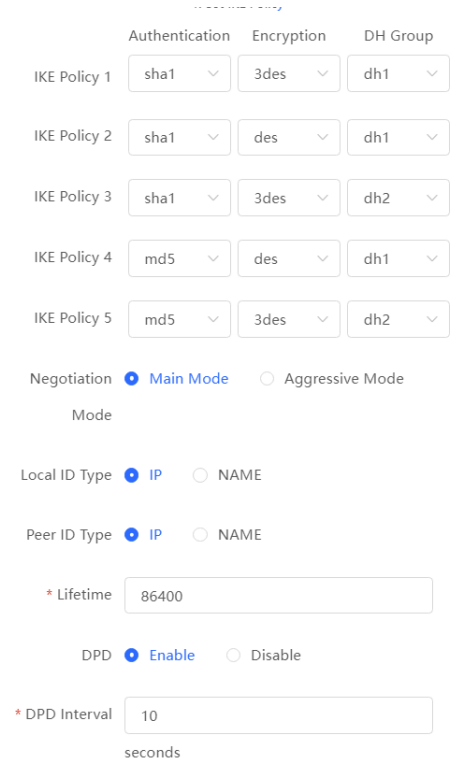


Figura 31 Configuración de la seguridad

- Configurando la política de conexión

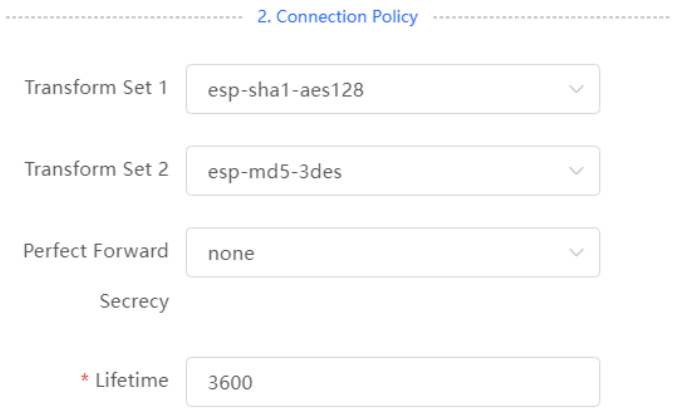


Figura 32 Configuración de la conexión

- Marco completo del IPSec

b)

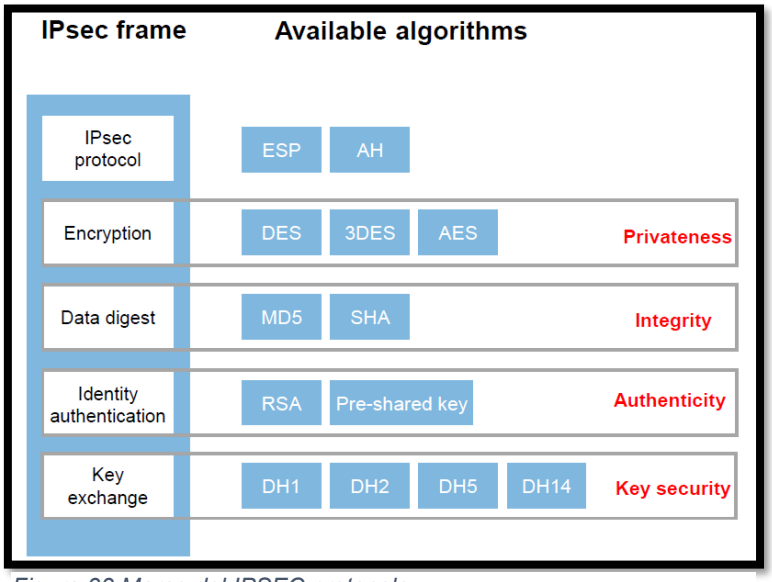


Figura 33 Marco del IPSEC protocolo

- Actividad 2 Probar el diseño entre las sedes, Para empezar con las pruebas del diseño, a continuación, se muestra la configuración actual del VPN en el consorcio, empezaremos con el Router Cliente, como se observa hay 2 secciones IPSec Security Policy y IpSec Connection Status

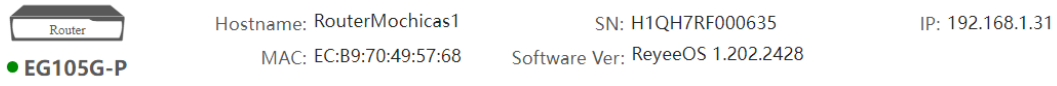


Figura 34 Detalles del router

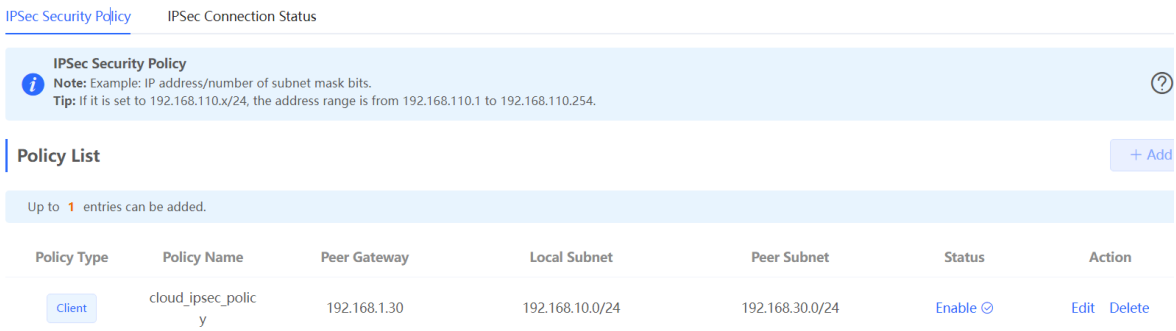


Figura 35 Lista de Políticas VPN

- Como se puede observar el nombre de la política es Cloud_ipsec_policy, siendo su pareja puerta de enlace el otro Router 192.168.1.30/24 y su pareja subnet 192.168.30.0/24

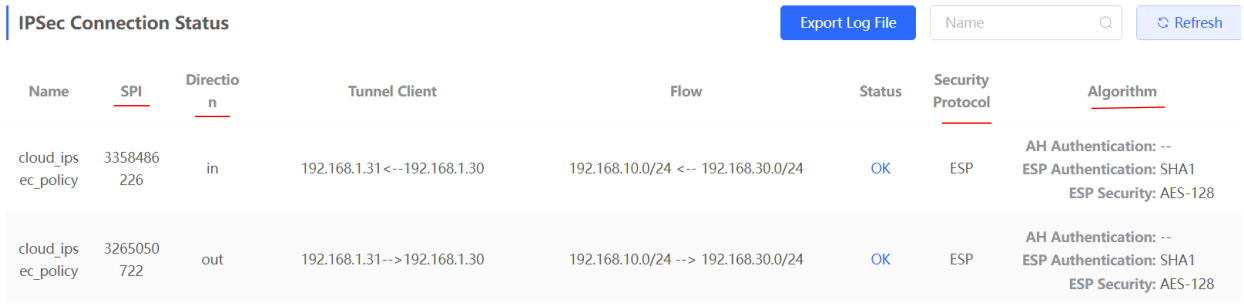


Figura 36 IPSec Estado de conexion

- El siguiente campo es IpSec Connection Status, donde se puede apreciar datos importantes como SPI (Stateful Packet Inspection), Dirección si es entrada o salida la regla, Túnel del cliente y el Flow de donde a donde pasara el trafico, Status, Tipo de seguridad siendo ESP, Algoritmos de la seguridad como SHA1 para Autenticación y AES-128 (la mas segura) para Seguridad.

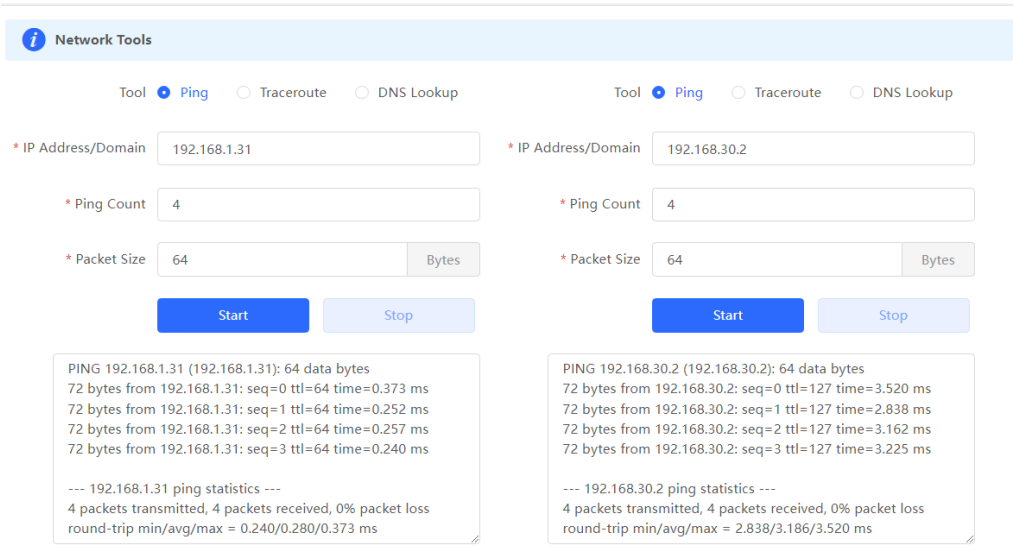


Figura 37 Prueba de Ping entre subnet

- Por ultimo con este Router Ruijie Sede Mochicas, se realiza el testeo prueba de ping para confirmar que se tiene una ruta entre las sedes, Se envia un ping a la puerta enlace del otro Router 192.168.1.31 y a su subnet asociada 192.168.30.0, arrojando las respuestas correctas y por lo tanto el correcto funcionamiento del VPN.

- Ahora veremos la configuración del Servidor de la oficina principal, quien alimenta con los recurso a las demás oficinas, Se observa que el tipo de Politica se encuentra en “SERVER”

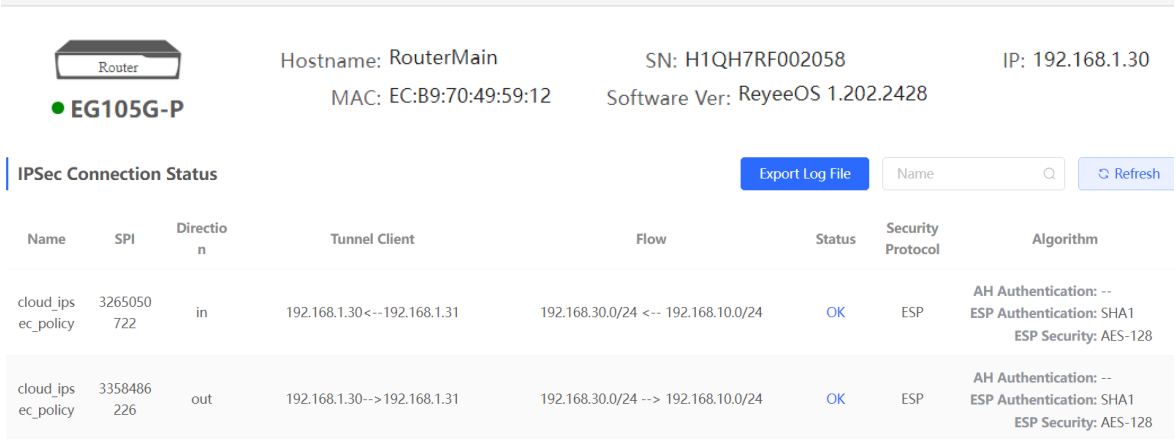


Figura 38 IPSec Estados de conexión

- ahora para los detalles del estado de conexión del servidor principal también se observa que cuenta con un SPI, Dirección de entrada y salida, Protocolo de seguridad ESP, los algoritmos SHA1 y AES-128.

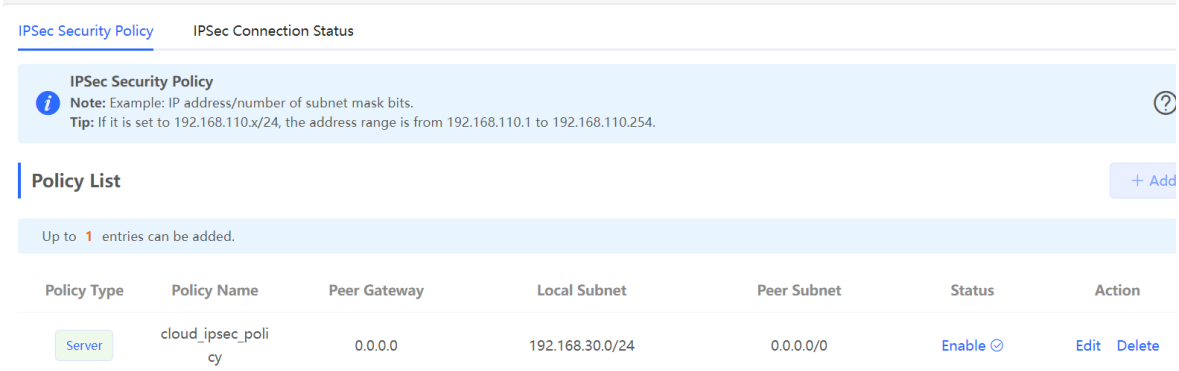


Figura 39 IPSec lista de seguridad

- Para la prueba de conexión desde el Router principal, se envía un ping hacia la oficina en Mochicas y su subred asociada para comprobar conectividad.

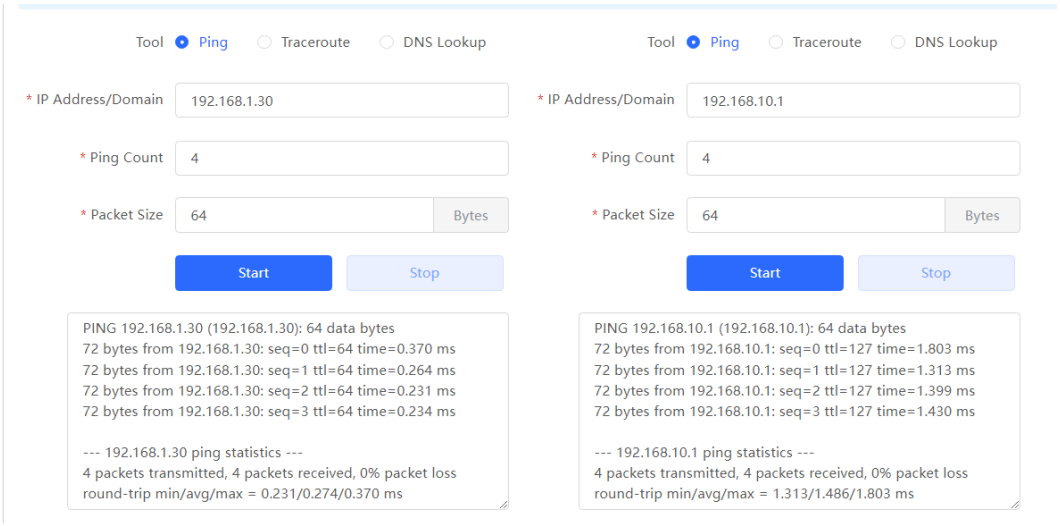


Figura 40 Prueba de pineo del servidor

Principio de Funcionamiento del IPSec

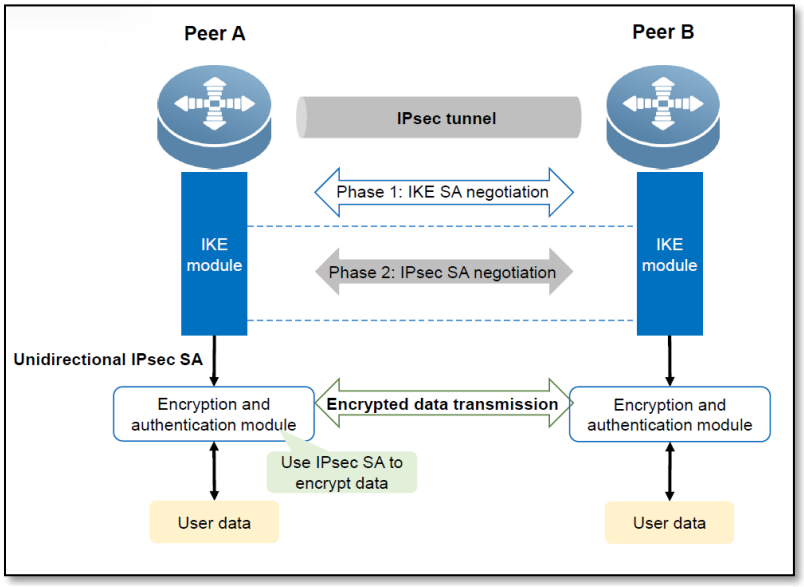


Figura 41 Funcionaiento del IPSec (Ruijie academy)

La imagen nos muestra el ciclo de vida que realiza el trabajo del IPSec hasta entregar la data al usuario

c) Actividad 3 Configurar las carpetas compartidas en la red VPN

Para configurar los recursos compartidos del Consorcio es necesario ingresar primero hacia la ruta predeterminada donde se guardan todos los archivos.

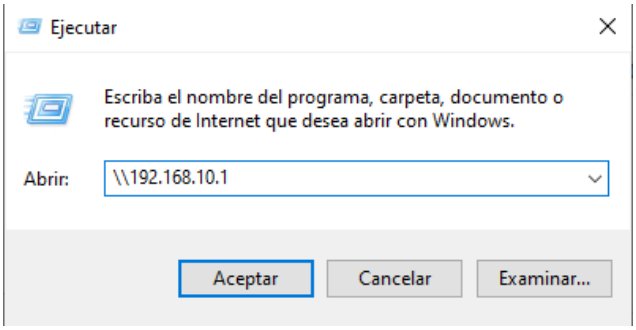


Figura 42 Ruta del servidor storage

- Si la configuración de la VPN no tuvo ningún problema y se genere correctamente, podremos ingresar a la dirección de red de manera local

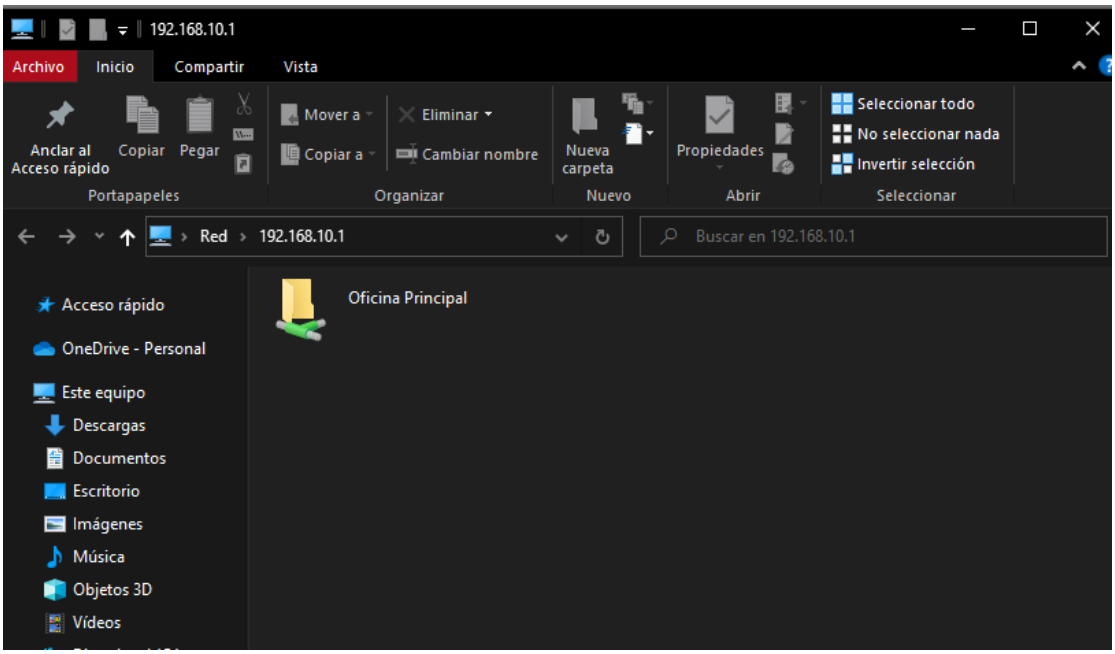


Figura 43 Ubicacion de red de nuestro Storage

- Ahora necesitas guardar nuestra ruta de acceso para hacerlo mas sencillo de encontrar para los usuarios finales, para este procedimiento se puede agregar desde Windows, intentado conectar con otra unidad de red, como el ejemplo a continuación

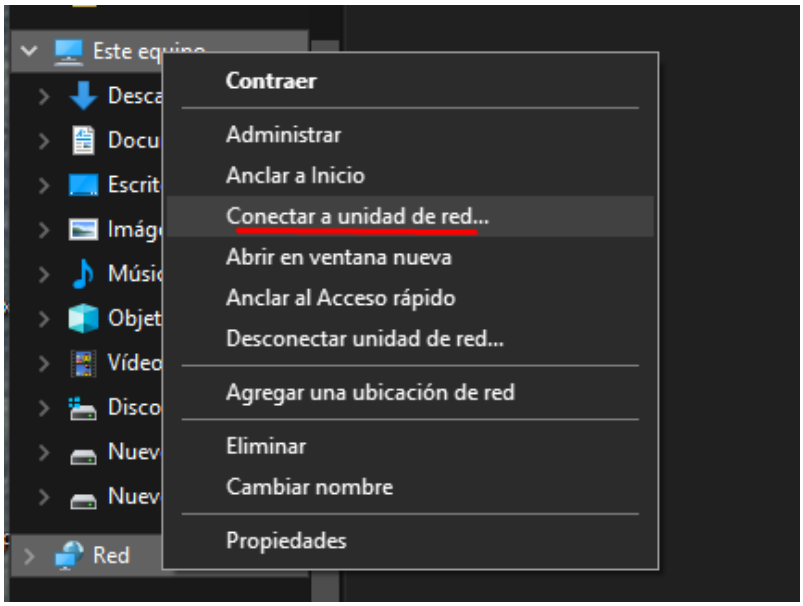


Figura 44 Agregando la ubicacion

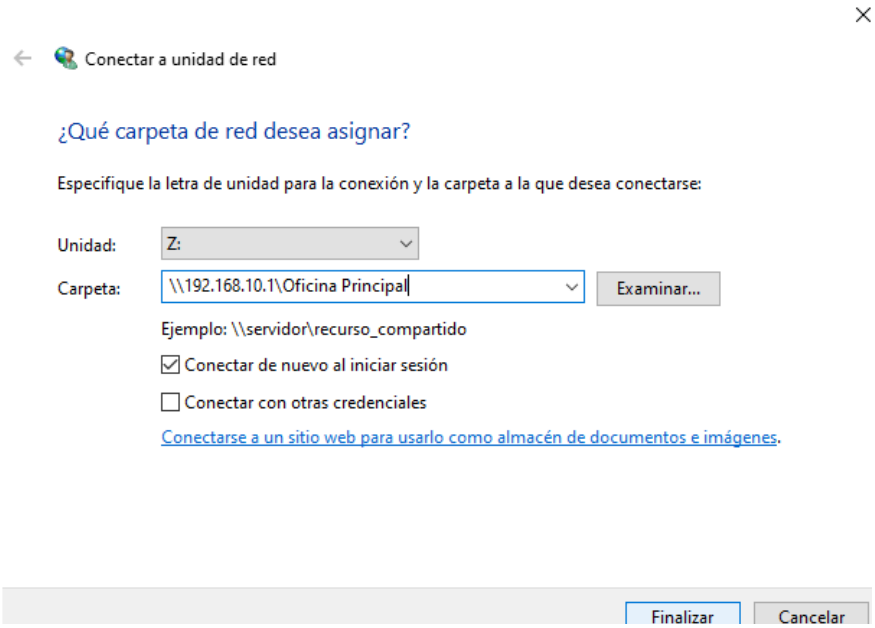


Figura 45 Asignando ruta y letra

Por último, tendremos si se realizaron los pasos mencionados, podremos tener nuestro recurso anclado en la categoría de ESTE EQUIPO, para su rápido acceso.

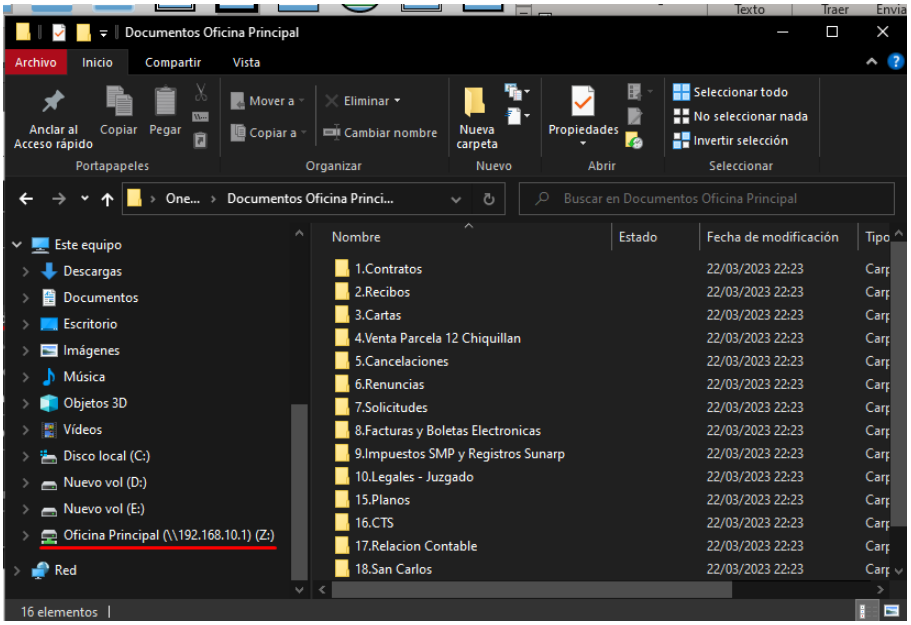


Figura 46 Ruta agregada correctamente