UNIVERSIDAD CIENTÍFICA DEL SUR

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN Y GESTIÓN

"REDES PRIVADAS VIRTUALES (VPN) PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE CATALOGACIÓN EN LA AGENCIA DE COMPRAS DE LAS FUERZAS ARMADAS"

Tesis para optar el título profesional de:
INGENIERO DE SISTEMAS DE INFORMACIÓN

Presentado por:

Jean Javier Martín Calderón Rangel (0000-0001-8467-6857)

Asesor:

Luis Enrique Acosta Medina (0000-0002-0477-0657)

Lima - Perú

2022

UNIVERSIDAD CIENTÍFICA DEL SUR

ACTA DE SUSTENTACIÓN DE TESIS

Lima, 30 de marzo de 2022 «FSUS»

Los integrantes del Jurado de tesis:

Presidente	**LUIS ALBERTO TORRES CABANILLAS**
Miembro 1	**ELMER HUMBERTO MARTIN PISFIL LANGUASCO**
Miembro 2	**JOSE ALBERTO RODRIGUEZ PARRA FERIA**

Se reúnen para evaluar la tesis titulada:
"REDES PRIVADAS VIRTUALES (VPN) PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE CATALOGACIÓN EN LA AGENCIA DE COMPRAS DE LAS FUERZAS ARMADAS"

Presentado por el(la) bachiller.
JEAN JAVIER MARTÍN CALDERÓN RANGEL

Para optar al título profesional de
INGENIERO DE SISTEMAS DE INFORMACIÓN

Asesorado(a) por:
LUIS ENRIQUE ACOSTA MEDINA

Luego de haber evaluado el informe final de tesis y evaluado el desempeño de(l) (los) estudiante de la Carrera de **Ingeniería de Sistemas de Información y Gestión** en la sustentación, concluyen de manera unánime (x) por mayoría simple ( ) calificar a:

Tesista:	**JEAN JAVIER MARTÍN CALDERÓN RANGEL**		
Nota (en letras):	**17**		
Aprobado ( )	Aprobado - Muy buena (X)	Aprobado - Sobresaliente ( )	Desaprobado ( )

Los miembros del jurado firman en señal de conformidad.

LUIS ALBERTO TORRES CABANILLAS
Presidente(a) del Jurado

LUIS ENRIQUE ACOSTA MEDINA
Asesor(a)

ELMER HUMBERTO MARTIN PISFIL LANGUASCO
Miembro 1

JOSE ALBERTO RODRIGUEZ PARRA FERIA
Miembro 2

T // (511) 610 6738
informes@cientifica.edu.pe
cientifica.edu.pe

Redes Privadas Virtuales (VPN) para la gestión de seguridad de la información del sistema de catalogación de la Agencia de Compras de Las Fuerzas Armadas

Jean Javier Martín Calderón Rangel[1] y Luis Enrique Acosta Medina[2]

[1] Carrera de ingeniería de información y gestión, 100038388@cientifica.edu.pe, Facultad de Ciencias Empresariales de la Universidad Científica del Sur. Lima, Perú.

[2] Docente investigador asociado. Facultad de Ciencias Empresariales de la Universidad Científica del Sur. Lima, Perú.

Dedicatoria

A mi madre Clara Rangel que con su cariño, abnegación y sacrificio me supo dar buenos consejos, su comprensión y apoyo en todo momento.

A mi amada esposa Gina, por su amor, comprensión, paciencia y aliento permanente para culminar este trabajo.

A mis hijos Martín y Joaquín, que son la inspiración y la razón de mi vida.

A mi hermana Sisley por su constante apoyo, desde mi época de estudiante, para cumplir mis objetivos profesionales.

A mi hermano Eduardo que está en el cielo, que me alentaba en todo momento para lograr mi meta.

Agradecimientos

A Dios bondadoso, que me ayudo en todo tiempo para lograr mis objetivos.

A mi asesor Mg. Luis Acosta, como testimonio de mi sincera gratitud, por su orientación y consejos en la elaboración de esta Tesis.

A mi amigo Dr. Jorge Cuba por su invalorable apoyo en los comentarios, corrección y edición que permitió culminar este trabajo.

Resumen

Las Redes Privadas Virtuales (VPN) permiten el intercambio de datos a través de internet donde los datos viajan encriptados y se realiza de una red netamente local a una red pública. El objetivo del presente estudio tuvo como propósito Implementar redes (VPN) para gestionar la seguridad de datos e información correspondiente a la catalogación perteneciente a Institución encargada de las compras del sector defensa del Perú (ACFFAA). El estudio investigativo fue de diseño pre-experimental y de tipo Aplicativo con enfoque cuantitativo, con pre-test y post-test de un solo grupo. La muestra fue de 30 colaboradores que fueron los especialistas de seguridad de información de las diferentes Fuerzas Armadas (FF.AA.), a quienes se les aplicaron dos instrumentos que contaron con validez y confiabilidad. Para probar la hipótesis se llegó a emplear la prueba estadística de Wilcoxon y también la de T que es para muestras relacionadas, se halló un positivo nivel de significancia igual a 0,000 y menor a 0.05, en la variable dependiente y sus dimensiones, se concluye, por lo tanto, que el implementar Redes Privadas Virtuales tiene un impacto muy relevante en la administración de seguridad de datos e información del sistema de catalogación de la ACFFAA.

Palabras Clave: Redes Privadas Virtuales, Impacto, Implementación, Seguridad de datos e información.

Virtual Private Networks (VPN) For The Security Management Of Catalog Information In The Armed Forces Purchasing Agency

Abstract

Virtual Private Networks (VPN) allow the exchange of data over the internet where the data travels encrypted and is carried out from a purely local network to a public network. The objective of this study was to implement networks (VPN) to manage the security of data and information corresponding to the cataloging belonging to the Institution in charge of purchasing the defense sector of Peru (ACFFAA). The research study was of a pre-experimental design and of the Applicative type with a quantitative approach, with pre-test and post-test of a single group. The sample consisted of 30 collaborators who were the information security specialists of the different Armed Forces (Armed Forces), to whom two valid and reliable instruments were applied. To test the hypothesis, the Wilcoxon statistical test was used and also the T test, which is for related samples, a positive level of significance equal to 0.000 and less than 0.05 was found, in the dependent variable and its dimensions, it is concluded, Therefore, the implementation of Virtual Private Networks has a very relevant impact on the data and information security administration of the ACFFAA cataloging system.

Keywords: Virtual Private Networks, Impact, Implementation, Data and information security.

Introducción

La presente investigación se refiere al tema de la seguridad de la información del sistema de catalogación para la defensa (SICAD), que según (ISO, 27001) puede definirse como "… la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización".

Las características principales para lograr la seguridad de la información es que estas deben estar disponibles cuando se les requiere, teniendo en cuenta la privacidad; debe tener accesos restringidos solo para el personal autorizados.

Para analizar esta problemática es necesario identificar y analizar sus causas. La principal causa de la inseguridad de la información confidencial del SICAD fue exponerla, a través de redes públicas (internet) que no cumplen con las características descritas en el parrado anterior.

De un tiempo a esta parte, las redes privadas virtuales (VPN) han gozado de gran popularidad en las organizaciones, desde la pública en los gobiernos hasta la privada en las empresas, sean pequeñas, medianas o grandes (Areitio, 2008), asegurando la confidencialidad de sus comunicaciones y por ende de su información, pero; sobre todo el navegar por internet sin ser espiado.

La ACFFAA según el (Decreto Legislativo 1128, 2012, pág. 2), nos menciona que es un organismo público ejecutor el cual se encuentra adscrito al Ministerio de Defensa Peruano, el que se encarga de realizar la planificación, organización y ejecución del Plan Estratégico para realizar las Compras del Sector nacional de Defensa, que tuvo como limitante el no acceso a bases de datos extranjeras quienes proporcionarían información sobre proveedores-mercado de origen, fabricantes, detalles técnicos de los diferentes equipos, como también las partes y piezas de los suministros. Ante esta limitante la (ACFFAA, 2019) firma contrato con (ISDEFE) de España, con el fin de implementar el sistema de catalogación (SICAD), que es una base de datos la que contiene información de los artículos de defensa de fabricantes y comercializadores de diversos países, permitiendo obtener, difundir y dar a conocer la información que identifica los diferentes equipos, armamentos, materiales y repuestos que requieren y son utilizados por la Fuerza Aérea, el Ejército, la Marina y el Comando Conjunto de las Fuerzas Armadas, a quienes denominaremos (OBAC). En tal sentido la información contenida en el SICAD es de carácter muy importante y sensible, la que deberá ser manejados con los más altos cuidados siguiendo los estándares de seguridad y también confidencialidad.

La (ACFFAA, 2021), procedió a extender el uso del SICAD a los OBAC utilizando redes públicas, constituyéndose esta extensión en un problema para la seguridad de la información que maneja el SICAD, ya que es un método de conexión inseguro, porque no cuenta con los mecanismos de seguridad y garantía adecuada para la información. De esta manera, la información que es muy sensible y confidencial de los materiales, repuestos y equipos pertenecientes a la gestión logística de los OBAC y de cada una de las empresas extranjeras y nacionales que los suministran, es expuesto a internet, siendo

vulnerable y quedando a disposición de cualquier atacante, como lo describe la Ilustración 1.

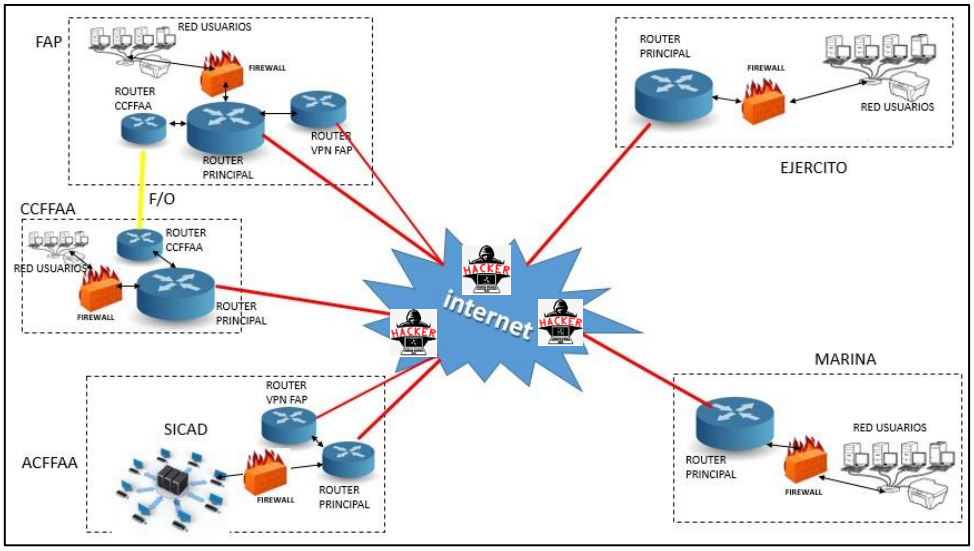


Ilustración 1. Redes entre la ACFFAA y los OBAC, antes de la implementación
Fuente: Elaboración Propia

Luego de plantear el problema aparece la interrogante que lleva a establecer una respuesta a la siguiente pregunta ¿en qué medida la implementación de redes VPN impacta en la gestión de seguridad de la información de catalogación en la ACFFAA?, ante la interrogante, se revisaron trabajos de diversos autores internacionales y nacionales que aportan lo siguiente:

En el caso internacional, los autores (Hajrizi, Bajraliu, Qehaja, & Shabani, 2016) en su Artículo[1], tuvieron a bien determinar nuevos métodos como: Redes Privadas Virtuales de Dinámica Multipunto (DMVPN), destacando los mejor y las buenas prácticas que corresponde tener e implementar a toda empresa, buscando garantizar y potenciar la seguridad en las comunicaciones por intermedio de sus oficinas que vienen funcionando remotamente, como una solución que permite realizar la conexión de manera directa entre todos los puntos sin tomar en cuenta el lugar donde se encuentren; este paper es considerado en nuestra investigación porque aporta conocimiento en cuanto a seguridad de las comunicaciones y de nuevos métodos en el uso de las VPN.

En ese sentido (León, 2018) en su tesis de Maestría[2], tuvo por objetivo abordar el tema enfocado en la Seguridad en las redes con un enfoque en la implementación adecuada de las VPN como también en las ventajas que esta ofrece para brindar una adecuada atención a la necesidad actual de la seguridad requerida en el ámbito de la informática y las comunicaciones; esta tesis de maestría fue considerada para nuestro artículo porque aporta en la identificación de las amenazas que las empresas han sufrido con respecto a su información en materia de aseguramiento, integridad y confidencialidad de los datos e información.

[1] *"Enterprise Integration, Networking and Virtual Communications"*
[2] *"Monitoreo de rendimiento para la seguridad de VPN a través de PfSense y OpenVPN"*

En el contexto nacional, (Niño, 2018), en su tesis de Maestría[3], cuyo objetivo fue realizar la modelación de un SGSI el cual permita el fortalecimiento de la disponibilidad, confidencialidad, integridad, realizando el monitoreo de los activos correspondientes a la información en cada uno de los procesos que están bajo la administración de la (ODEI) "Oficina Descentralizada Estadística de Información" en Lambayeque. Así, llego a la conclusión que el SGSI es de gran apoyo en la dirección de las organizaciones, como también en la parte de control y operación de forma transparente y sistemática en sus diversos procesos con la finalidad de obtener éxito en cada una de sus actividades, otra conclusión fue que la "NTP ISO/IEC 27001:2014" es una solución al problema ante falta de administración de seguridad de datos e información de la ODEI; esta tesis de maestría fue seleccionada y considerada en la presente investigación, ya que gran parte de sus lineamientos realizaron un aporte al conocimiento sobre la integridad, confidencialidad y disponibilidad de la información en materia seguridad de datos e información, fortaleciendo nuestro trabajo.

Luego de la revisión de los antecedentes y en un entorno donde los datos y la información han cobrado relevancia y se han convertido indudablemente en un activo estratégico para el desarrollo de las organizaciones, el flujo de la información que transita por las redes, debe garantizar en sus enlaces y prolongaciones seguridad en las mismas. Las cuales son de todas maneras particulares por tener la catalogación de privadas, virtuales y muy seguras teniendo por característica a: a) realizar el transporte de paquetes IP haciendo la utilización de un túnel desde las redes que se manejan remotamente de forma transparente ofreciendo soporte a protocolos múltiples, sin que se hagan notar que tienen una separación por redes públicas, b) se agrega el cifrado o encriptado, decodificando todos los datos de manera que los paquetes IP que sea interceptados sean indescifrables, c) realizar la autenticación exitosa para prevenir cualquier ataque a los diferentes recursos. Para la implementación utilizamos como base la metodología PPDIOO[4] de CISCO (Arteaga & Huamán, 2014, pág. 25).

Los principales beneficiarios de esta implementación son los OBAC tal como lo muestra la Ilustración 3, pues el análisis efectuado de los antecedentes ayudó a realizar la identificación y la eliminación de los diversos riesgos negativos que son los causantes disminuir la eficiencia al gestionar la seguridad del uso de la información del sistema de catalogación perteneciente a la ACFFAA.

[3] *"Modelo de un sistema de administración de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática – INEI filial Lambayeque"*

[4] a) Preparar; b) Planificar; c) Diseñar; d) Implementar; e) Operar; y f) Optimizar

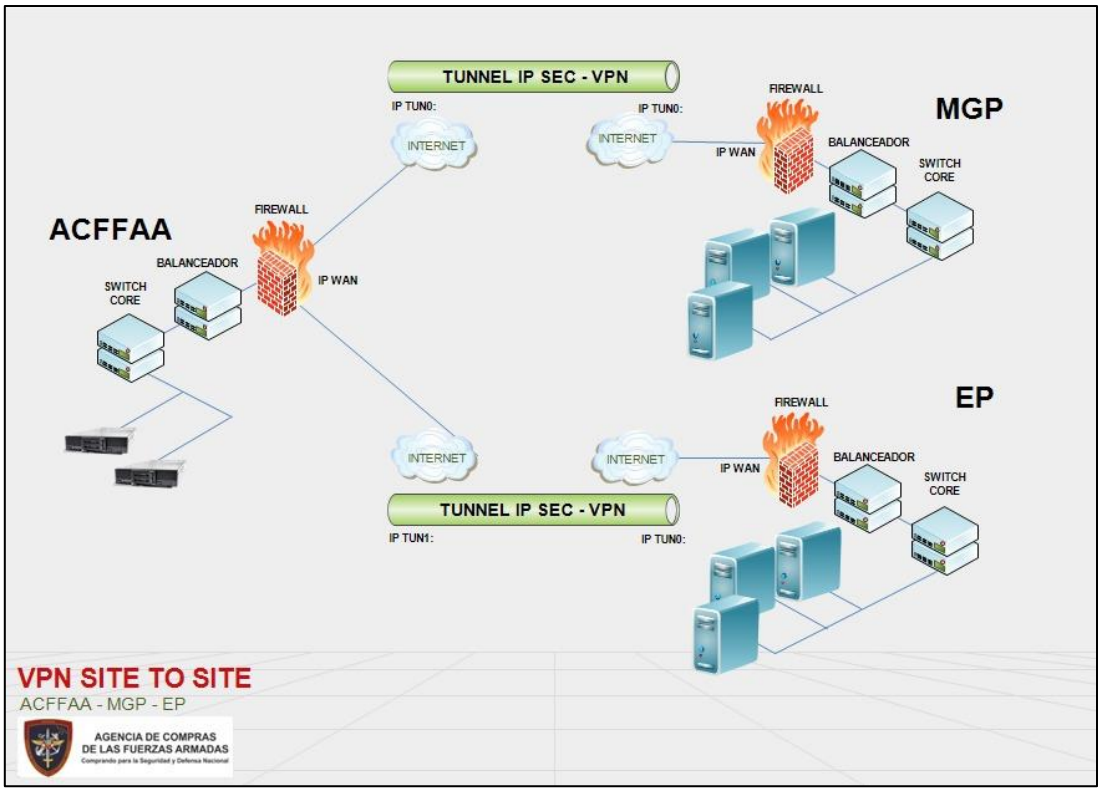


Ilustración 2. Redes Privadas Virtuales entre la ACFFAA y los OBAC después de la implementación
Fuente: Elaboración Propia

Cabe resaltar que mantener adecuadamente una infraestructura, con dichas características tiene por requerimiento conocimientos y habilidades por parte del equipo de TI; pues las diferentes redes modernas demandan verdaderos retos de diseño al llegar a ser muy dificultosos de manejar; en este entorno, las VPN conjuntamente con la seguridad de datos e información cobran un sentido especial para la protección de datos en Internet, por ello y frente a lo descrito en los párrafos precedentes, la presente investigación tuvo por objetivo determinar el impacto de El implementar Redes Privadas Virtuales sobre la ACFFAA (Seguridad de datos e información del sistema de catalogación) al acceder a través de redes públicas (internet) de forma segura (data encriptada) a la red privada (LAN) de la ACFFAA, garantizando de esta manera que los OBAC logren el intercambio de información de forma segura.

Así, gracias a las VPN, podemos cubrir los principios fundamentales de la seguridad informática: a) la confidencialidad, solo para los usuarios OBAC quienes serán los únicos autorizados que podrán acceder a los diversos recursos, datos e información del sistema de catalogación de la ACFFAA, b) integridad, el objetivo de este principio mantendrá sin modificaciones la información del SICAD, cuando no hay una autorización de por medio, c) disponibilidad, el SICAD siempre debe estar listo para ser utilizado, sin presentar problemas de rendimiento o acceso cuando se requiera.

Para el desarrollo del presente trabajo se logró identificar las variables que serán objeto de estudio, como variable independiente definimos a la red privada virtual (VPN) y como variable dependiente a la Seguridad de la Información, donde se determinó sus dimensiones bajo la que será analizada: como es la confiabilidad de la información, integridad de la información y la disponibilidad de la Información. En este trabajo podemos describir el problema general como ¿en qué medida la implementación de redes VPN impacta en la gestión de seguridad de la información de catalogación en la ACFFAA?, y como problemas específicos: ¿en qué medida la implementación de redes VPN impacta en la gestión de confiabilidad de la información de catalogación en la ACFFAA?, ¿en qué medida la implementación de redes VPN impacta en la gestión de integridad de la información de catalogación en la ACFFAA? y ¿en qué medida la implementación de redes VPN impacta en la gestión de disponibilidad de la información de catalogación en la ACFFAA?.

El objetivo general de nuestra investigación es el de lograr Implementar Redes VPN para la gestión de Seguridad de la información de Catalogación en la ACFFAA, mientras que los objetivos específicos están orientados a lograr mejoras en la gestión de Confiabilidad, Integridad y Disponibilidad de la información de Catalogación en la ACFFAA.

Como en toda investigación se ha definido la hipótesis general y las hipótesis específicas para poder describir la estadística. Así la hipótesis general, considera que la implementación de Redes VPN tiene un impacto estadísticamente significativo en la gestión de Seguridad de la información de Catalogación en la ACFFAA. Las hipótesis específicas consideran que: la implementación de Redes VPN tiene un impacto estadísticamente significativo en la gestión de confiabilidad, integridad y disponibilidad de la información de catalogación en la ACFFAA.

Para poder evaluar las hipótesis se implementó un cuestionario con nueve preguntas que corresponden a un escenario antes de la implementación de las Red VPN y 9 preguntas que corresponden a un escenario después de la implementación de la red VPN, con el cuestionario se intenta conocer la percepción de los trabajadores con respecto a la implementación de las redes VPN, la muestra fue conformada por 30 trabajadores quienes respondieron de manera virtual mediante un formulario diseñado en Google.

Finalmente podemos indicar que la presente investigación es de vital importancia porque la implementación de VPN, al interior de la ACFFAA, permitirá subsanar las deficiencias de la seguridad de la información en que incurrió la ACFFAA, al compartir información relevante y reservada, a través de un canal (internet) que no garantiza las condiciones de disponibilidad, integridad y confiabilidad.

Métodos

La presente investigación es de tipo aplicada, que según (Chávez, 2007) " […] tiene como fin principal resolver un problema en un periodo de tiempo corto. Dirigida a la aplicación inmediata mediante acciones concretas para enfrentar el problema, mediante actividades precisas para enfrentar el problema". El propósito de la investigación es brindar una solución inmediata relacionada al problema identificado en la gestión de seguridad de la información del SICAD de la ACFFAA, al descentralizar su acceso a las Instituciones Armadas, utilizando Redes Públicas (internet). Nuestra investigación propone para la solución a este problema la Implementación de redes VPN en el proceso de descentralización.

Como señalan Hernández, Fernández & Baptista (2006), en los diseños pre experimentales:

"[…] se manipulan deliberadamente, al menos, una variable independiente para observar su efecto sobre una o más variables dependientes, sólo que difieren de los experimentos "puros" en el grado de seguridad que pueda tenerse sobre la equivalencia inicial de los grupos". (Hernández, Fernández, & Baptista, 2014)

"[…] los sujetos no se asignan al azar a los grupos ni se emparejan, sino que dichos grupos ya están conformados antes del experimento: son grupos intactos (la razón por la que surgen y la manera como se integraron es independiente o aparte del experimento)". (Hernández, Fernández, & Baptista, 2014)

La investigación tendrá un diseño pre experimental porque pretende medir la variable independiente (Redes VPN)

El enfoque que se utilizará para el presente estudio es el enfoque cuantitativo. Se investigará a partir de un problema específico y bien definido y, luego de revisar la literatura sobre la materia, se construirá un marco teórico y a partir de éste, se establecerán las hipótesis, que serán verificadas luego de la recolección y análisis de datos, las cuales se plantean a través de un diseño de investigación que utiliza métodos analíticos para lograrlo, presentando los resultados en forma numérica (Hernández, Fernández, & Baptista, 2014).

Las variables identificadas en el estudio son:

1) Variable Independiente (X) = Red Privada Virtual (VPN)

   A la que (Veron, 2010), define como " un enlace establecido por intermedio de internet de una red local a una red pública, los datos viajan encriptados y solo pueden ser entendidos por el origen y el destino.

2) Variable Dependiente (Y) = Seguridad de la Información

   A la que (Godoy, 2014), como: "al conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma".

Operacionalización de las variables

Variable Independiente (X) = Red Privada Virtual (VPN)

Dimensiones:

- Conexiones
- Internet
- Seguridad

Variable Dependiente (Y) = Seguridad de la Información

Dimensiones:

- Confiabilidad
- Integridad
- Disponibilidad

Población (criterios, inclusión y exclusión)

Comprenderá 30 personas funcionarios de las Oficinas de Informática de los OBAC y la ACFFAA, cuyas actividades están vinculadas a la administración de la gestión de la Seguridad de la Información del SICAD otorgado por la ACFFAA.

La población comprenderá al personal antes mencionado de las siguientes entidades: 06 funcionarios del Centro de Informática del Ejército del Perú (CINFE), 06 funcionarios de Dirección de Telemática (DIRTEL) Marina de Guerra del Perú (MGP), 06 funcionarios del Servicio de Informática (SINFA) Fuerza Aérea del Perú (SINFA), 06 funcionarios de la 6ta DIEMCFFAA Comando Conjunto de las FF.AA. (CCFFAA) y 06 funcionarios de la Oficina de Informática ACFFAA.

La muestra será igual al total de la población, es decir comprenderá a las 30 personas que trabajan en las Oficinas de Informática de las Instituciones mencionadas en la población.

El muestreo es probabilístico por conveniencia al 100% de la población.

La técnica de recolección de la información necesaria para lograr los objetivos de nuestro estudio será la encuesta. Este proceso de recolección de datos nos permitirá comunicarnos con observadores individuales a través de un cuestionario, “consistente en un conjunto de preguntas relacionadas con una o más variables que se están midiendo” (Hernández, Fernández, & Baptista, 2014).

La Encuesta, permitirá la recolección de información en forma oral y escrita, a través de preguntas o cuestionarios que se realizarán a funcionarios de las Oficinas de Informática de los OBAC y la ACFFAA, cuyas actividades están relacionadas con la gestión de la Seguridad de la Información del SICAD otorgado por la ACFFAA, se utilizarán procedimientos estándar, para que a cada encuestado se les haga la misma pregunta o en más o menos la misma manera.

La Recopilación documental y bibliográfica de libros, revistas y publicaciones y recursos electrónicos que contengan información asociada al tema de investigación. La información obtenida se utilizará de forma preliminar en el desarrollo del marco teórico y conceptual de la investigación, pues recogerá

importantes estudios, investigaciones, datos e información sobre el problema construido.

Encuestas, basadas en una serie de preguntas, que se diseñará y utilizará específicamente para medir opiniones sobre ciertos hechos o eventos.

Cuestionarios de Opinión, con preguntas en la escala de Likert, destinado a obtener respuestas sobre el problema en estudio y que el consultado llena por sí mismo en formato impreso. Permitiendo medir las reacciones o actitudes de las personas hacia las variables encuestadas.

Fichas Bibliográficas, a través del cual se recopilan y recuperan datos de investigación importantes de fuentes bibliográficas como libros, revistas, periódicos, internet, y otras fuentes no bibliográficas.

Se consideró el consentimiento informado como cumplimiento de cada uno de los aspectos éticos al momento de recolectar los datos y encontrar los óptimos resultados para la investigación, tuvieron que ser sometidas al comité de investigación de la UCSUR para confirmar si toda la información recopilada realmente era confiable.

La autenticidad de nuestro instrumento de recolección de datos "cuestionario" será corroborada a través de juicio de expertos, para ello se recibirá el apoyo de profesionales de la Universidad Científica del Sur, para realizar el análisis del contenido y rectificar que los ítems plasmados sean los correctos.

Para obtener la certeza de los resultados obtenidos luego de utilizar nuestra herramienta de recolección de datos, se medirá usando el coeficiente Alfa de Cronbach con el propósito de medir la integridad. "Generalmente existen márgenes de error en los modelos estadísticos" (Kerlinger & Lee, 2002). "Dependiendo del valor erróneo obtenido en la evaluación del instrumento medición, este será poco o más confiable" (Quero Virla, 2010). En el trabajo de investigación de (Hernández & Pascual Barrera, 2018) citaron a (George & Mallery , 2003) donde sugieren como recomendación estimar los coeficientes de alfa de Cronbach.

El procesamiento da datos estadísticos comenzará con la importación de cuestionarios aplicados en un formato predefinido para importar información del cuestionario preparado. Una vez realizadas las operaciones de recojo de información, se seguirá con el proceso de organización de los datos, previo proceso de conteo y otros que se generaron. Los datos serán ingresados por el mismo investigador.

Para procesar de la información recopilada y organizada se utilizará el SPSS versión 22 en la versión de Windows apoyándonos en el Microsoft Excel, obteniéndose los resultados estadísticos de acuerdo con nuestro estudio. Los datos se presentarán en estadísticas univariadas que se representan en tablas de distribución de frecuencias con sus respectivas métricas. Para evaluar los resultados estadísticos obtenidos se utilizarán las pruebas de estadística "T y Wilcoxon".

El análisis de los datos nos permitirá describir y conocer, a partir de las tablas y datos estadísticos que se construyeron, cómo es que estaba

estructurado el problema materia de investigación, para lo cual se observará cada uno de sus componentes. Este se considera como un primer análisis en base a los datos de manera “aislada” que ofrece cada uno de las tablas construidas con información numérica.

La interpretación de la información obtenida, permitirá explicar el significado de las cosas, hechos y sucesos relevantes de la investigación ocurridos en el análisis previo. Sin embargo, para dar un significado real a la acción colectiva, la información que se analiza e interpreta se colocará en relación con otros datos ampliando así el significado explicativo de las cosas. Los datos no se separarán, y siempre se interpretarán y comprenderán en relación con otros datos, pudiendo estos datos también incluir fuentes de información de referencia.

En este proceso de análisis e interpretación, se definirá de manera previa y precisa el sentido de la investigación, sabiendo lo que pretendemos y teniendo claro que, con el uso de la Redes Virtuales Privadas (VPN) como fundamento teórico, es más fácil evaluar la información recogida.

El marco teórico utilizado y el conocimiento asociado al mismo, permitirán una mejor comprensión de los resultados obtenidos para que puedan ser explicados con un respaldo y no solo desde la evaluación empírica.

Esta investigación se realizará sobre la base de tres principios éticos básicos: i) Respeto a las personas; ii) Justicia y iii) Búsqueda del bien, esforzándonos por maximizar los beneficios y minimizar el daño y el error.

El investigador asume su responsabilidad ética diseñando e implementación estándares de conducta profesional y reconociendo esta obligación (moral y ética) hacia la sociedad.

Dentro del desarrollo de nuestra investigación hemos enfrentado algunas limitaciones que a continuación se detallan:

La primera limitación está referida al poco tiempo que lleva de funcionamiento la ACFFAA y al poco tiempo que se tendrá para evaluar el impacto post test que ejercerá la implementación de la VPN sobre la gestión de la seguridad de la información.

La segunda limitación está en la disponibilidad de tiempo del personal de Infraestructura de redes de los diferentes OBAC que por sus labores cotidianas y por su recargada carga laboral no disponían del tiempo adecuado.

La tercera limitación del presente trabajo es el desconocimiento técnico en el uso avanzado de los gateways por parte de algunos encargados de Infraestructura de redes de las FF.AA.

La población comprenderá a funcionarios y empleados de la Oficina de Informática de las siguientes instituciones castrenses: Ejército del Perú (EP), Marina de Guerra del Perú (MGP), Fuerza Aérea del Perú (FAP), Comando Conjunto de las FFAA (CCFFAA) y la Agencia de Compras de las Fuerzas Armadas (ACFFAA).

La muestra será igual al total de la población, es decir, comprenderá a las 30 personas especialistas en Seguridad de la Información que trabajan en las Oficinas de Informática de las Instituciones mencionadas en la población.

Los procedimientos relacionados con la recolección de datos, forman parte esencial del presente trabajo, para lo cual identificamos la muestra, el muestreo el instrumento, el tratamiento y seguridad de los datos, consentimiento informado y las limitaciones que se puedan presentar podemos indicar que la investigación es de tipo aplicada, ofrece una solución importante con relación al problema latente de la inseguridad en la información del SICAD en la ACFFAA, cuando esta es publicada a través de internet; el diseño será pre experimental, con un enfoque cuantitativo, como lo indica (Hernández, Fernández, & Baptista, Metodología de la Investigación, 2010) construimos un marco teórico y realizado la propuesta de hipótesis, que fue verificada y contrastada con la estadística correspondiente.

Para completar el cuestionario desarrollado, se consideró el consentimiento informado como cumplimiento de los aspectos éticos, así como el tratamiento anónimo de la información recolectada en el instrumento, indicamos que antes de someter a práctica, el instrumento de recolección de datos fue sometido al comité de investigación de la UCSUR para confirmar si toda la información recopilada realmente era confiable.

En el consentimiento informado, se indica que los participantes pueden abandonar la investigación en cualquier momento, si en algún momento se siente afectado por alguna pregunta, sin afectar su condición como trabajador, podemos indicar como limitaciones al estudio poder sentirse obligados a poder completar el cuestionario, por la naturaleza del puesto de trabajo, ante esta situación se indica en el consentimiento informado se indica que las preguntas estas dirigidas a poder conocer su apreciación con respecto al uso de la VPN y como el uso colabora en el desarrollo de su trabajo en una condición de trabajo a distancia.

La muestra fue constituida por 30 trabajadores del sector Defensa, quienes cumplen roles de especialistas en seguridad de datos e información, quienes pertenecen a las siguientes instituciones Comando Conjunto de las Fuerzas Armadas (06), Ejército del Perú (06), Marina de Guerra del Perú (06), Fuerza Aérea del Perú (06), Personal de la Agencia de Compras (06).

Descripción del instrumento de recolección de datos

El instrumento utilizado fue un cuestionario virtual elaborado en Google Forms®, con nueve (09) preguntas en el Pre-test y nueve (09) preguntas en el Post-test para la variable dependiente: seguridad de datos e información, integrada en sus tres dimensiones: confidencialidad, integridad y disponibilidad de la información. Se hizo uso de la escala de Likert del 1 al 5 donde (1) Nunca, (2) Casi nunca, (3) A veces, (4) Casi siempre y (5) Siempre. Los instrumentos se validaron por tres expertos especialistas del área y para el proceso de confiabilidad se realizó a través del Alpha de Cronbach los resultados fueron en el “pre-test de 0.705 (aceptable)” y para el “post-test de 0.873 (bueno)”. Se procesaron los datos con el aplicativo SPSS, para la prueba de hipótesis con la

prueba de T y Wilcoxon. Para realizar la medición de la variable dependiente y sus dimensiones se ha utilizado Baremo según lo especifica la Tabla 1.

Tabla 1. Tabla de Baremo

Seguridad de la información
9 a 21 - (Nivel según baremo: Bajo) *22 a 34* - (Nivel según baremo: Medio) *35 a 45* - (Nivel según baremo: Alto)

Fuente: Elaboración por cuenta propia con el software IBM SPSS.

En la Tabla 2 se observa la fiabilidad del instrumento el cual fue realizado a través del "Alfa de Cronbach", para la variable dependiente "seguridad de datos e información" utilizado en el pre-test, el cual está compuesto de 9 items obteniendo como resultado 0.705 lo cual está definido como Aceptable.

Tabla 2. Estadístico de Fiabilidad de Instrumentos 1 (seguridad de datos e información) Pre-test

Confiabilidad según "Alfa de Cronbach"	N° de Elementos
.705	9

Fuente: Elaboración por cuenta propia con el software SPSS

En la Tabla 3 se observa la fiabilidad del instrumento realizada a través del Alfa de Cronbach para la variable dependiente "seguridad de datos e información" utilizado en el post-test, el cual está compuesto de 9 ítems y nos ha dado como resultado 0.873 lo cual está definido como Bueno.

Tabla 3. Estadístico de Fiabilidad de Instrumentos 2 (Seguridad de datos e información) Post test

Confiabilidad según "Alfa de Cronbach"	N° de elementos
.873	9

Fuente: Elaboración por cuenta propia con el software SPSS

Resultados

Nuestra investigación al ser de diseño pre experimental y tipo Aplicada, tuvo etapas para la recolección de datos, teniendo una primera etapa (Pre-test) donde las Redes Privadas Virtuales no han sido implementadas y otra (Post-test) donde las Redes Privadas Virtuales ha sido implementadas y ejecutadas, permitiendo realizar una comparación entre ambos momentos, los que posteriormente fueron procesados con el aplicativo estadístico SPSS.

a) Análisis Estadístico de la Muestra

Se trabajó con la muestra de la población de estudio, que es un total de 30 encuestados, quienes son los especialistas en seguridad de datos e información divididos de la siguiente manera: Comando Conjunto de las Fuerzas Armadas (06), Ejército del Perú (06), Marina de Guerra del Perú (06), Fuerza Aérea del Perú (06), así como también de la Institución encargada de las compras del sector defensa (06).

b) Análisis descriptivo de la Variable

Tablas cruzadas

La Tabla 4 que a continuación se detalla, indica que el 46.7% nos hace referencia a un nivel alto, seguido de un 3.3% de nivel medio. y el 50% de nivel bajo.

*Tabla 4. Tipo de Prueba*Seguridad de datos e información tabulación cruzada*

			Seguridad de datos e información			
			Nivel baremo bajo	Nivel baremo medio	Nivel baremo alto	Total
Tipo de Prueba	Pre-Test	Recuento	30	0	0	30
		% del total	50,0%	0,0%	0,0%	50,0%
	Post-Test	Recuento	0	2	28	30
		% del total	0,0%	3,3%	46,7%	50,0%
Total		Recuento	30	2	28	60
		% del total	50,0%	3,3%	46,7%	100,0%

Fuente: Elaboración por cuenta propia con el software SPSS

Como podemos visualizar la Ilustración 4, luego de ser aplicado el instrumento en el pre-test, los 30 especialistas de seguridad de datos e información seleccionados respondieron que no había una adecuada gestión de la seguridad de datos e información antes de implementar las Redes Privadas Virtuales siendo de nivel bajo, en el post-test después de la implementación de las Redes Privadas Virtuales dos (02) especialistas de seguridad de datos e

información (3.3%) respondieron que percibían a veces una correcta gestión de la seguridad de datos e información siendo de nivel medio, y el (46.7%) veintiocho (28) especialistas respondieron que después de la implementación de las Redes Privadas Virtuales percibían que había mejorado significativamente la gestión adecuada de la seguridad en la información.

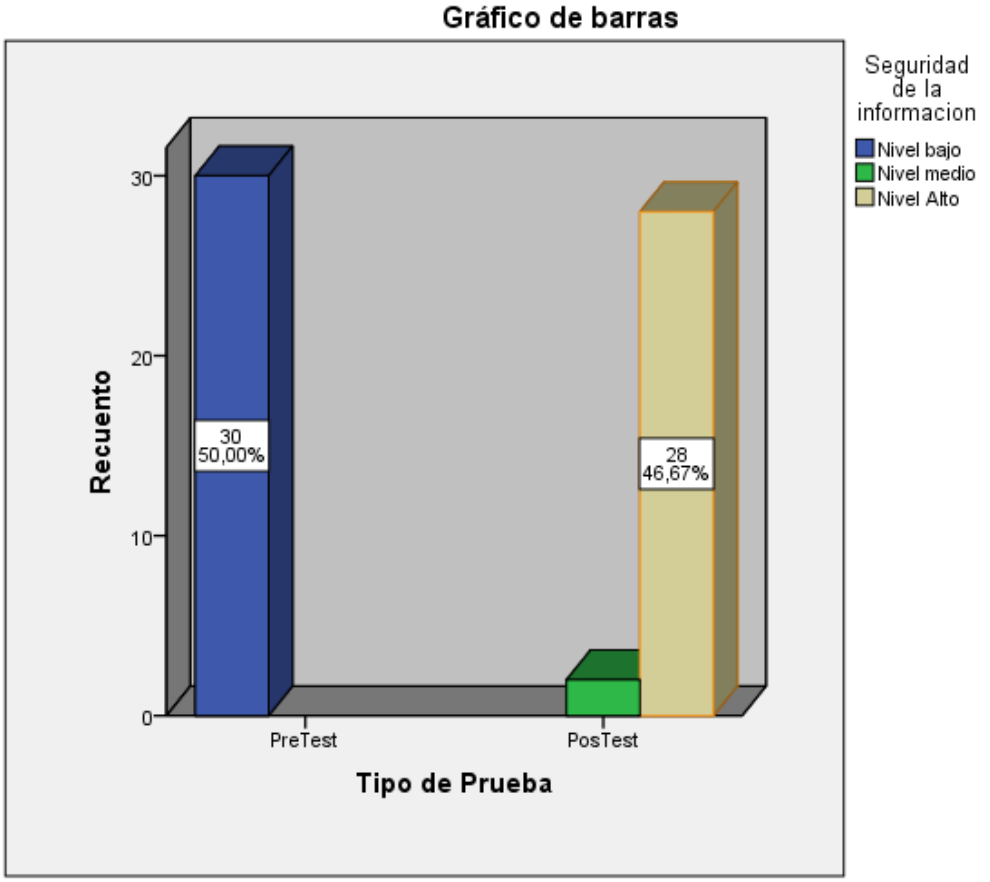


Ilustración 3. Gráfico de barras
Fuente: Elaboración por cuenta propia con el software SPSS

c) Prueba de la normalidad

La prueba se realiza tomando en consideración el método “Shapiro-Wilk”, ya que la muestra se conforma por 30 especialistas de seguridad de datos e información de los OBAC y de la ACFFAA donde abarca los indicadores de confidencialidad, integridad y disponibilidad de la información.

Si:
Significancia < 0.05 adopta una distribución no normal
Significancia >= 0.05 adopta una distribución normal
Donde la significancia es el nivel crítico del contraste

H0: Los datos provienen de una distribución normal

H1: Los datos no provienen de una distribución normal

Nivel de significancia: 0.05

Criterio de prueba: Sig < 0.05, donde se rechaza la H0. Sig > 0.05, se acepta la H0

Tabla 5. Prueba de Normalidad de Shapiro-Wilk

	Shapiro-Wilk			Criterio
	Estadístico	gl	Sig.	Sig<0.05
pre_total	,948	30	,154	"Normal"
pre_d1	,906	30	,012	"No normal"
pre_d2	,896	30	,007	"No normal"
pre_d3	,910	30	,015	"No normal"
post_total	,861	30	,001	"No normal"
post_d1	,814	30	,000	"No normal"
post_d2	,866	30	,001	"No normal"
post_d3	,722	30	,000	"No normal"

Fuente: Elaboración por cuenta propia con el software SPSS

Considerando que el nivel de Sig. = 0,000 < 0.05, se va a rechazar la H0, concluyendo que los datos no son provenientes de una distribución netamente normal, en las variables y dimensiones. Por lo tanto, considerando que son distribuciones no normales, se utilizaran procedimientos enfocados en la estadística no paramétrica.

d) Contrastación de (hipótesis general)

Se establecen las siguientes hipótesis:

H0: El implementar Redes Privadas Virtuales no tiene un impacto muy relevante en la administración de seguridad de datos e información del sistema de catalogación perteneciente a la Agencia de Compras de las FFAA.

H1: El implementar Redes Privadas Virtuales tiene un impacto muy relevante en la administración de seguridad de datos e información del sistema de catalogación perteneciente a la Agencia de Compras de las FFAA.

Nivel de Sig.: 0.05

Criterio de la prueba: Significancia < 0.05 lo cual hace que se rechace H0, de otro modo, se tiene que aceptar.

Tabla 6.Prueba de las muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior			
Par 1	Seguridad de la Información (Pretest) - Seguridad de la Información (Postest)	-1,93333	,25371	,04632	-2,02807	-1,83860	-41,738	29	,000

SFuente: Elaboración por cuenta propia con el software SPSS

De acuerdo a la prueba de T para muestras relacionadas, para la comparación de las muestras similares, se obtuvo un Sig = 0.000 < 0.05, por lo tanto, la prueba es significativa, y se llega a la conclusión que, al implementar las Redes Privadas Virtuales, estas tienen un impacto muy relevante en la administración de seguridad de datos e información del sistema de catalogación perteneciente a la Institución encargada de las compras del sector defensa de las FFAA.

e) Contrastación de la hipótesis especificas

Prueba de hipótesis especificas 1

H0: El implementar Redes Privadas Virtuales NO tiene un impacto muy relevante en la administración de Confidencialidad de la información del sistema de catalogación perteneciente a la Agencia de Compras de las FFAA.

H1: El implementar Redes Privadas Virtuales tiene un impacto muy relevante en la administración de Confidencialidad de la información del sistema de catalogación perteneciente a la Agencia de Compras de las FFAA.

Nivel de Sig.: 0.05

Criterio de la prueba: Significancia < 0.05 lo cual hace que se rechace H0, de otro modo, se tiene que aceptar.

Tabla 7.Estadísticos de prueba[a]

	Confidencialidad de la Información (Pos test) - Confidencialidad de la información (Pre test)
Z	-5,231[b]
Sig. asintótica (bilateral)	,000

Fuente: Elaboración por cuenta propia con el software SPSS

De acuerdo a la prueba de rangos de Wilcoxon, para la comparación de las muestras, se obtuvo una significancia = 0.000 < 0.05, por lo tanto, se confirma que la prueba es significativa, y se llega a la conclusión que, al implementar las Redes Privadas Virtuales, estas tienen un impacto muy relevante en la gestión de Confidencialidad de la información del sistema de catalogación perteneciente a la Institución encargada de las compras del sector defensa de las FFAA.

Prueba de hipótesis especificas 2

H0: El implementar Redes Privadas Virtuales NO tiene un impacto muy relevante en la administración de Integridad de la información del sistema de catalogación perteneciente a la Institución encargada de las compras del sector defensa de las FFAA.

H1: El implementar Redes Privadas Virtuales tiene un impacto muy relevante en la administración de Integridad de datos e información del sistema de catalogación perteneciente a la Institución encargada de las compras del sector defensa de las FFAA.

Nivel significación: 0.05

Criterio de la prueba: Significancia < 0.05 lo cual hace que se rechace H0, de otro modo, se tiene que aceptar.

Tabla 8.Estadísticos de prueba[a]

	Integridad de la Información (Pos test) - Integridad de la Información (Pretest)
Z	-5,152[b]
Sig. asintótica (bilateral)	,000

Fuente: Elaboración por cuenta propia con el software SPSS

De acuerdo a la prueba de rangos de Wilcoxon, para la comparación de las muestras, se obtuvo un Sig = 0.000 < 0.05, por lo tanto, la prueba es muy significativa, y se llega a la conclusión que, al implementar las Redes Privadas

Virtuales, estas tienen un impacto muy relevante en la gestión de Integridad de datos e información del sistema de catalogación perteneciente a la Institución encargada de las compras del sector defensa de las FFAA.

Prueba de hipótesis especificas 3

H0: El implementar Redes Privadas Virtuales NO tiene un impacto muy relevante en la gestión de Disponibilidad de la información del sistema de catalogación perteneciente a la Institución encargada de las compras del sector defensa de las FFAA.

H1: El implementar Redes Privadas Virtuales tiene un impacto muy relevante en la gestión de Disponibilidad de datos e información del sistema de catalogación perteneciente a la Institución encargada de las compras del sector defensa de las FFAA.

Nivel significación: 0.05

Criterio de la prueba: Significancia < 0.05 lo cual hace que se rechace H0, de otro modo, se tiene que aceptar.

Tabla 9.Estadísticos de prueba[a]

	Disponibilidad de la Información (Pos test) - Disponibilidad de la Información (Pre test)
Z	-5,303[b]
Sig. asintótica (bilateral)	,000

Fuente: Elaboración por cuenta propia con el software SPSS

De acuerdo a la prueba de rangos de Wilcoxon, para la comparación de las muestras, se obtuvo un Sig = 0.000 < 0.05, por lo tanto, la prueba es significativa, y se concluye que, al implementar las Redes Privadas Virtuales, estas tienen un impacto muy relevante en la administración de Disponibilidad de la información en la Institución encargada de las compras del sector defensa de las FFAA.

Discusión

En base a nuestros resultados llegamos a determinar el cumplimiento de nuestro objetivo general el cual fue planteado para implementar las Redes Privadas Virtuales que permita gestionar la seguridad de datos e información, dando por cumplimiento a nuestra hipótesis general que al implementarse las Redes Privadas Virtuales entonces estas tienen un impacto muy relevante al gestionar la seguridad de datos e información, este resultado comparado con la investigación de (León, 2018) indica que el Monitoreo para el rendimiento de la seguridad de VPN ofrece ventajas significativas para atender la necesidad actual de seguridad de datos e información empresarial. Con quien concordamos y validamos los mismos resultados, aunque en escenarios distintos. Como también concordamos con los autores (Hajrizi, Bajraliu, Qehaja, & Shabani, 2016), quienes determinaron nuevos métodos donde "las redes privadas virtuales Dinámica Multipunto (DMVPN)", destacan las buenas prácticas que debe implementar la organización dar garantía de una alta seguridad en las diversas comunicaciones y la información que manejan.

En referencia a nuestra hipótesis especifica 1, Al Implementar Redes Privadas Virtuales, estas tienen un impacto muy relevante al gestionar la confidencialidad de datos e información la cual ha sido comprobada estadísticamente, en comparativa con (Seclén, 2016), quien nos menciona de los factores pueden afectar el proceso para implementar el sistema de administración de seguridad de datos e información en las instituciones del sector público peruano de acuerdo a la "NTP-ISO/IEC 27001" con quien estamos de acuerdo porque identifica como objetivo dichos factores, resaltando la confidencialidad de la información como parte de sus resultados.

En referencia a nuestra hipótesis especifica 2 Al Implementar Redes Privadas Virtuales, estas tienen un impacto muy relevante al gestionar de la Integridad de datos e información la cual ha sido comprobado estadísticamente, en comparativa con (Tacza, 2018) quien nos menciona el objetivo busca entender con claridad que aspectos de seguridad de datos e información propone hacer cumplir el plan de seguridad con referencia a la norma ISO 27001:2005 y lo que demanda como necesidad de las entidades públicas del estado peruano para poder implementar y garantizar la seguridad estando de acuerdo con sus resultados ya que están orientadas al establecimiento de buenas prácticas en relación con la implementación referidas en nuestro trabajo de investigación.

En referencia a nuestra hipótesis especifica 3 Al Implementar Redes Privadas Virtuales, estas tienen un impacto muy relevante al gestionar la disponibilidad de datos e información la cual ha sido comprobado estadísticamente, en comparativa con (Usca, 2018) quien nos da a conocer como objetivo la posibilidad realizar la evaluación del rendimiento efectivo del protocolo MPLS / VPN utilizando la aplicación de una VPN, y ver como esta influye en el sistema de transmisión de datos, se hizo una comparativa cuantitativa de la red lo que permito un ahorro de recursos, con lo cual estamos muy de acuerdo con sus resultados adicionando que la red se encuentra disponible, confiable y segura en al realizar la transmisión de datos.

Conclusiones

Se realizó la implementación de las Redes VPN permitiendo gestionar de manera adecuada la seguridad de la información de Catalogación en la ACFFAA, permitirá manipular la información de los activos militares que conciernen a la seguridad de la defensa nacional del país y de otros países que conforman este sistema, y según la percepción de los especialistas del área de seguridad de la información de las FF.AA. confirman que la seguridad, está en un nivel alto con 46.7% después de nuestra implementación.

Se implementaron las Redes VPN para la gestión de la confidencialidad de la información de Catalogación en la ACFFAA, lo que garantizó que la información del SICAD sea accesible de forma única a las personas autorizadas para que no sea divulgada. Recordando que no es el carácter de público o privado lo que se pone en riesgo sino el uso que se hace de ellos.

La implementación desarrollada de las Redes VPN para la gestión de la integridad de la información de Catalogación en la ACFFAA, mejoró la performance de la integridad del paquete de datos del SICAD, ya que los paquetes llegan más rápido a su destino.

Se implementó las Redes VPN para la gestión de la disponibilidad de la información de Catalogación en la ACFFAA, lo que garantizó la disponibilidad en todo momento, evitando interrupciones del servicio del SICAD el cual puede provocar pérdidas considerables a la Institución, para la toma de decisiones.

Referencias bibliográficas

ACFFAA. (23 de 09 de 2019). *www.gob.pe/acffaa*. Obtenido de https://www.gob.pe/ru/institucion/acffaa/noticias/187821-agencia-de-compras-de-las-fuerzas-armadas-adquiere-herramienta-que-permitir-implementar-sistema-otan-de-catalogaci-n

ACFFAA. (23 de 09 de 2019). *www.gob.pe/institucion/acfffaa*. Obtenido de https://www.gob.pe/ru/institucion/acffaa/noticias/187821-agencia-de-compras-de-las-fuerzas-armadas-adquiere-herramienta-que-permitir-implementar-sistema-otan-de-catalogaci-n

ACFFAA. (23 de 09 de 2019). *www.gob.pe/institucion/acfffaa*. Obtenido de https://www.gob.pe/ru/institucion/acffaa/noticias/187821-agencia-de-compras-de-las-fuerzas-armadas-adquiere-herramienta-que-permitir-implementar-sistema-otan-de-catalogaci-n

ACFFAA. (09 de 08 de 2021). *infodefensa.com.* Obtenido de https://www.infodefensa.com/texto-diario/mostrar/3110939/agencia-compras-peru-cataloga-bienes-militares-defensa

ACFFAA. (07 de 2021). *www.gob.pe/acffaa*. Obtenido de https://www.gob.pe/institucion/acffaa/normas-legales/2034536-040-2021-acffaa

Areitio, J. (2008). *Principios básicos de seguridad de la información.* Magallanes, España: In P. in Spain.

Arteaga , F., & Huamán, J. (2014). *Sistema de Consultoría On-line aplicando la Metodología PPDIOO para el proceso de Comercialización en la empresa Sabha Perú (Tesis para optar el título profesional de Ingeniero de Sistemas)*. Obtenido de http://repositorio.autonoma.edu.pe/handle/AUTONOMA/128.

Brown, S. (2008). *Implementación de Redes Privadas Virtuales (RPV).* Houston: McGraw-Hill Interamericana Editores.

Bruno, A., & Jordan, S. (2011). *CCDA Official Cert Guide. Indianapolis*. (C. Press, Ed.) Indianapolis, EE.UU: ISBN: 1-58714-257-0.

Chávez, N. (2007). *Introducción a la Investigación Educativa* (Tercera edición ed.). Maracaibo, Venezuela: La Columna. Recuperado el 28 de 09 de 2021

DaxNet, S.A. (1999). *Interconexión de redes virtuales privadas con tecnologías de Firewall. [En línea]*. Obtenido de Daxnet: http://daxnet.com/

Decreto Legislativo 1128. (07 de 12 de 2012). *Leyes Congreso*. Obtenido de https://www.leyes.congreso.gob.pe/Documentos/DecretosLegislativos/01128.pdf

Dierkens, T., & Rescorla, E. (2008). *RFC 5246: The Transport Layer Security (TLS) Protocol 1.2 RTFM.* Inc.

GDX - GROUP. (26 de 07 de 2019). *gdx-group.com*. Obtenido de https://gdx-group.com/cuando-es-necesario-cifrado-de-datos/

George, D., & Mallery , P. (2003). *SPSS for Windows step by step: A simple guide and reference* (11.0 update (4thed.) ed.). Boston, Estados Unidos: Allyn & Bacon.

Godoy, R. (2014). *Seguridad de Información.* Guatemala: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica.

Hajrizi, E., Bajraliu, A., Qehaja, B., & Shabani, A. (2016). Enterprise Integration, Networking and Virtual Communications. *IFAC-PapersOnLine, 49*, 144-147. doi:10.1016/j.ifacol.2016.11.090

Hernández, H., & Pascual Barrera, A. (2018). *VALIDACIÓN DE UN INSTRUMENTO DE INVESTIGACION PARA EL DISEÑO DE UNA METODOLOGÍA DE AUTOEVALUACIÓN DEL SISTEMA DE GESTIÓN AMBIENTAL.* Campeche, México. Obtenido de https://hemeroteca.unad.edu.co/index.php/riaa/article/view/2186

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodología de la Investigación* (Sexta Edición ed.). México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V. Recuperado el 26 de 09 de 2021

Hernández, R., Fernández, C., & Baptista, P. (2010). *Metodología de la Investigación* (5ta edición ed.). México: Mc Graw Hill.

infodefensa.com. (09 de 08 de 2021). *infodefensa.com*. Obtenido de https://www.infodefensa.com/latam/2021/08/09/noticia-aprueba-multianual-catalogacion-20212023.html

Information & Desing Solutions S.L. (25 de 09 de 2021). *infodefensa.com.* Obtenido de https://www.infodefensa.com/texto-diario/mostrar/3128632/peru-compra-herramienta-sicad-isdefe-implantar-catalogacion-otan

ISO. (27001). *(Organización Internacional de Estándares) Sistema de Gestión de Seguridad de Información (SGSI).* España. Obtenido de www.ISO27000.ES

ISO. (27001). *(Organización Internacional de Estándares) Sistema de Gestión de Seguridad de Información (SGSI).* España. Obtenido de www.ISO27000.es

Kerlinger, F., & Lee, H. (2002). *Investigación del comportamiento. Métodos de investigación en ciencias sociales.* México: McGraw-Hill.

León, A. (2018). Monitoreo de rendimiento para la seguridad de VPN a través de PfSense y OpenVPN. Veracruz, México. Recuperado el 19 de 09 de 2021, de https://cdigital.uv.mx/bitstream/handle/123456789/48648/LeonGomezAlejandro.pdf?sequence=1&isAllowed=y

Limari, V. (2004). *Tesis Protocolos de Seguridad para Redes.* Obtenido de http://cybertesis.uach.cl/tesis/uach/2004/bmfcil732p/sources/bmfcil732p.pdf

Mar, J. (2016). Propuesta de implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima – Cusco del INEI. Cusco, Perú.

MAZLAN, & RAHMAN, R. (2010). *Technical comparison analysis of encryption algorithm on Site-to-Site, IPSec VPN, Faculty of Electrical Engineering, Universiti Teknologi MARA.*

Mendoza, J. (2010). *PROPUESTA DE IMPLEMENTACIÓN DE UN ENTORNO DE VPN EMPRESARIAL EN LA EMPRESA ELECTRO ORIENTE S.A. SAN MARTIN.* Obtenido de http://repositorio.unsm.edu.pe/handle/11458/2796

Murillo, W. (2008). *La investigación científica*. Recuperado el 26 de 09 de 2021, de http//www.monografias.com/trabajos15/invest-científica/invest-científica.shtm

Niño, N. (2018). *MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI, PARA FORTALECER LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y MONITOREAR LOS ACTIVOS DE INFORMACIÓN PARA EL INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA - INEI FILIAL LAMBAYEQUE*. Lambayeque, Perú. Recuperado el 19 de 09 de 2021, de https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/5935/BC-TES-TMP-788%20NI%c3%91O%20MORANTE.pdf?sequence=1&isAllowed=y

Oppenheimer, P. (2011). *Top-Down Network Design* (Tercera edición ed., Vol. CiscoPress). Indianapolis, Estados Unidos: Cisco Ed.

Pedhazur, E., & Schmelkin, L. (1991). *Medición, diseño y análisis: un enfoque integrado.* Lawrence Erlbaum Associates, Inc. Recuperado el 27 de 09 de 2021

Piper, D. (1998). *«The Internet IP Security Domain of Interpretation for ISAKMP,».* Network Alchemy.

Quero Virla, M. (2010). *Confiabilidad y coeficiente Alpha de Cronbach.* (U. P. Chacín, Ed.) Maracaibo, Venezuela. Obtenido de https://www.redalyc.org/pdf/993/99315569010.pdf

Ramírez, L. (2018). *PROPUESTA PARA LA IMPLEMENTACIÓN DE UNA VPN.* Obtenido de https://repository.usta.edu.co/bitstream/handle/11634/14804/2019luisramirez.pdf?sequence=4&isAllowed=y

Rivera, J. (2016). *Fundamentos de redes informáticas* (Segunda ed.). España: IT Academy.

Rosero, J. (2021). *2021juanrosero.pdf*. Obtenido de https://repository.usta.edu.co/bitstream/handle/11634/33538/2021juanrosero.pdf?sequence=1

Seclén, J. (2016). Factores que afectan la implementación del sistema de gestión de seguridad de la información de las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001. Lima, Perú. Obtenido de https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/4884/Seclen_aj.pdf?sequence=1&isAllowed=y

Tacza, I. (2018). *Cumplimiento del Plan de Seguridad de la Información con relación a la Norma ISO 27000 en la Universidad Nacional Tecnológica de Lima Sur, año 2017*. Huánuco, Perú. Recuperado el 19 de 09 de 2021, de http://repositorio.unheval.edu.pe/bitstream/handle/UNHEVAL/2952/PTIC%2000007%20T12.pdf?sequence=1&isAllowed=y

Trujillo, E. (2006). *Diseño e implemantacion de una VPN en una empresa comercializadora utilizando IPSec.* Escuela Politecnica Naciona.

Usca, R. (02 de 2018). Evaluación del protocolo MPLS con la aplicación de VPN para mejorar el rendimiento del sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolivar. Chimborazo, Riobamba, Ecuador: Escuela Superior Politécnica de Chimborazo. Recuperado el 19 de 09 de 2021, de http://dspace.espoch.edu.ec/handle/123456789/8112

Velasquez , M., & Ronald, V. (2019). *Diseño de una red de comunicación VPN sobre internet para un distribuidor de claro basado en RFC 2764.* (F. d. ingenierías, Ed.) Universidad peruana de ciencas aplicadas .

Veron, J. (2010). *Prácticas de redes.* CERTEZA, España. Recuperado el 26 de 09 de 2021

Zapata Rodríguez, M., Pacheco Chiguano, F., De la Torre, E., & Vallejo Baldeón, M. (12 de 2017). Evaluación de Parámetros de QoS en una Red VPN-MPLS Diffserv bajo un Entorno Completo de Emulación de Software Libre. *Revista Científica y Tecnológica UPSE, IV*(3), 74-82. doi:https://doi.org/10.26423/rctu.v4i3.285

Anexos

1. Matriz de consistencia
2. Matriz de operacionalización
3. Instrumento
4. Base de datos
5. Evidencia del envió a la revista

Anexo 1: Matriz de consistencia

Problema general	Objetivo general	Hipótesis general	METODO
¿En qué medida la implementación de Redes VPN impacta en la gestión de Seguridad de la información de Catalogación en la ACFFAA?	Implementar Redes VPN para la gestión de Seguridad de la información de Catalogación en la ACFFAA.	La implementación de Redes VPN tiene un impacto estadísticamente significativo en la gestión de Seguridad de la información de Catalogación en la ACFFAA.	**Enfoque:** Cuantitativo **Método:** Transversal - Hipotético - Deductivo **Tipo:** Aplicada **Diseño:** Pre experimental **Población:** La población comprenderá a funcionarios y empleados de la Oficina de Informática de las siguientes instituciones castrenses: Ejército del Perú (EP), Marina de Guerra del Perú (MGP), Fuerza Aérea del Perú (FAP), Comando Conjunto de las FFAA (CCFFAA) y la Agencia de Compras de las Fuerzas Armadas (ACFFAA). **Muestra:** La muestra será igual al total de la población, es decir, comprenderá a las 30 personas especialistas en Seguridad de la Información que trabajan en las Oficinas de Informática de las Instituciones mencionadas en la población. **Técnica de procesamiento de datos**: **Técnica de recolección de datos**: Encuestas **Instrumento**: Cuestionario **Método de análisis de datos:** Software estadístico SPSS 27 Prueba T y Wilcoxon
Problemas Específicos	**Objetivos Especifico**	**Hipótesis Específicos**	
1. ¿En qué medida la implementación de Redes VPN impacta en la gestión de Confiabilidad de la información de Catalogación en la ACFFAA?	1. Implementar Redes VPN para la gestión de Confiabilidad de la información de Catalogación en la ACFFAA.	1. La implementación de Redes VPN tiene un impacto estadísticamente significativo en la gestión de Confiabilidad de la información de Catalogación en la ACFFAA.	
2. ¿En qué medida la implementación de Redes VPN impacta en la gestión de Integridad de la información de Catalogación en la ACFFAA?	2. Implementar Redes Privadas VPN para la gestión de Integridad de la información de Catalogación en la ACFFAA.	2. La implementación de Redes VPN tiene un impacto estadísticamente significativo en la gestión de Integridad de la información de Catalogación en la ACFFAA.	
3. ¿En qué medida la implementación de Redes VPN impacta en la gestión de Disponibilidad de la información de Catalogación en la ACFFAA?	3. Implementar Redes VPN para la gestión de Disponibilidad de la información de Catalogación en la ACFFAA.	3. La implementación de Redes VPN tiene un impacto estadísticamente significativo en la gestión de Disponibilidad de la información de Catalogación en la ACFFAA.	

Fuente: Elaboración propia

Anexo 2: Matriz de operacionalización

VARIABLES	DEFINICION	DIMENSION	INDICADOR	ITEM	ESCALA	INSTRUMENTO
Variable Independiente (X) Red Privada Virtual (VPN)	(Veron, 2010), define a la Red VPN como un enlace establecido por intermedio de internet de una red local a una red pública, los datos viajan encriptados y solo pueden ser entendidos por el origen y el destino.			Ítem 1 - 9	1. Nunca 2. Casi Nunca 3. A veces 4. Casi siempre 5. Siempre	Cuestionario de preguntas Pre-test (9) Post-test (9)
Variable Dependiente (Y) Seguridad de la información	Según (ISO, (Organización Internacional de Estándares) Sistema de Gestión de Seguridad de Información (SGSI), 27001), "consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización".	Confidencialidad de la información	○ Niveles de acceso ○ Equipos desechados			
		Integridad de la información	○ Políticas de integridad ○ Completitud ○ Conformidad ○ Consistencia			
		Disponibilidad de la información	○ Disponibilidad del servicio ○ Gestión de Riesgos ○ Continuidad del Negocio			

Fuente: Elaboración propia

Anexo 3: Ficha de cuestionario antes de la implementación de las Redes VPN (pre-test)

CUESTIONARIO

Siguiendo la siguiente escala valorativa marcar la numeración que corresponda a cada pregunta. "Pedimos ser honestos con sus respuestas por favor"

Entrevistado:

_____Cargo:_____

Escala Valorativa.

Nunca	Casi Nunca	A Veces	Casi Siempre	Siempre
1	2	3	4	5

Objetivo

A través de las siguientes preguntas contenidas en esta ficha de encuesta se busca recolectar datos cualitativos en cuanto a opiniones diversas (de acuerdo a la pregunta planteada) frente a la forma en que viene gestionando la información dentro de la Agencia de Compras de las Fuerzas Armadas (ACFFAA). Una respuesta consiente ayudara al investigador a realizar un mejor trabajo.

Instrucciones

Lea con mucho cuidado cada una de las preguntas planteadas y marque con una x dentro del recuadro de la opción que crea conveniente.

VARIABLE DEPENDIENTE: SEGURIDAD DE LA INFORMACIÓN					
INDICADORES DE ESTUDIO	ESCALA VALORATIVA				
• **Confidencialidad de la información**	**1**	**2**	**3**	**4**	**5**
1. Al estar disponible la información del SICAD en internet. La privacidad de la información está garantizada al 100%.	1	2	3	4	5
2. Considera usted que al utilizar SICAD por Internet, ¿la confiabilidad de los datos está asegurada?	1	2	3	4	5
3. ¿Comparte su computador o sus contraseñas del acceso al SICAD con otras personas de la Institución?	1	2	3	4	5
• **Integridad de la información**					
4. Al utilizar el SICAD por Internet, se siente seguro al momento de trasmitir información.	1	2	3	4	5

5. Como especialista de Seguridad de la Información de su Institución, ¿desconoce de los peligros que rondan por internet, en cuanto a garantizar la calidad e integridad de la información?	1	2	3	4	5
6. Su Institución utiliza sistemas de cifrado para acceder al SICAD, que garantice la entereza de la información.					
• **Disponibilidad de la información**					
7. ¿Los administradores de infraestructura de las redes de su Institución abordan oportunamente las incidencias presentadas cuando el SICAD no se encuentra disponible?	1	2	3	4	5
8. El acceso de la información al SICAD por Internet de manera rápida y oportuna, presenta altos niveles de dificultad por la forma en que se realiza.	1	2	3	4	5
9. En su Institución, ¿existen políticas de almacenamiento en servidores externos para garantizar la información del SICAD?	1	2	3	4	5

Anexo 4: Ficha de cuestionario después de la implementación de las Redes VPN

(post-test)

CUESTIONARIO

Siguiendo la siguiente escala valorativa marcar la numeración que corresponda a cada pregunta. "Pedimos ser honestos con sus respuestas por favor"

Entrevistado:

_____Cargo:_____

Escala Valorativa.

Nunca	Casi Nunca	A Veces	Casi Siempre	Siempre
1	2	3	4	5

Objetivo

A través de las siguientes preguntas contenidas en esta ficha de encuesta se busca recolectar datos cualitativos en cuanto a opiniones diversas (de acuerdo a la pregunta planteada) frente a la implementación de la red VPN dentro de la ACFFAA. Una respuesta consciente ayudará al investigador a realizar un mejor trabajo.

Instrucciones

Lea con mucho cuidado cada una de las preguntas planteadas y marque con una x dentro del recuadro de la opción que crea conveniente.

INDICADORES DE ESTUDIO	ESCALA VALORATIVA				
• **Confidencialidad de la información**	**1**	**2**	**3**	**4**	**5**
10. Las redes VPN implementadas entre la ACFFAA y los OBAC constituyen una solución fiable y segura para la transmisión de información del SICAD.	1	2	3	4	5
11. ¿Se siente seguro al momento de transferir información confidencial del SICAD a través de la Red Privada Virtual?	1	2	3	4	5
12. ¿Considera usted que las redes VPN implementadas contribuyen al aumento de la confidencialidad del SICAD?					
• **Integridad de la información**					
13. La Institución concentra los esfuerzos suficientes para garantizar la autenticidad, calidad e integridad de la información del SICAD.	1	2	3	4	5

14. La información del SICAD es encriptada y viaja por redes públicas a través de un túnel VPN. ¿Cree usted que los datos encriptados del SICAD aseguran la probidad de la información?	1	2	3	4	5
15. Los ataques informáticos a Redes VPN son frenados, al estar la información cifrada e inelegible a personas no autorizadas (hackers), asegurando la integridad de la información del SICAD.	1	2	3	4	5
• **Disponibilidad de la información**					
16. El acceso a la información SICAD mediante Redes VPN, ¿está disponible desde las redes registradas en el firewall de su Institución?	1	2	3	4	5
17. Los procedimientos para realizar copias y restauración de seguridad del SICAD que garantizan la recuperación de la información ante sucesos imprevistos. ¿Funcionan correctamente?	1	2	3	4	5
18. Los implementadores de las redes VPN abordan oportunamente las incidencias presentadas, restableciendo el servicio en el menor tiempo.	1	2	3	4	5

Anexo 5: Base de datos

Pre-test

1	1	1	1	3	1	1	2	1
2	1	2	1	1	1	2	1	2
2	2	2	1	1	3	2	2	2
2	1	2	1	1	1	1	2	1
2	1	2	3	2	2	3	1	3
2	3	2	2	1	2	3	2	3
1	1	1	1	1	1	3	2	2
3	3	3	1	1	3	1	3	2
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	2	1	2	1	1	2	1	2
2	2	2	1	2	2	2	2	2
1	1	1	3	1	1	1	1	1
1	2	1	1	2	2	2	3	2
2	2	2	2	2	1	1	2	1
1	1	1	1	1	1	2	2	2
2	2	2	3	2	3	1	2	1
2	3	2	2	1	1	2	2	2
2	2	1	1	2	1	2	1	1
2	2	2	2	2	2	1	2	2
2	1	2	2	2	2	3	2	2
1	2	1	3	2	1	1	2	1
2	2	2	2	1	2	2	1	2
3	2	2	2	2	1	1	2	1
2	1	2	3	2	2	1	1	1
1	2	3	2	1	1	2	2	2
1	2	1	2	3	2	2	3	1
2	1	2	2	2	1	1	1	2
1	1	1	1	1	1	1	1	1

Post-test

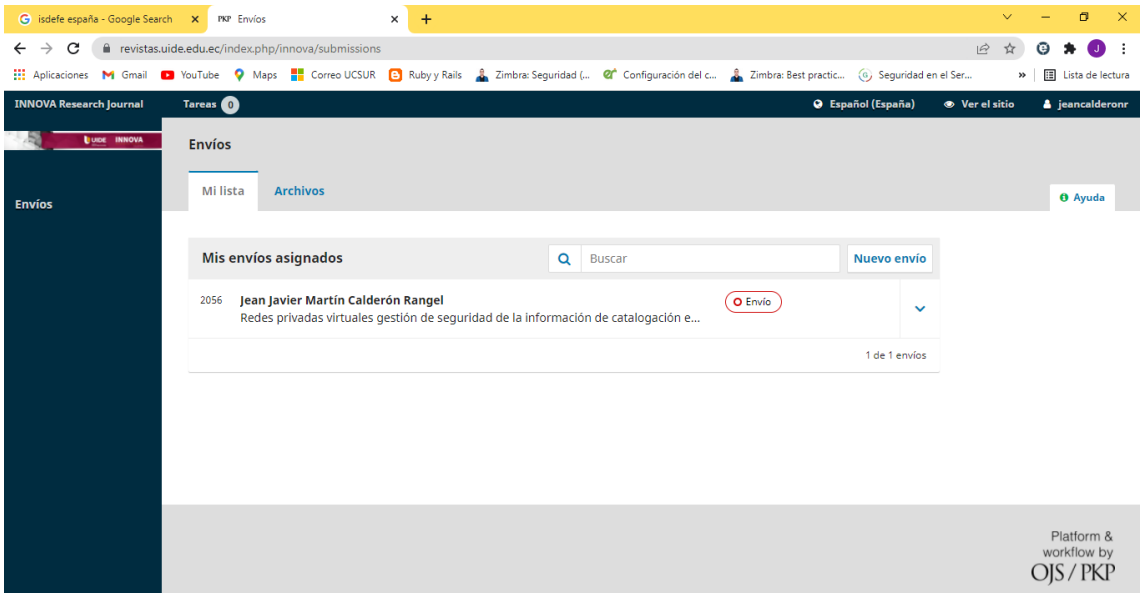
5	5	5	4	5	5	5	5	5
5	5	5	4	5	5	5	5	5
4	4	4	4	4	4	5	5	5
4	4	3	3	4	4	4	4	4
4	4	4	4	5	3	4	5	4
5	5	5	5	5	5	5	5	5
5	5	5	5	5	5	5	5	5
5	5	5	5	5	5	5	5	5
3	3	1	4	3	4	3	3	3
5	5	5	5	5	5	5	5	5
4	4	5	5	5	5	4	5	5
5	5	4	4	5	4	4	5	5
4	4	4	4	5	5	5	5	5
5	5	5	4	4	4	5	4	4
4	4	4	3	4	4	4	4	4
4	5	5	5	5	5	5	5	4
4	4	4	5	3	4	5	4	3
4	4	4	4	5	5	5	5	5
5	4	4	4	4	5	5	4	5
5	4	4	4	4	5	5	5	5
4	4	4	5	5	5	4	5	5
5	5	5	5	4	4	5	5	4
4	5	4	4	4	3	5	5	5
4	4	5	5	4	4	5	5	5
5	5	5	4	5	4	4	4	5
5	5	4	4	4	5	5	5	5
4	4	4	4	4	4	4	5	5
5	4	5	5	5	5	5	5	4
5	4	4	5	5	5	5	5	5
5	5	5	5	5	5	5	5	5

Anexo 6: Evidencia del envió a la revista

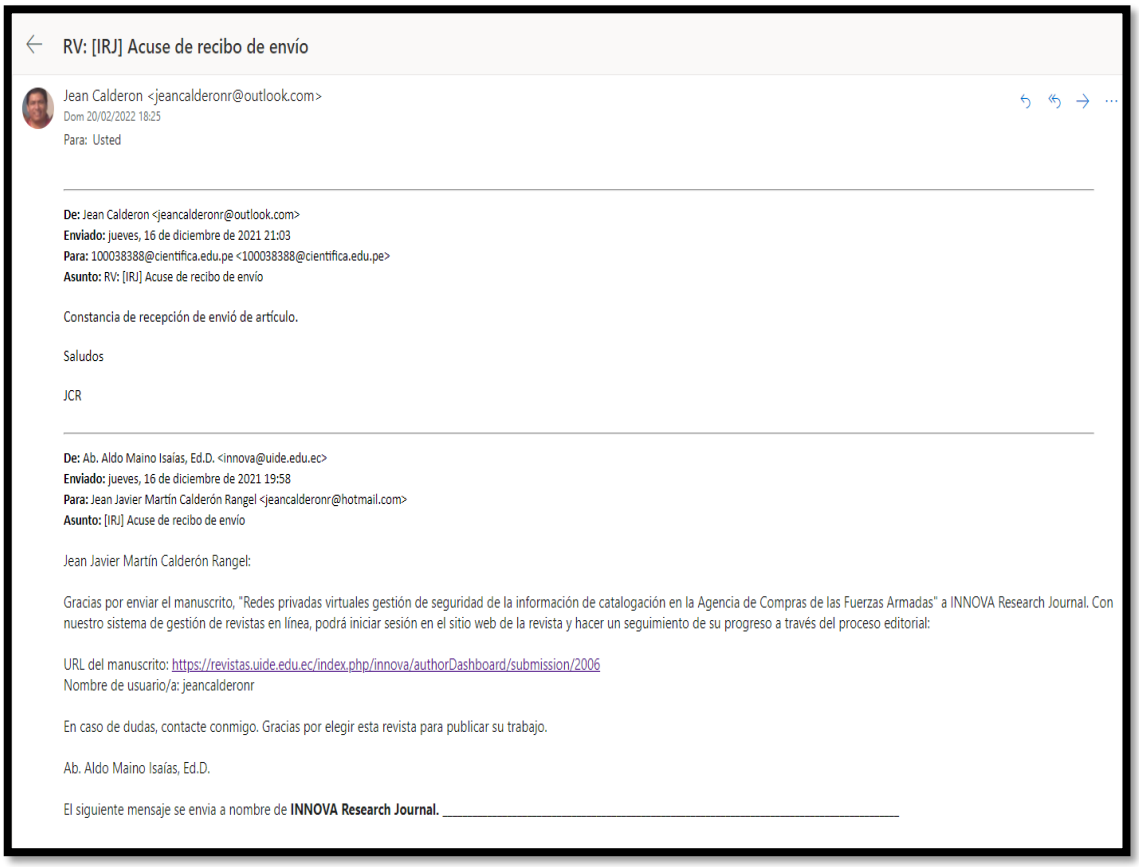
Datos técnicos de la Revista: Revista INNOVA RESERARCH JOURNAL ISSN: 2477-9024

Pantalla del sistema, indicando que él envió esta completado

Pantalla del sistema: registro del estado del articulo



Pantalla del correo donde indica la recepción del articulo



RV: [IRJ] Acuse de recibo de envío

Jean Calderon <jeancalderonr@outlook.com>
Dom 20/02/2022 18:25
Para: Usted

De: Jean Calderon <jeancalderonr@outlook.com>
Enviado: jueves, 16 de diciembre de 2021 21:03
Para: 100038388@cientifica.edu.pe <100038388@cientifica.edu.pe>
Asunto: RV: [IRJ] Acuse de recibo de envío

Constancia de recepción de envió de artículo.

Saludos

JCR

De: Ab. Aldo Maino Isaías, Ed.D. <innova@uide.edu.ec>
Enviado: jueves, 16 de diciembre de 2021 19:58
Para: Jean Javier Martín Calderón Rangel <jeancalderonr@hotmail.com>
Asunto: [IRJ] Acuse de recibo de envío

Jean Javier Martín Calderón Rangel:

Gracias por enviar el manuscrito, "Redes privadas virtuales gestión de seguridad de la información de catalogación en la Agencia de Compras de las Fuerzas Armadas" a INNOVA Research Journal. Con nuestro sistema de gestión de revistas en línea, podrá iniciar sesión en el sitio web de la revista y hacer un seguimiento de su progreso a través del proceso editorial:

URL del manuscrito: https://revistas.uide.edu.ec/index.php/innova/authorDashboard/submission/2006
Nombre de usuario/a: jeancalderonr

En caso de dudas, contacte conmigo. Gracias por elegir esta revista para publicar su trabajo.

Ab. Aldo Maino Isaías, Ed.D.

El siguiente mensaje se envia a nombre de **INNOVA Research Journal.** _____

Anexo 7: Implementación de la VPN en la ACFFAA

En el desarrollo de la presente investigación, a continuación, explicamos los procedimientos, como es la implementación de la red VPN, los temas relacionados con la toma de la muestra y el procedimiento de los datos, conforme a la figura 3.

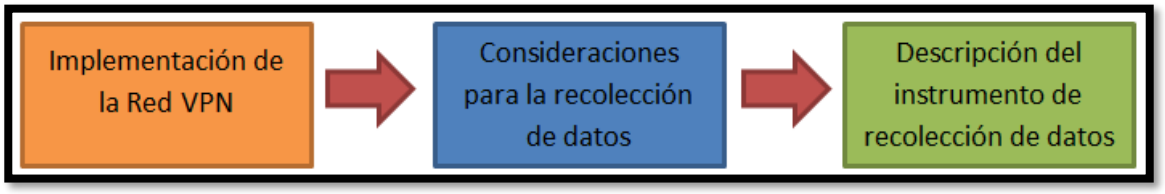


Ilustración 4. Redes diagrama de bloque de la metodología

Implementación de la red VPN

En el proceso de implementación de la red VPN, primero creamos el túnel con la opción: IPsec Tunnels, a continuación, se presenta imágenes que corresponden a la configuración de la red VPN:

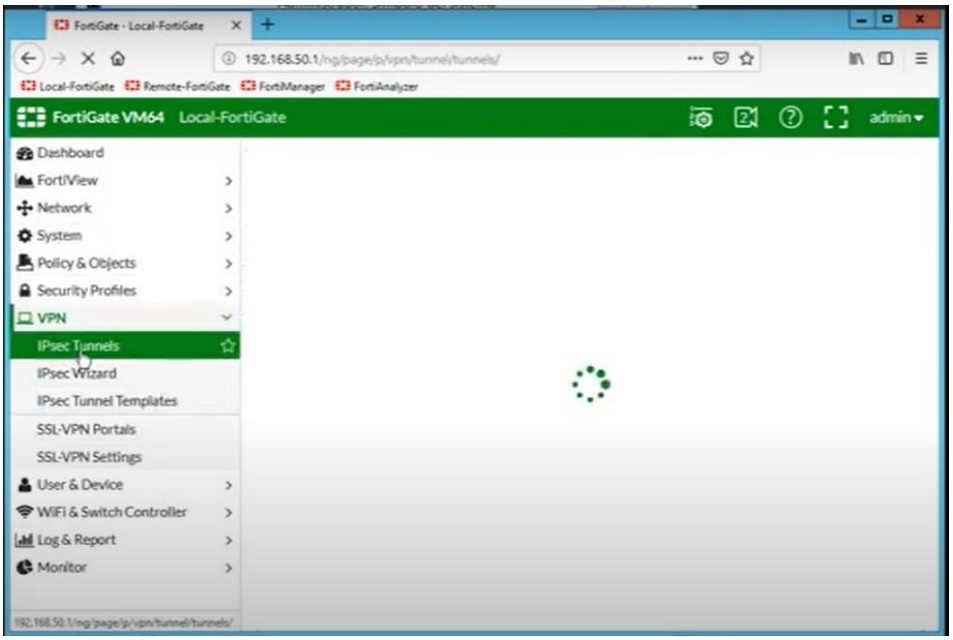


Ilustración 5. Pantalla inicial de la configuración de la VPN

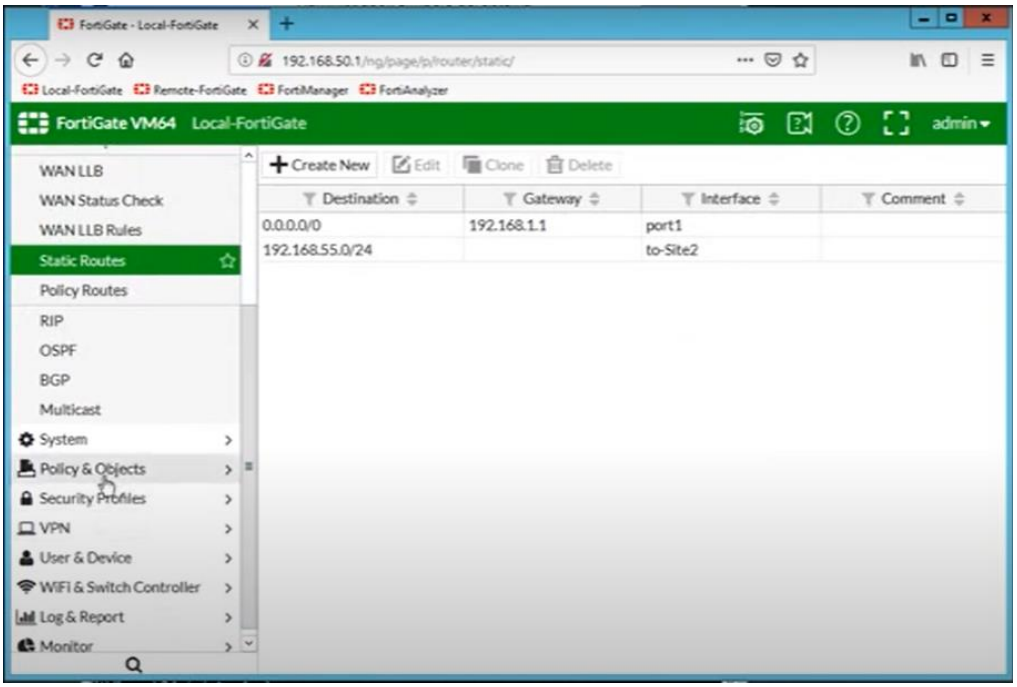


Ilustración 6. Pantalla donde se indica la creación del túnel

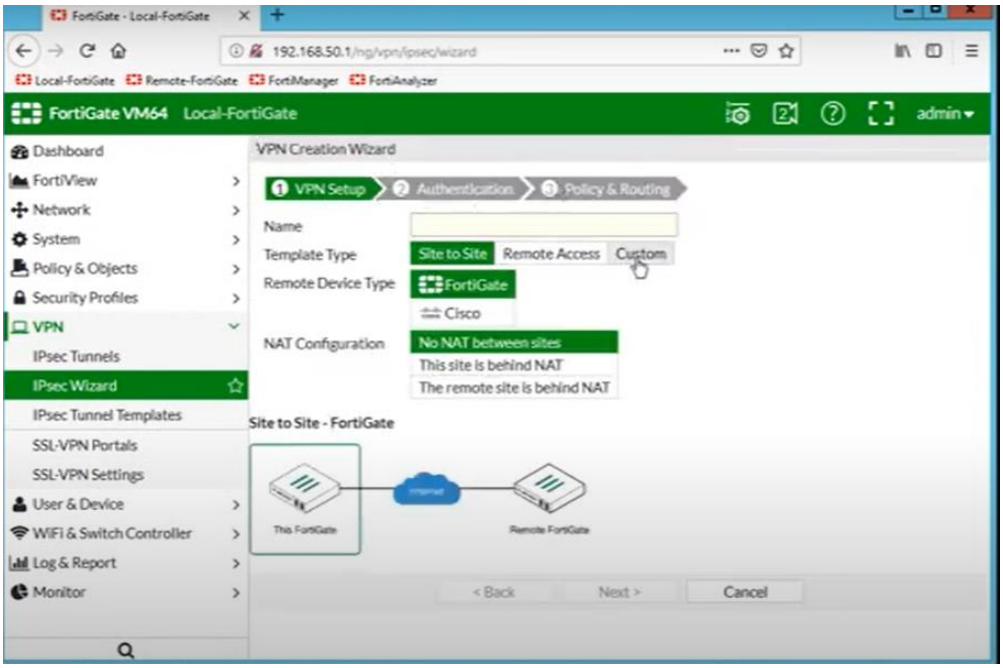


Ilustración 7. Pantalla donde se evidencia la configuración de la VPN

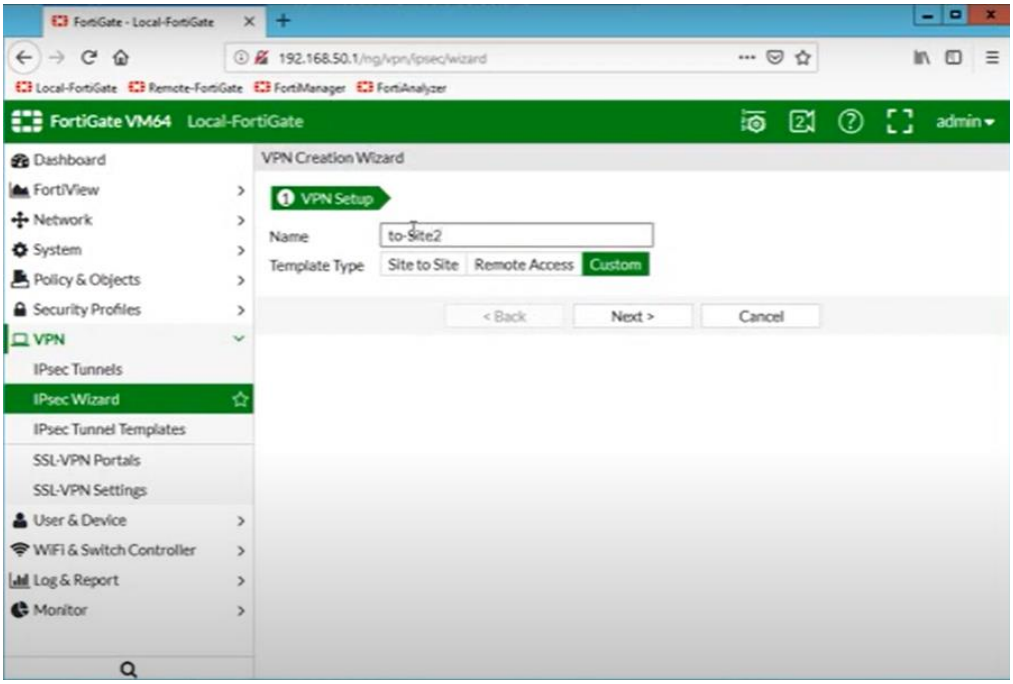


Ilustración 8. Pantalla donde se configura la IP del Gateway remoto

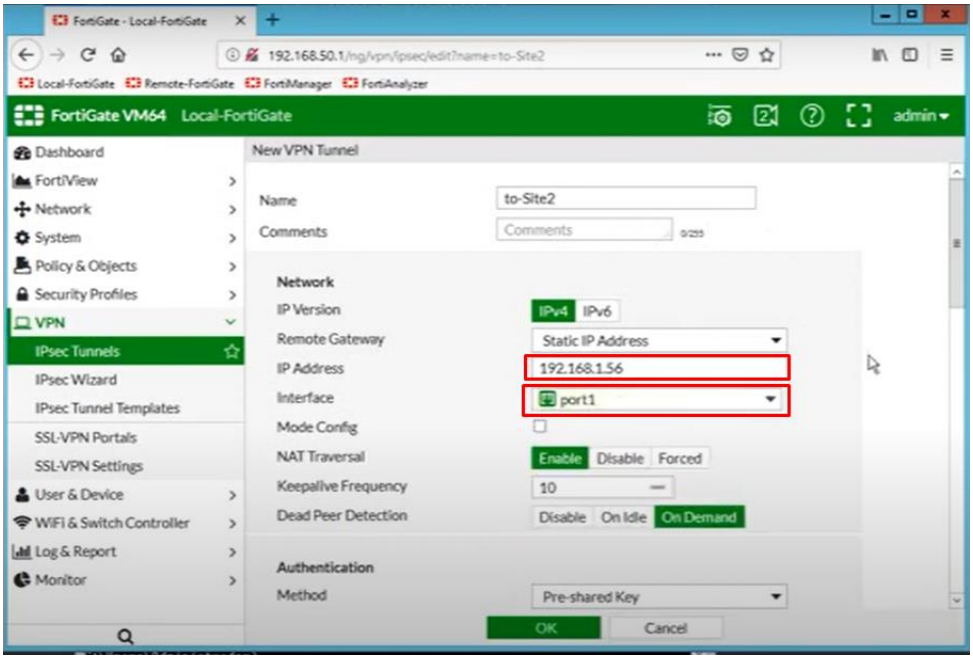


Ilustración 9. Pantalla donde se configura la interface por la que se conecta al Gateway (y se crea la VPN en modo interface) que te permite desarrollar varios escenarios VPN

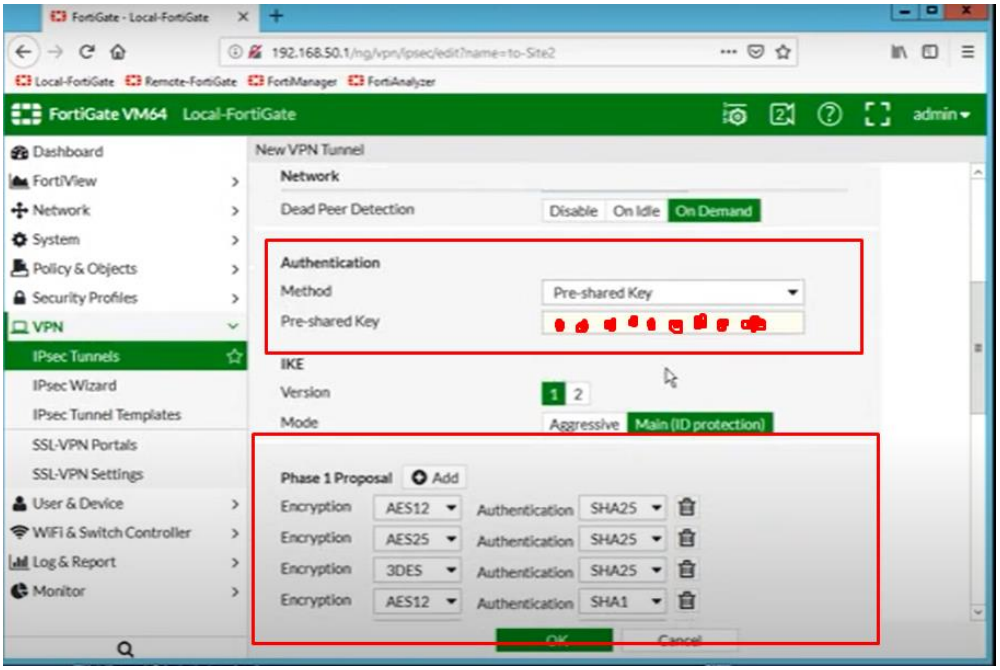


Ilustración 10. Pantalla donde se configura la IP del Gateway remoto

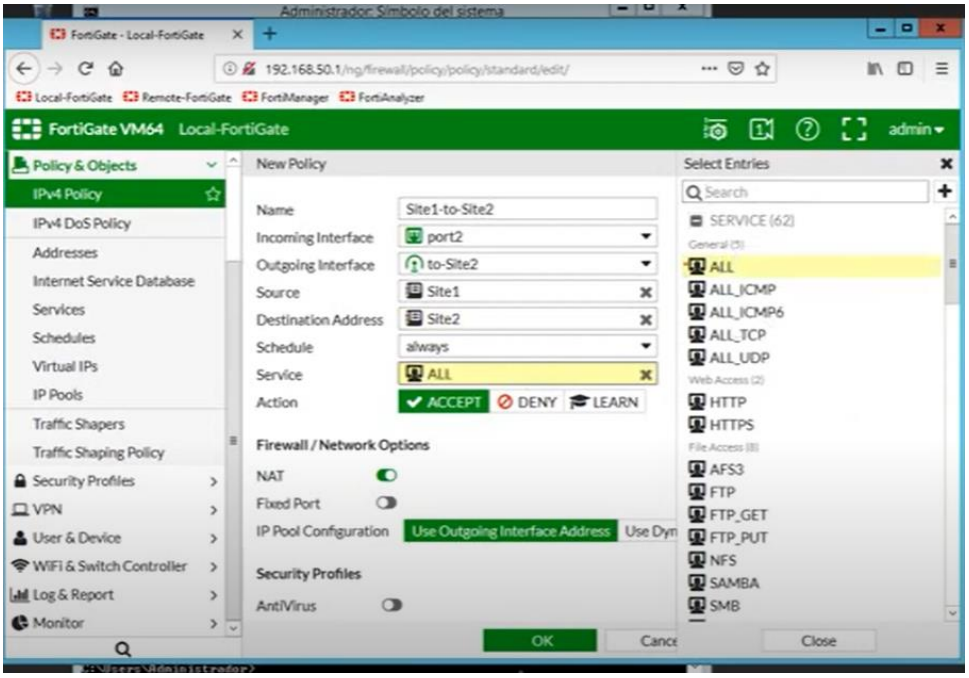


Ilustración 11. Pantalla de configuración de las políticas

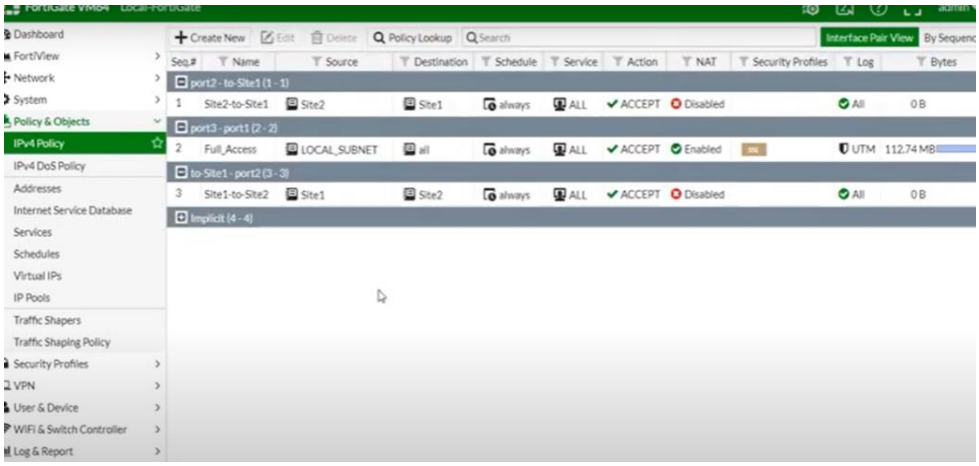


Ilustración 12. Pantalla donde se evidencia la configuración de las políticas

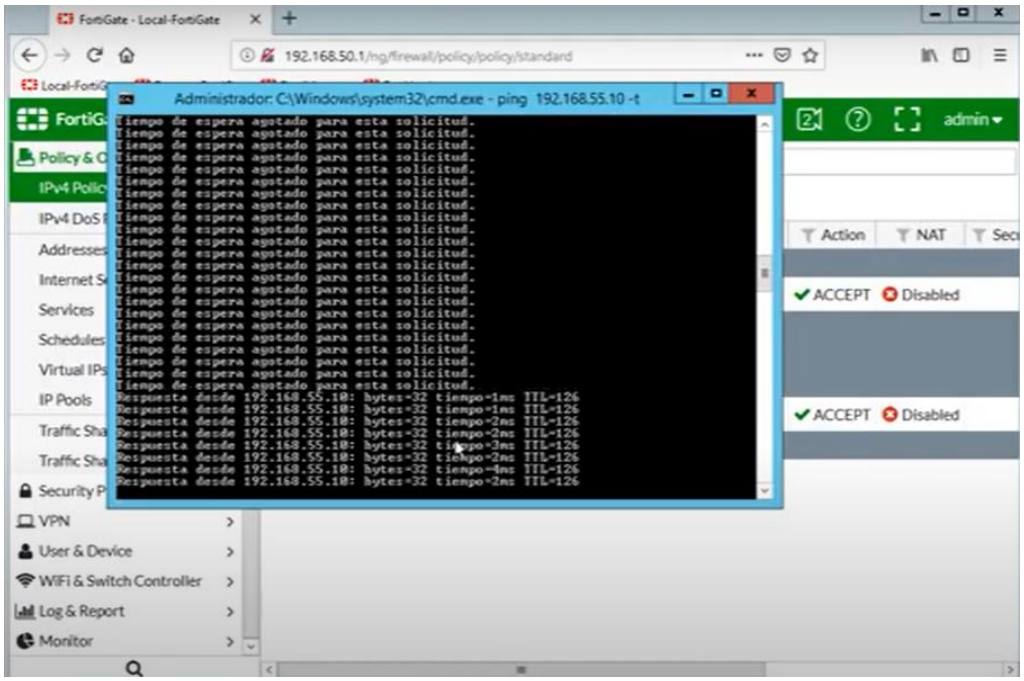


Ilustración 13. Pantalla de verificación que la VPN está en línea