UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO para la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
INGENIERO DE SISTEMAS

AUTOR :

Justiniano Tello, Eddie Armando Paul (ORCID:0000-0002-0808-5438)

ASESOR:

Dr. Gamboa Cruzado, Javier Arturo (ORCID:0000-0002-0461-4152)

LÍNEA DE INVESTIGACIÓN:

Infraestructura y Servicios de Redes y Comunicaciones

PIURA - PERÚ

2021

DEDICATORIA

A mis padres por el apoyo que me brindaron desde siempre, a mi esposa por ser mi centro de apoyo moral al llenarme de estabilidad emocional, a mi hijo JUSTINIANO REYES ETHAN MATEO por ser mi inspiración día a día.

AGRADECIMIENTO

Al Ing. Correa Calle, Teófilo Roberto por el apoyo constante en el asesoramiento como especialista y al Ing. Gamboa Cruzado, Javier Arturo por su asesoramiento metodológico que nos brindó semana tras semana de clases.

ÍNDICE DE CONTENIDOS

Índice de tablas

Índice de figuras e ilustraciones

Resumen

Ante el avance exponencial de la tecnología y el acceso de las organizaciones en Internet, ha originado la imperiosa necesidad de brindar mecanismos de seguridad para los usuarios tanto externos como internos de la red, con el fin de evitar que se exploten las vulnerabilidades de estas redes informáticas. En ese mismo sentido la realidad peruana no es ajena a ella, y se ven expuestas sus activos de información a intrusiones, ataques entre otros que bien podría reducirse mediante la implementación de sistemas de seguridad perimetral.

La actual investigación tiene como finalidad la implementación un sistema de seguridad perimetral, considerando el modelo SAFE de CISCO para mejorar la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A. Investigación de tipo aplicada y experimental puro, se tuvo un grupo control (Gc) y un grupo experimental (Ge), conformados por 30 procesos ejecutados en cada muestra.

En la investigación se demostró que se lograron mejoras significativas en los resultados del grupo experimental (Ge), con respecto al grupo de control (Gc), siendo de relevancia los indicadores de tiempo de ida y vuelta de 33.3 a 21.5 milisegundos, paquetes perdidos de 7.89 a 0.38 promedio por envío, número de intrusiones de 9.63 a 2.93 veces y el número de vulnerabilidades de 18.9 a 2.73, concluyendo que mediante la implementación de un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO mejora significativamente la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A.

Finalmente, se recomienda la utilización de herramientas de monitoreo certificadas para la medición constante de los indicadores de la infraestructura de red.

Palabras claves: Seguridad perimetral, Infraestructura de red, modelo SAFE, seguridad de la red y las comunicaciones

Abstract

Given the exponential advancement of technology and the access of organizations to the Internet, the urgent need to provide security mechanisms for both external and internal users of the network has originated, in order to prevent the vulnerabilities of these networks from being exploited. computer science. In the same sense, the Peruvian reality is not alien to it, and its information assets are exposed to intrusions, attacks among others that could well be reduced through the implementation of perimeter security systems.

The current research aims to implement a perimeter security system, considering the CISCO SAFE model to improve the management of the network and communications infrastructure in the company Agrofrutos Trading S.A. Research of applied and pure experimental type, there was a control group (Gc) and an experimental group (Ge), made up of 30 processes executed in each sample.

The research showed that significant improvements were achieved in the results of the experimental group (Ge), with respect to the control group (Gc), being of relevance the round trip time indicators of 33.3 to 21.5 milliseconds, lost packets of 7.89 to 0.38 average per shipment, number of intrusions from 9.63 to 2.93 times and the number of vulnerabilities from 18.9 to 2.73, concluding that by implementing a perimeter security system, based on CISCO's SAFE model, it significantly improves the management of the infrastructure of networks and communications in the company Agrofrutos Trading SA

Finally, the use of certified monitoring tools is recommended for the constant measurement of network infrastructure indicators.

Keywords: Perimeter security, Network infrastructure, SAFE model, network and communications security

I. INTRODUCCIÓN

I.I. REALIDAD PROBLEMÁTICA

Hoy en día en el mundo, ante los grandes cambios y masificación de la tecnología, ha suscitado la imperiosa necesidad de brindar seguridad en las redes informáticas, Tal es el caso de Ecuador, que, debido a la existencia de individuos inescrupulosos que, mediante el conocimiento de herramientas, aprovechan las vulnerabilidades de estas redes de computadoras, ocasionando múltiples perdidas en las empresas en forma reiterada, se implementó un sistema de seguridad perimetral, logrando con ello confianza para hacer uso de los recursos y servicios de red de la empresa (López Paredes, 2015).

La masificación de internet, ha contribuido en la comunicación global de todo el mundo y debido al continuo uso tanto en las empresas como a nivel personal, ha colocado en la palestra el termino de seguridad, pues debido a esto se han expuesto vulnerabilidades, que han sido aprovechados para realizar accesos no autorizados, no solo ataques externos sino también internos a la misma. Ante ello, en el contexto internacional, en Ecuador ante una amenaza inminente a la seguridad, y ante la incertidumbre si ya se accedió a información de la empresa, se implementó una solución perimetral, con la premisa que ante la vulnerabilidad se podría repercutir en la productividad de la empresa (Morales, y otros, 2020).

En este mismo contexto en Colombia, se considera en cuanto a la seguridad perimetral, consiste en proteger desde afuera, al sistema informático, es como un escudo de protección a los recursos tecnológicos que son vulnerables a diversos ataques como virus, troyanos, gusanos, ataques de fuerza bruta, denegación de servicio entre otros (Andres Bohorquez, y otros, 2017). En este mismo país, se concluye que estas amenazas latentes en Internet, ha generado diversas vertientes filosóficas de la protección de las empresas: a nivel de red y a nivel de contenidos. En cuanto a la primera la representan las intrusiones y ataques de hackers; respecto a la segunda, tenemos los gusanos, virus, phishing, spam, malware entre otros (Bolaños Botina, 2018).

En el Perú, las organizaciones de los diferentes rubros se interrelacionan de acuerdo a su giro de negocio, por ello las comunicaciones son una necesidad

básica tanto para los trabajadores como personal de los diferentes estamentos para sostener la continuidad de los servicios y poner a disposición información tanto para la operatividad como para las transacciones que en ella se realizan, por ello acceden a las redes tanto LAN como WAN, compartiendo información sensible con el soporte de los proveedores de comunicación, suscitando la necesidad de algún mecanismo de resguardo, en el transcurso de su transitabilidad entre los diferentes recursos tecnológicos para llegar a un destinatario (Castillo Palomino, y otros, 2017).

Agrofrutos Trading S.A, es una empresa que exporta mango, limón, palta y maracuyá; estos en diversas presentaciones tales como aceite, cáscara y jugo. En el interior está conformada por las áreas de mesa de partes, logística, administración, contabilidad y sistemas; la red está conformada por 04 Routers distribuida con internet de banda ancha, para 18 usuarios. Debido a la coyuntura del rubro de la empresa, en forma continua se pagan a proveedores, mediante transacciones financieras, asimismo se envían cotizaciones, facturas y otros documentos privados entre clientes y proveedores. Esto se ha multiplicado en la actualidad ante la coyuntura de pandemia, pues los usuarios de la red acceden diariamente, sin ningún tipo de control compartiendo información, convirtiéndose ante ello en un blanco vulnerable a disposición de los ataques de individuos u organizaciones criminales que mediante diferentes formas como pishing, ataques sql, fuerza bruta, ransomware y otros, puedan hacerse de información relevante y utilizarla para fines inescrupulosos (Delgado Zambrano, y otros, 2017).

En Agrofrutos Trading S.A, se evidencia acciones para la protección de la información, siendo estas más en forma reactiva, pues ante eventos de seguridad, solo se han limitado a realizar parches de seguridad en los servidores y actualización de antivirus para un número limitado de dispositivos, dejando expuestos otros por considerarse muchas veces un gasto más que una inversión, por tal no se manejan credenciales para los usuarios para el acceso a los recursos tecnológicos y servicios de red. Esta exposición de datos en forma recurrente podría generar en cualquier momento pérdidas económicas y de confianza tanto de los clientes y proveedores; por ello la seguridad de la data no debe considerarse un gasto, sino una inversión para la protección de estos.

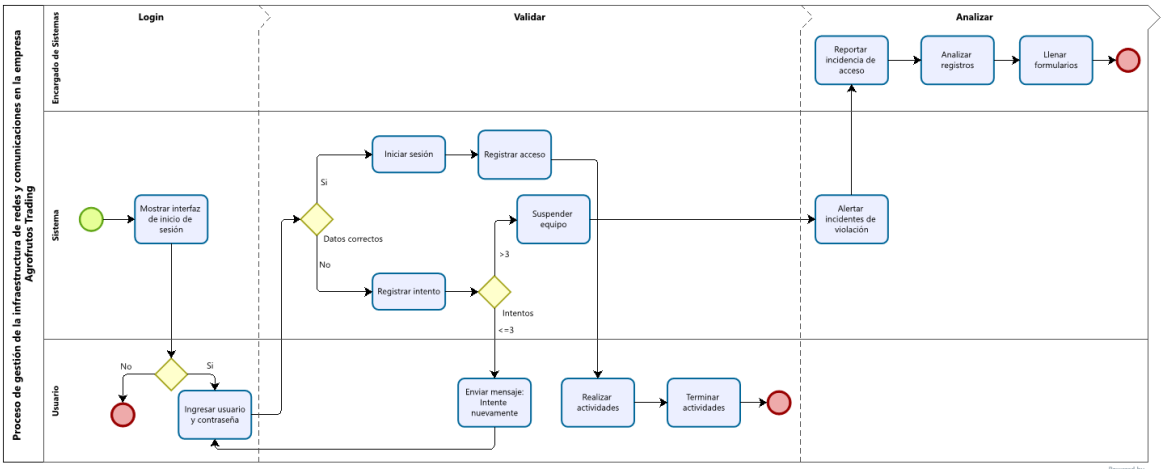

Figura 1. Proceso de gestión de accesos al sistema redes y comunicaciones en la empresa Agrofrutos Trading S.A

Por ello la gestión de la infraestructura de redes y comunicaciones de la empresa evidencia problemas en: Tiempo de ida y vuelta (Patterson, David A.; Hennessy, 2016), (Toapanta Viracocha, 2019), paquetes perdidos (Pilacuán Erazo, 2016), número de intrusiones (Toapanta Viracocha, 2019), (Ruiz Vieira, y otros, 2018) y número de vulnerabilidades (Calderón Diáz, y otros, 2019), (Toapanta Viracocha, 2019), (Da Silva De Oliveira, 2016).

Para solucionar estos problemas de seguridad existente, se plantea la implantación de un sistema de seguridad perimetral que brinde la protección adecuada de los datos no solo de la empresa sino además de clientes y proveedores.

Por lo tanto, el problema general de investigación es: ¿En qué medida la implementación de un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO mejora la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A.

Las preguntas específicas de investigación son: ¿En qué medida la implementación de un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO disminuye el tiempo de ida y vuelta en la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A.?, ¿De qué manera la implementación de un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO disminuye la perdida de paquetes en la gestión de la

infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A.?, ¿De qué manera la implementación de un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO disminuye el número de intrusiones en la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A.?, ¿De qué manera la implementación de un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO disminuye el número de vulnerabilidades en la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A.?

El objetivo general del estudio es Implementar un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO para la mejora de la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A., los objetivos específicos son disminuir el tiempo de ida y vuelta en la gestión de la infraestructura de redes, disminuir los paquetes perdidos en la gestión de la infraestructura de redes, disminuir el número de intrusiones en la gestión de la infraestructura de redes y disminuir el número de vulnerabilidades en la gestión de la infraestructura de redes.

La justificación metodológica de la investigación, se fundamenta con la utilización de un modelo metodológico fundamentado en CISCO, la misma que se basa en la contextualización de las fases en forma descendente o ascendente para su aplicabilidad en la infraestructura de la red para lograr una solución según la realidad de la empresa, esto conllevará a identificar políticas acordes a las vulnerabilidades encontradas con el objetivo de cubrir la brecha de seguridad, para ello se considera de referencia la norma ISO/IEC 27001 (Jarita, y otros, 2019). Asimismo es importante su implementación en la empresa, pues será un aporte relevante, en lo que respecta a la seguridad de sus datos, mediante el diseño de un perímetro para su protección tanto de su producción como los resultados de esta de acuerdo al rubro y disponer de confiabilidad en la red de comunicación de datos en beneficio de la empresa como de sus proveedores, los mismos que requieren de establecimiento de estándares de seguridad para el desarrollo de sus operaciones (Silva Ledesma, y otros, 2016). En lo tecnológico, su aplicabilidad se justifica, como una solución que conlleva a la gestión de los recursos tecnológicos existentes en la empresa, enfocándose en mecanismos que en conjunto logren

brindar soluciones de seguridad para minimizar las brechas existentes para evitar intrusiones maliciosas en la red de datos y comunicación.

Se plantea la presente hipótesis: Si se implementa un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO mejora de la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A. Y como hipótesis específicas: Si se implementa un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO disminuye el tiempo de ida y vuelta de la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A., si se implementa un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO disminuye la pérdida de paquetes en la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A., si se implementa un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO disminuye el número de intrusiones en la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A. y si se implementa un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO disminuye el número de vulnerabilidades en la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A.

II. MARCO TEÓRICO

En el presente estudio, se consideró investigaciones afines a las variables de estudio, realizadas por diferentes investigadores en un plano internacional y nacional, los cuales son el sustento de los indicadores para corroborar mediante resultados.

En lo que respecta a los antecedentes, en el ámbito internacional Bohorquez, y otros (2017), realizo la investigación referente al Diseño de un sistema de seguridad perimetral en las instalaciones del consorcio Expansión PTAR Salitre, el cual tiene como objetivo el planteamiento de un sistema de seguridad perimetral, considerando tipologías para proteger tanto la infraestructura lógica como física de la red en la institución. La investigación es de tipo descriptiva, nivel pre-experimental; como población se consideró a los empleados de la organización y como muestra toda la población. Plantea como resultados de la investigación la defensa de host, aplicación, red, así como la seguridad física y perimetral. Asimismo, en Colombia Camacho, y otros (2017), en su investigación acerca del diseño de un sistema perimetral en la empresa Américas Business Process Services, cuyo objetivo es diseñar un sistema de seguridad perimetral de la infraestructura de la empresa en mención, con el propósito de cubrir las brechas de seguridad existentes. La población consideró al personal de la institución, la muestra representativa fue de 1066. Como resultado de la investigación se propone 03 iniciativas, la primera opción es un sistema de seguridad basado en un Firewall Virtual, en segundo lugar, se tiene un firewall de capa 3, con funcionalidades de antispam, antivirus, con caracteristicas de desempeño de dedicacion y tercer lugar un Firewall modelo NextGen implementado con software de deteccion y prevencion de ataques, forzando politicas de seguridad para protocolos, puertos y a nivel de aplicaciones. Asimismo, en Ecuador Manosalvas y otros (2016) realizaron en su investigación acerca de la implantación de un sistema de seguridad perimetral en la granja de la UDLA, tuvo como objetivo la implementación de un sistema de seguridad perimetral. El estudio fue no experimental nivel descriptiva, los galpones y la granja 02 se consideraron como muestra. Se diseño un enlace entre los galpones y la casa principal de la granja, asimismo se adoptó normativas para el correcto uso del sistema que se encarga de monitorear las cámaras IP.

De igual manera, en el contexto nacional Toapanta (2019), en su investigación implementó un sistema de seguridad perimetral para asegurar la información de la contratación pública, siendo su propósito fue la implementación fue la virtualización de un sistema de seguridad para minimizar las brechas de seguridad en la institución. En cuanto a la población y muestra se consideró a los procesos de la infraestructura de la red. Como resultado las pruebas de comunicación entre las 02 redes, con el comando ping el tiempo de ida y vuelta fue de 2.5 milisegundos y el acceso a la VPN, fue mediante el cliente GlobalProtect. Además, para contrarrestar los ataques en tiempo real fluctúa entre 1 y 10 minutos, lo cual sin el sistema perimetral se realizaba entre 10 y 15 minutos, también el firewall paloalto networks, ofrece estabilidad proporcionando un alto rendimiento pues sin el sistema perimetral, la administración era muy lenta pues el CPU tenia un consumo de 100% lo que daba una baja protección. También, Calderón y otros (2019) implementaron un sistema de seguridad perimetral en la empresa JFC Electrical Engineering S.A.S., su propósito fue apoyarse en la ISO 27001 e ISO 27002 para la implementaron un sistema de seguridad perimetral en esta organización. La investigación fue descriptiva, no experimental; las redes de JFC Electrical Engineering S.A.S. formaron parte de la muestra de investigación. En los resultados según los hallazgos la implementación del firewall IPFIRE es 40% más económico que FORTIGATE, asimismo se estableció políticas en cuanto a seguridad física, lógica y acceso la red. Además, se logró disminuir el riesgo de navegar, así como el riesgo de ataques. Finalmente, en este contexto en la ciudad de Chiclayo, Ruiz y otros (2018), implementaron un sistema de seguridad perimetral Open Source en la Universidad Nacional Pedro Ruiz Gallo, se propuso como objetivo la mejora de la seguridad de los servicios de datos de la UNPRG. En cuanto a su finalidad se considera investigación aplicada y de diseño no experimental. Los 07 servicios de la red telemática, se consideraron como población, y en cuanto a los ataques la población se considera infinita. Entre los resultados, antes de implementar un firewall se tuvieron 78 accesos no autorizados exitosos y 74 intentos no fueron exitosos, en lo que respecta a los servicios la media fue de 104.5 accesos no autorizados exitosos; mientras que con la implementación del firewall 10 intentos fueron exitosos y 1 en los servicios respectivamente.

Así mismo, se describe la variable independiente que es Sistema de seguridad perimetral**,** se consideró la siguiente temática:

Según (Morales, y otros, 2020) la seguridad perimetral, está conformado por los recursos tecnológicos tales como móviles, laptops, computadoras de escritorio, servidores de la empresa. Para poder mitigar las amenazas es necesario la planificación para asegurar la continuidad del negocio. De igual manera Costas (2015) lo teoriza como una tecnología de coraza basada en un firewall, cuya finalidad es la protección de la red interna, de los ataques provenientes tanto de conexiones internas como de las provenientes de internet.

Según Costas Santos (2015), en cuanto a las amenazas, manifiesta que estas van dirigidas a programas de apoyo que, a las aplicaciones esenciales, y no es que no valgan la pena tales aplicaciones, pues muchas de ellas poseen información reservada pero los atacantes dirigen sus esfuerzos al software de red y sistemas operativos, esto por el conocimiento que se tiene de las vulnerabilidades de estos y existe una diversidad de herramientas para la realización de una variedad de ataques y violaciones a la seguridad de la red. En estos según la frecuencia de ataques se tiene los browsers, servidores de archivos, web, servicios web, clientes de correo, protocolos SNMP; asimismo se realizan ataques a bases de datos como MySQL, Microsoft SQL Server, Oracle entre otras.

Según (Costas Santos, 2015), los virus de computadoras, son los tipos de programas malintencionado que nacieron con internet, estos suelen adjuntarse dentro de otros programas y cuya finalidad es destruir archivos y suelen reproducirse asimismo mediante copias de sí mismo. Los Worms, suelen ser de las mismas características de los virus, con la diferencia que estos no necesitan adjuntarse en otros archivos para reproducirse en redes de comunicaciones de datos, generalmente suelen explotar servicios de correo. Los troyanos son programas que parecen útiles, pues se presentan como inofensivos, pero internamente el programador malintencionado coloca una serie de sentencias como para eliminar archivos, corromper datos, capturar información del usuario y utilizar recursos de procesamiento del dispositivo infectado, tales como envíos de correos de spam, ataques de DOS o phishing.

Asimismo, para describir la variable dependiente de la investigación Gestión de Infraestructura de redes y comunicaciones, se tomó en cuenta los siguientes conceptos:

Según Gómez Vieites (2015) la infraestructura de red, tiene como propósito ser el soporte para la empresa, siendo flexible para brindar satisfacción a los clientes cubriendo sus necesidades, facilitando los flujos de información mediante mecanismos, políticas y procedimientos que faciliten esta tarea. Para el cumplimiento de estas consideraciones, se debe tener características como disponibilidad, eficiencia, funcionalidad, capacidad de administración, rendimiento y escalabilidad. La disponibilidad, consiste en poseer acceso a los recursos, considerando redundancia para que las aplicaciones críticas accedan a estos en cualquier circunstancia; la eficiencia, considerando equipos con alta performance y software idóneo para asegurar un óptimo rendimiento; capacidad de administración, mediante la inclusión de tecnologías emergentes que optimicen el control de la red; rendimiento, mediante el uso de sistemas operativos de red actualizados y configurados adecuadamente, soportado por hardware escalable que asegure la continuidad del servicio y escalabilidad, para lograr un crecimiento sostenido alineados con los objetivos trazados por la organización.

Para el presente estudio se consideró 04 indicadores como son: Tiempo de ida y vuelta, perdida de paquetes, número de intrusiones, numero de vulnerabilidades, de los cuales se consideró las siguientes conceptualizaciones:

El Tiempo de ida y vuelta, según Johnny, y otros (2018), se considera el tiempo que demora un paquete de datos que es enviado desde el host emisor, llegar al host receptor y volver al host que envío el paquete.

Tiempo de ida y vuelta = (Total de todos los tiempos de ida y vuelta / cantidad de solicitudes de envío)

Según Johnny, y otros (2018), perdida de paquetes, es la perdida de datos al ser enviados desde el host emisor(origen) hasta llegar al host receptor(destino); es decir no se recibe la información completa.

Perdida de paquetes = (Total de paquetes enviados - Total de paquetes recibidos

Según Carcelén Méndez, y otros (2017), Número de intrusiones, son los accesos no autorizados con la intención de acceder a los recursos informáticos de una red para modificar la integridad de la información. Estos ataques pueden ser activos o pasivos según la gravedad y las consecuencias de los mismos.

Según Ariganelo (2016), Número de vulnerabilidades, son las características de debilidad de una red de datos, la misma que estando expuesta es pasible de amenazas, tanto en forma accidental como intencional, permitiendo que se pueda acceder a información de acceso privado, debido a que la red presenta puntos críticos débiles.

Asimismo, en lo concerniente a la variable interviniente modelo SAFE de Cisco, se tomó en cuenta estos conceptos:

Según Cisco (2019), SAFE de CISCO, es un modelo de seguridad de redes que brinda una gama de mejores prácticas, para diseñar e implementar redes seguras, siendo una guía para los interesados, lo cual permite seleccionar productos de seguridad, centrándose en las amenazas existentes y los medios que podemos disponer para enfrentarlas. Se describe las siguientes fases:

Planear: Consiste en identificar en forma sistemática las amenazas existentes en los activos de comunicación de la empresa, y evaluar los riesgos relacionados al uso de estos

Diseñar: Es el proceso de seleccionar y diseño de las plataformas existentes, adoptando las buenas prácticas de seguridad, con el propósito de cerrar las brechas existentes, minimizando el riesgo con el fin de lograr la satisfacción en el uso de los recursos de la red

Implementar: Consiste en desplegar en forma separada de la plataforma para abordar capacidades de seguridad en forma secuencial

Operar: Es el proceso de monitoreo de la infraestructura que se ha implementado con el propósito de minimizar el riesgo

Optimizar: Consiste en identificar posibles brechas de seguridad y evaluar en forma constante su potencial riesgo en el uso de los recursos de la red

III. METODOLOGÍA

3.1. Tipo y diseño de la investigación

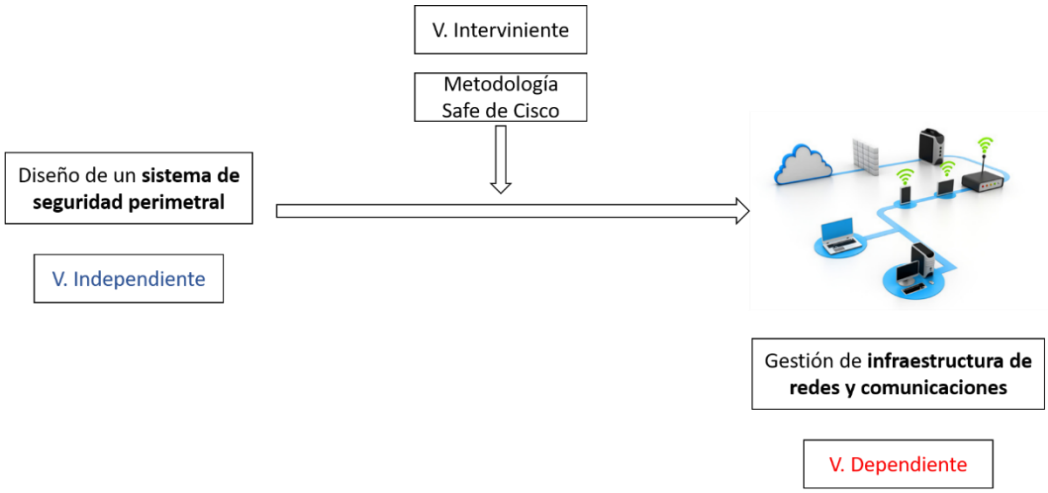

Figura 1. Tipo de investigación

Como se visualiza en la Figura 2, el estudio es de diseño experimental del tipo experimental verdadero, debido a que se manejó la variable independiente (Sistema de seguridad perimetral), basándose en ella para evaluar el impacto sobre la variable dependiente (Gestión de infraestructura de redes y comunicaciones), y se determinó el criterio de éxito.

Tipo de investigación: Aplicada

Diseño de investigación: Experimental Puro

RG_e X O_1

RG_c -- O_2

Donde:

R= Asignación aleatoria. Los sujetos del estudio fueron asignados al azar a un determinado grupo

Ge= Grupo experimental: Grupo de sujetos del estudio que se le aplicó el diseño del sistema de seguridad perimetral

Gc= Grupo control: Grupo de sujetos de estudio a los que no se le aplicó el diseño del sistema de seguridad perimetral

X: Sistema de seguridad perimetral.

O1: Datos PosPrueba de los indicadores de la variable dependiente.

O2: Datos PosPrueba de los indicadores de la variable dependiente.

--: Falta de la condición experimental o estímulo.

Se utilizaron 02 grupos por ser el diseño de investigación Experimental Puro.

3.2. Variables y operacionalización

3.2.1. Variables

Variable dependiente: Gestión de la infraestructura de redes y comunicaciones

Variable Independiente: Sistema de seguridad perimetral

Variable interviniente: Modelo SAFE de CISCO

Tabla 1. *Variables e indicadores*

VARIABLES	INDICADORES
1. Independiente: **Sistema de seguridad perimetral.**	• Presencia_Ausencia
2. Dependiente: **Gestión de la Infraestructura de redes y comunicaciones**	• Tiempo de ida y vuelta • Paquetes perdidos • Número de intrusiones • Número de vulnerabilidades

3.2.2. Indicadores

a) Conceptualización

Variable Independiente: Implementación de un sistema de seguridad perimetral

Tabla 2. *Variable independiente*

Indicador	Descripción
Nivel de cumplimiento de los requerimientos de la empresa	Es el grado de cumplimiento de los requerimientos en el uso de los recursos de la red en la empresa Agrofrutos Trading S. A
Servicios implementados de seguridad	Es el número de servicios de seguridad implementados en la red de la empresa Agrofrutos Trading S. A
Monitorización de eventos	Es la cantidad de eventos monitorizados en el uso de los recursos de la red en la empresa Agrofrutos Trading S. A
Alertas de indisponibilidad	Cantidad de alertas de indisponibilidad de existentes en el uso de los recursos de la red en la empresa Agrofrutos Trading S. A

Variable Dependiente: Infraestructura de redes y comunicaciones

Tabla 3. *Variable dependiente*

Indicador	Descripción
Tiempo de ida y vuelta	Es el tiempo que demora el ping de un IP en tener conectividad con un host de la red
Paquetes perdidos	Es la cantidad de paquetes que se pierde al realizar un ping de un IP por tratar de tener conectividad con un host de la red
Numero de intrusiones	Es la cantidad de accesos no autorizados con la intención de acceder a los recursos informáticos de una red para modificar la integridad de la información
Numero de vulnerabilidades	Es la cantidad de características de debilidad en una red de datos, que son susceptibles a ser explotados en forma intencional o accidental.

b) Operacionalización de Variables

Variable Independiente: Implementación de un sistema de seguridad perimetral

Tabla 4. *Variable dependiente*

INDICADOR	INDICE
Presencia_Ausencia	**No, Si**

Variable Dependiente: Infraestructura de redes y comunicaciones

Tabla 5. *Variable independiente*

DIMENSIONES	INDICADOR	ÍNDICE	UNIDAD DE MEDIDA	FÓRMULA	UNIDAD DE OBSERVACIÓN
DISPONIBILIDAD	Tiempo de ida y vuelta	[0-80]	Milisegundo / Envío	$\sum_1^n$ TIV/n **TIV=**Tiempo de ida y vuelta n= número de envíos	Ficha de Observación/Directa
	Paquetes perdidos	[0-100]	Promedio de paquetes / Envío	$\sum_1^n \frac{PE - PR}{n}$ **PE**=Paquetes enviados **PR**=Paquetes recibidos n= número de envíos	Ficha de Observación/Directa
SEGURIDAD	Número de intrusiones	[0-100]	Cantidad de intrusiones	----------	Ficha de Observación/Directa
	Número de vulnerabilidades	[0-50]	Cantidad de vulnerabilidades	----------	Ficha de Observación/Directa

3.3. Población, muestra y muestreo

Tabla 6. *Población, muestra y muestreo*

Unidad Muestral:	Gestión de la infraestructura de redes y comunicaciones Restricciones • Empresas agro exportadoras
Universo:	Todos los procesos de la gestión de Infraestructura de redes y comunicaciones de las empresas agro exportadoras. Debido a que no es posible reconocer ni precisar la cantidad de procesos, antes mencionado se tiene: N= Indeterminado
Muestra:	Procesos de la gestión de la Infraestructura de redes y comunicaciones de la empresa Agrofrutos Trading S.A
	n=30 procesos
Tipo de Muestreo:	Probabilístico

3.4. Técnicas e instrumentos de recolección de datos

Tabla 7. *Instrumentos*

INSTRUMENTOS
• Ficha de observación

3.5. Procedimiento de recolección de datos

Tabla 8. *Técnica de recolección de datos*

Técnica
Observación Directa: • Participante

3.6. Métodos de análisis de datos

En este item de la investigación se menciona la ejecución del estudio de los datos de la siguiente forma:

3.6.1 Etapas del análisis de resultados

Los pasos para el análisis de los resultados se detallan a continuación:

- Selección del programa estadístico para el análisis de los datos
- Ejecutar el software estadístico a utilizar, en este caso Minitab
- Explorar, analizar y visualizar los datos por indicador de estudio
- Se efectúa el análisis estadístico descriptivo correspondiente a los indicadores del estudio
- Se efectúan el análisis estadístico inferencial de las hipótesis que se plantearon
- Se procesa los resultados de los indicadores
- Los resultados son preparados para su presentación

3.6.2 Software de análisis de datos

Para el presente estudio se utilizó el software Minitab

3.6.3 Medidas de estadística descriptiva

La Distribución de frecuencias gráficas, se realizó mediante tablas de frecuencia e histogramas. Las medidas de tendencia central utilizadas para la investigación fueron mediana, media y moda. Como medidas de variabilidad se consideró desviación estándar y varianza.

Para el análisis estadístico inferencial, para la aceptación o rechazo de las hipótesis poblacionales, se consideró como parámetros:

Nivel de significancia:0.05, debido a que los datos corresponden a una distribución normal, la prueba de Hipótesis se realizó mediante el análisis paramétrico con la prueba T

3.7. Aspectos éticos

Se reconoce el respeto a los derechos de autor de las fuentes de información referenciadas en el presente trabajo de investigación, considerando el estilo internacional ISO 690:2010, el mismo que describe la forma de citar y referenciar.

Se considera las normas y reglas, según se especifica en el código de ética profesional del Colegio de Ingenieros del Perú, en ella se incluyen todos los reglamentos para evitar falta alguna, sea esta leve o grave (1987 p. 6).

La investigación se ciñe al artículo N°43 del código de ética profesional del CIP acerca de la inviolabilidad del trabajo ajeno, debido a que no se ha apropiado de trabajos realizados por otras personas para su desarrollo y por ello se referencio en forma apropiada los trabajos de otros autores. De igual forma se cumplió con el articulo N° 41, pues en los análisis de estos se consideró las ideas vertidas por otros autores manteniendo la consideracíon de su autoría.

En la Universidad César Vallejo, el código de ética de la investigación sostiene en sus artículos, terminos considerados faltas de ética y sanciones, los mismos que han sido analizados y observados con el fin de no estar inmerso en alguna de estas, para no recibir alguna sanción, por ello esta investigación se basa en en honestidad y rigor científico, con el proposito de obtener un estudio de calidad (Universidad César Vallejo, 2020 p. 8)

En esta investigación se cumple el artículo N°1 del código de ética de la Universidad Cesar Vallejo, y se desarrolló considerando al máximo el rigor científico, responsabilidad y honestidad, precisando conocimiento cientifico eficiente. Asimismo se consideró el artículo N°15, el mismo que precisa que el plagio es el delito, que consiste en pasar como un trabajo propio, idea u obra ajena, ya sea en forma parcial o total, por tanto la presenten investigación se realizó de manera original por el autor referenciado, por tanto se citó los parrafos provenientes de trabajos de otros autores, cumpliendo lo precisado en el artículo N°16.

IV. RESULTADOS

4.1 Implementación de un sistema de seguridad perimetral: aplicando la metodologia SAFE de CISCO

4.1.1. Fase 1: Planeamiento

En esta etapa se evaluó las amenazas existentes y los riesgos de los activos de la organización considerando es aspecto de seguridad de los dispositivos de comunicación y de datos. Para la evaluación se consideró categorizar los activos de acuerdo a su tipo, según tabla.

Tabla 9. *Categoría de activos*

CATEGORÍA DE ACTIVOS			
TIPO	**CÓDIGO**	**CATEGORÍA**	**DESCRIPCIÓN**
Activos de Hardware	H1	Equipo de procesamiento de datos	Servidores, computadoras, laptops, entre otros
	H2	Equipo de comunicaciones	Routers, switchs, access point, antenas, modems entre otros
Servicios	S1	Procesamiento y comunicaciones	Servicio de procesamiento de la información, telefonía, celular entre otros

De acuerdo a lo especificado, considerando el aspecto de seguridad de los datos para determinar el nivel de riesgo, se calcula mediante la fórmula de Nivel de Riesgo = Probabilidad de Ocurrencia x Impacto.

Tabla 10. *Probabilidades de ocurrencia*

PROBABILIDAD DE OCURRENCIA		
VALOR	**PUNTAJE**	**CRITERIO**
Bajo	1	Muy rara vez
Mediano	2	Hasta dos veces al Año
Alto	3	Hasta una vez al mes
Muy alto	4	Más de una vez al mes
Extremo	5	Varias veces a la semana o al día

Tabla 11. *Valores para el impacto*

IMPACTO		
VALOR	**PUNTAJE**	**CRITERIO**
Menor	1	Frecuencia en ocasiones excepcionales, como una vez cada 2 años
Significativo	2	Frecuencia poco probable, como 3 veces cada año
Dañino	3	Frecuencia en algún momento, como una vez al mes
Serio	4	Frecuencia de que ocurra de 2 a más veces a la semana
Grave	5	Frecuencia de 4 a más veces al día

Tabla 12. *Nivel de riesgo de los activos de seguridad*

Id Activo	Nombre Del Activo	Categoría	Probabilidad de Ocurrencia	Impacto	Nivel Del Riesgo
H1001	Servidor SQL Anywhere	TI	4	3	12
H1002	Servidor SQL Anywhere	TI	4	3	12
H1003	Servidor de Copias de respaldo	TI	2	1	2
H1004	Laptop IBM	Administración	3	2	6
H1005	Laptop COMPAQ	Administración	3	2	6
H1006	Laptop DELL	Trazabilidad	3	2	6
H1007	Laptop IBM	Contabilidad	3	2	6
H1008	Laptop IBM	Contabilidad	3	2	6
H1009	Laptop IBM	Senasa	3	2	6
H1010	Laptop COMPAQ	Mantenimiento	3	2	6
H1011	Laptop DELL	Exportación	3	2	6
H1012	Laptop IBM	Exportación	3	2	6
H1013	Laptop IBM	Almacén	3	2	6
H1014	CPU DELL	Administración	3	2	6
H1015	CPU DELL	Administración	3	2	6
H1016	CPU DELL	Administración	3	2	6
H1017	CPU DELL	Administración	3	2	6
H1018	CPU DELL	Administración	3	2	6

H1019	CPU DELL	Trazabilidad	3	2	6
H1020	CPU DELL	Trazabilidad	3	2	6
H1021	CPU DELL	Trazabilidad	3	2	6
H1022	CPU DELL	Contabilidad	3	2	6
H1023	CPU DELL	Contabilidad	3	2	6
H1024	CPU DELL	Senasa	3	2	6
H1025	CPU DELL	Senasa	3	2	6
H1026	CPU DELL	Senasa	3	2	6
H1027	CPU DELL	Mantenimiento	3	2	6
H1028	CPU DELL	Mantenimiento	3	2	6
H1029	CPU DELL	Mantenimiento	3	2	6
H1030	CPU DELL	Exportación	3	2	6
H1031	CPU DELL	Exportación	3	2	6
H1032	CPU DELL	Exportación	3	2	6
H1033	CPU DELL	Exportación	3	2	6
H1034	CPU DELL	Exportación	3	2	6
H1035	CPU DELL	Almacén	3	2	6
H1036	CPU DELL	Almacén	3	2	6
H1037	CPU DELL	Almacén	3	2	6
H2001	Radio Enlace MIKROTIK	Usuarios	1	1	1
H2002	Radio Enlace MIKROTIK	Usuarios	1	1	1
H2003	Radio Enlace MIKROTIK	Usuarios	1	1	1
H2004	Radio Enlace MIKROTIK	Usuarios	1	1	1
H2005	Radio Enlace MIKROTIK	Usuarios	1	1	1
H2006	Radio Enlace MIKROTIK	Usuarios	1	1	1
H2007	Radio Enlace MIKROTIK	Usuarios	1	1	1
H2008	Access Point UBIQUITI	Usuarios	2	2	4
H2009	Access Point UBIQUITI	Usuarios	2	2	4
H2010	Access Point UBIQUITI	Usuarios	2	2	4
H2011	Access Point UBIQUITI	Usuarios	2	2	4
H2012	Access Point UBIQUITI	Usuarios	2	2	4
H2013	Access Point UBIQUITI	Usuarios	2	2	4
H2014	Access Point UBIQUITI	Usuarios	2	2	4
H2015	Access Point UBIQUITI	Usuarios	2	2	4
H2016	Access Point UBIQUITI	Usuarios	2	2	4
H2017	Switch TPLINK	Usuarios	2	1	2
H2018	Switch TPLINK	Usuarios	2	1	2
H2019	Switch TPLINK	Usuarios	2	1	2
H2020	Switch TPLINK	Usuarios	2	1	2

H2021	Switch TPLINK	Usuarios	2	1	2
H2022	Switch TPLINK	Usuarios	2	1	2
H2023	Switch TPLINK	Usuarios	2	1	2
H2024	Switch TPLINK	Usuarios	2	1	2
H2025	Switch TPLINK	Usuarios	2	1	2
H2026	Switch TPLINK	Usuarios	2	1	2
H2027	Switch TPLINK	Usuarios	2	1	2
H2028	Switch TPLINK	Usuarios	2	1	2
H2029	Switch TPLINK	Usuarios	2	1	2
H2030	Switch TPLINK	Usuarios	2	1	2
H2031	Switch TPLINK	Usuarios	2	1	2
H2032	Switch TPLINK	Usuarios	2	1	2
H2033	Switch TPLINK	Usuarios	2	1	2
H2034	Switch TPLINK	Usuarios	2	1	2
H2035	Switch TPLINK	Usuarios	2	1	2
H2036	Switch TPLINK	Usuarios	2	1	2
H2037	Switch TPLINK	Usuarios	2	1	2
H2038	Switch TPLINK	Usuarios	2	1	2

4.1.2. Fase 2: Diseño

Diseño Físico

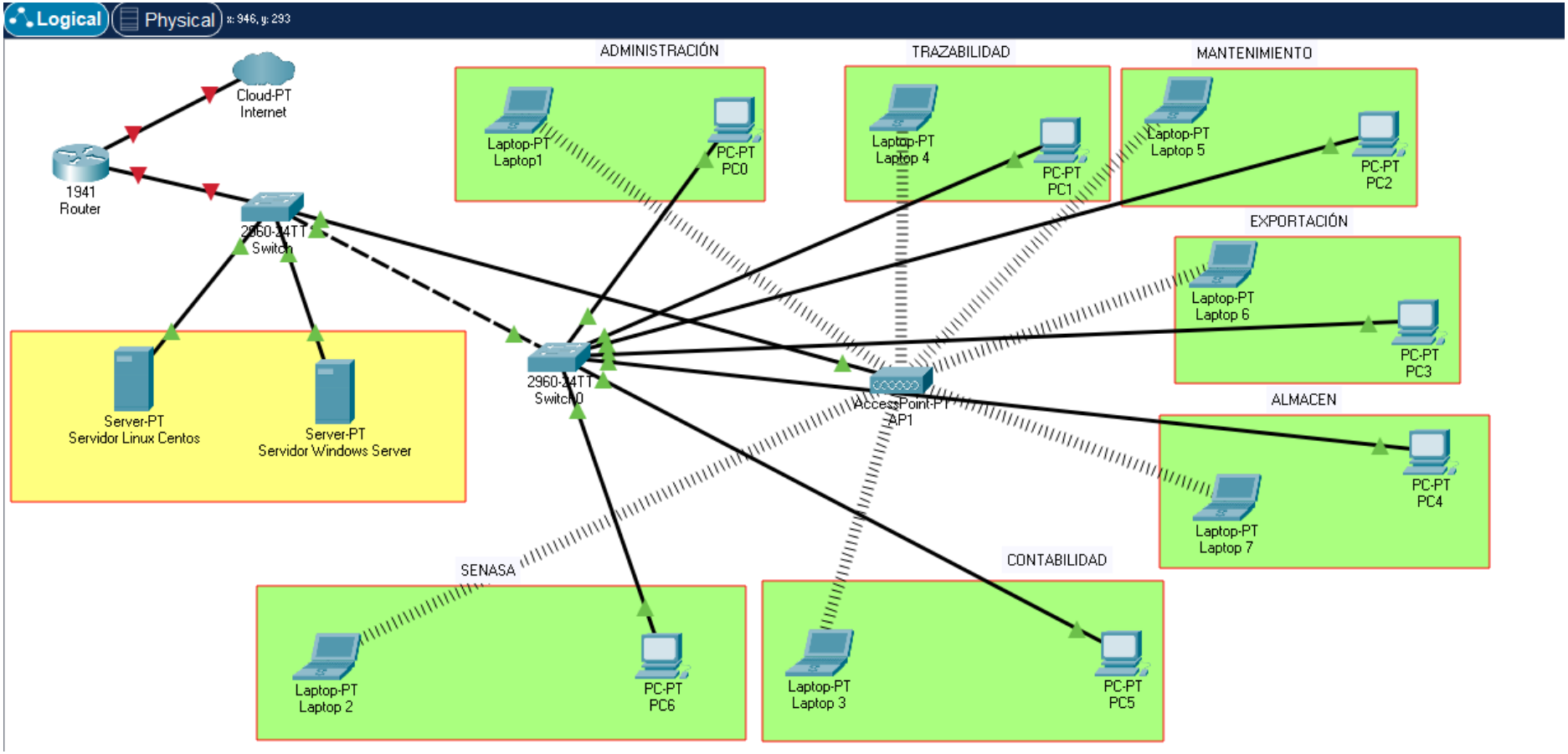

Figura 2. Diseño anterior

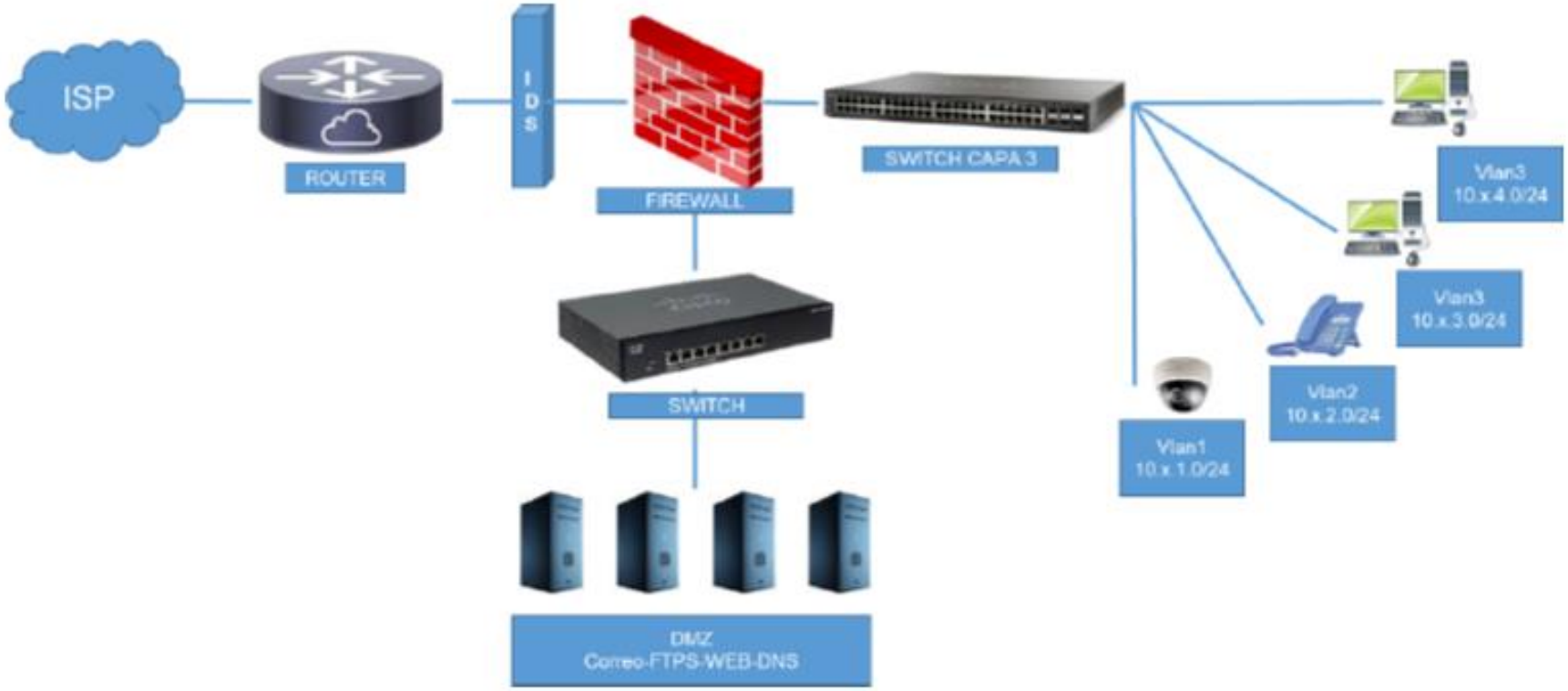

Figura 3. Diseño actual

Diseño Lógico

Instalacion y configuración del Controlador del dominio

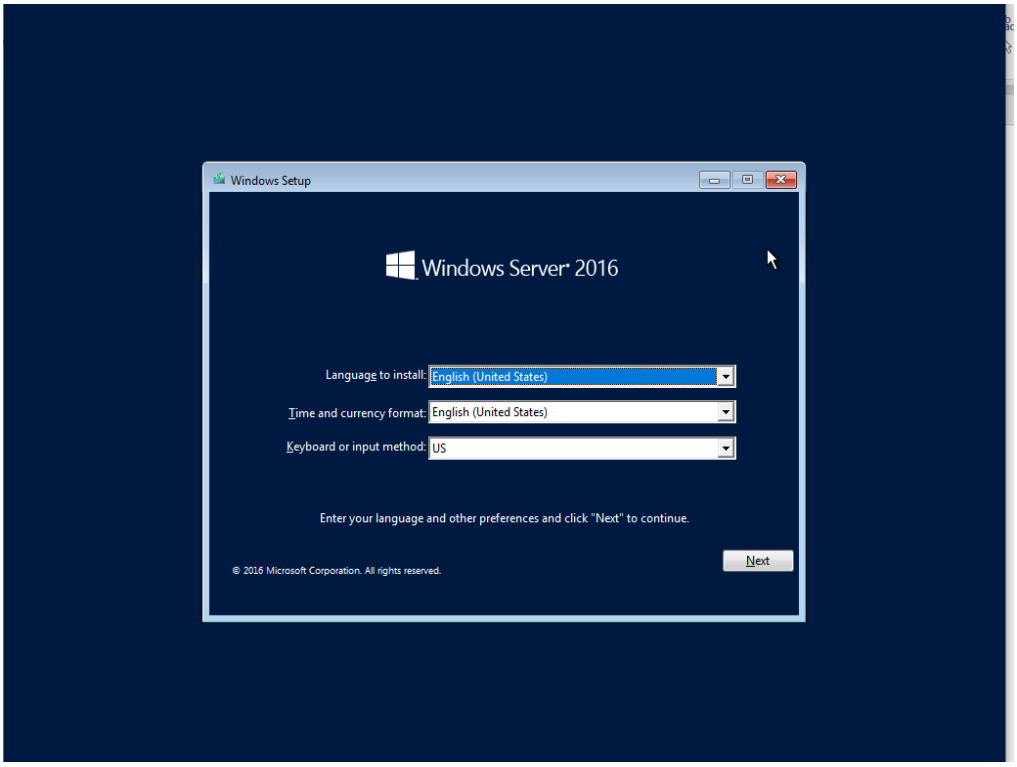

Figura 4. Instalación Windows Server 2016

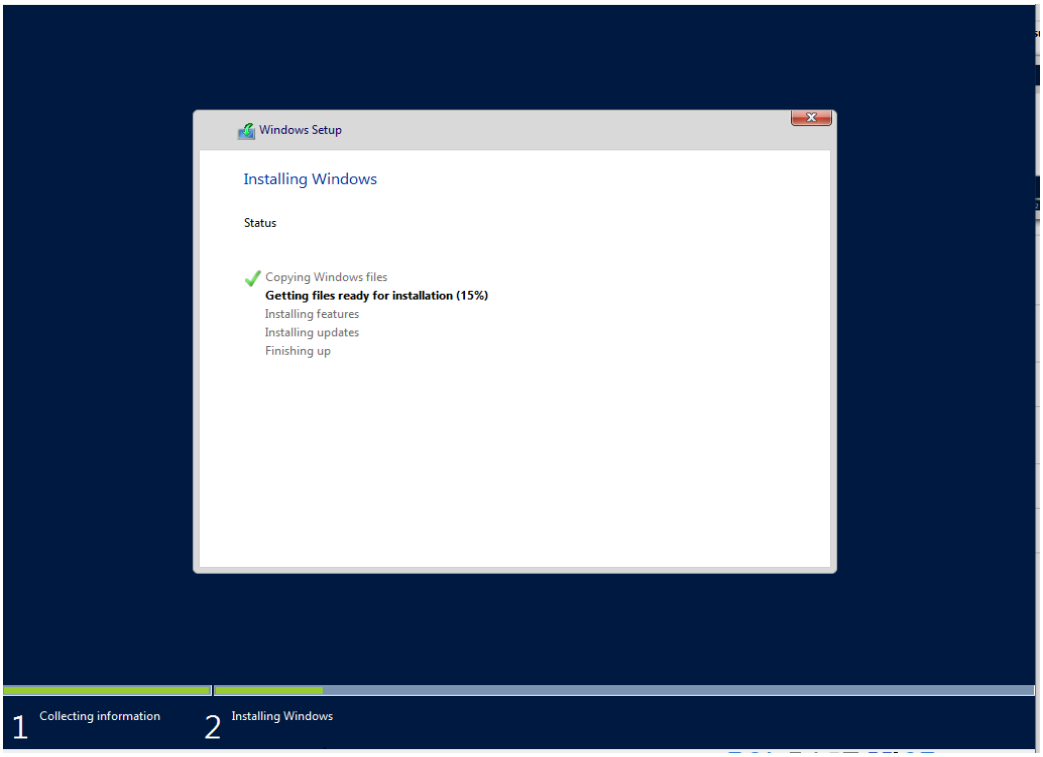

Figura 5. Configuración Windows Server 2016

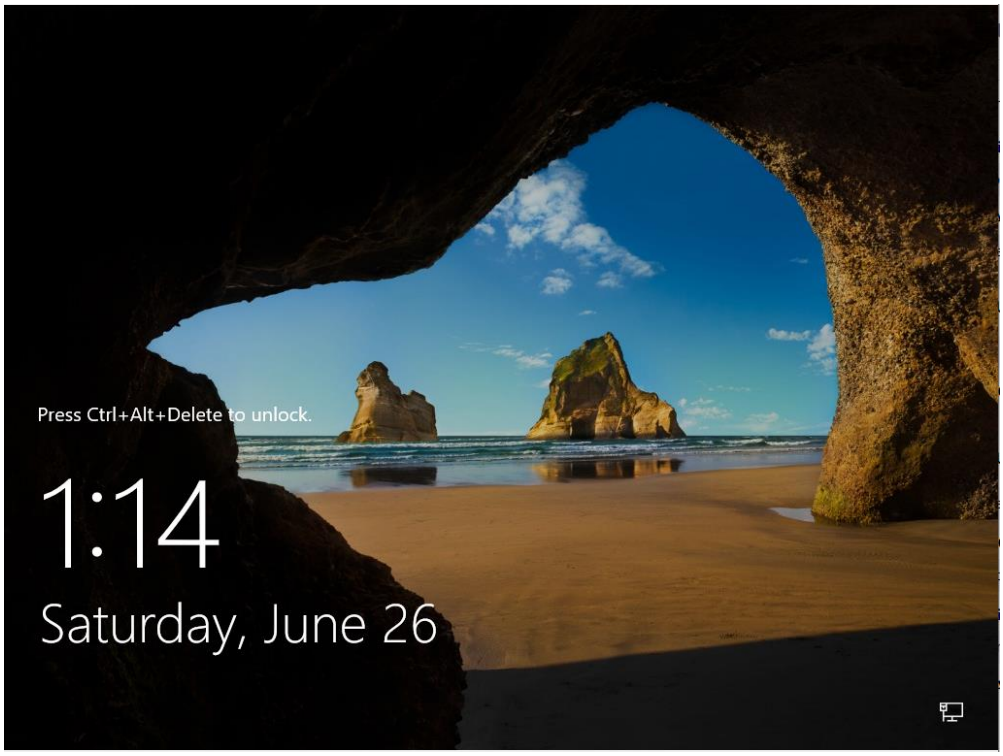

Figura 6. inicio Windows Server 2016

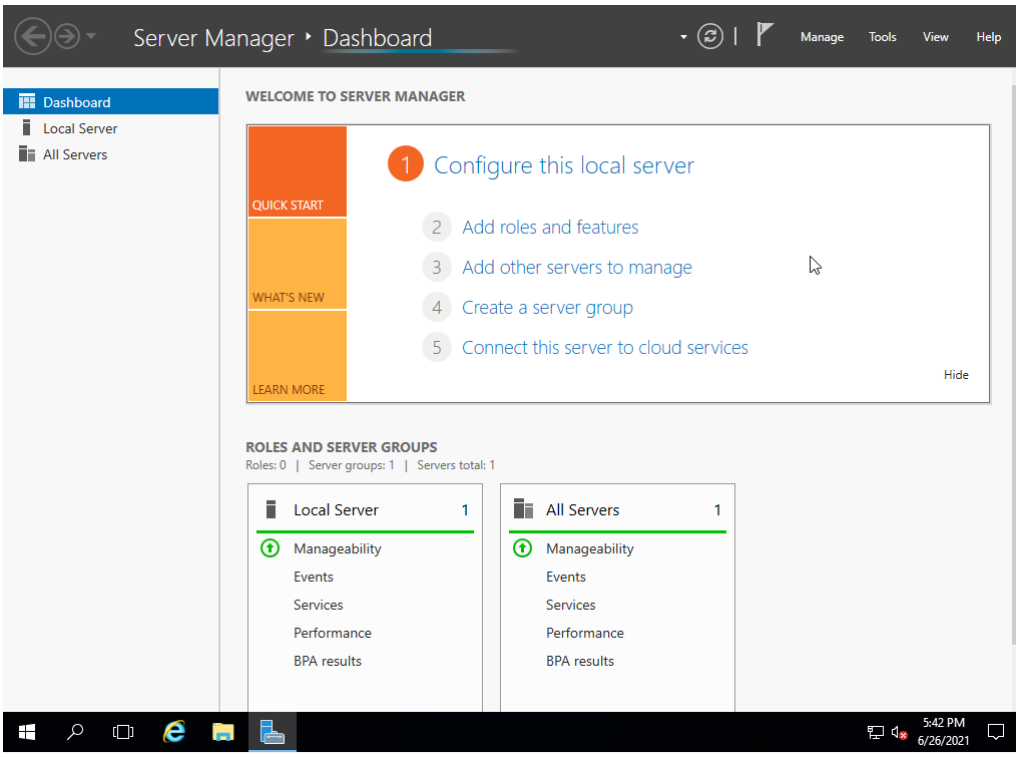

Figura 7**.** Administrador Windows Server 2016

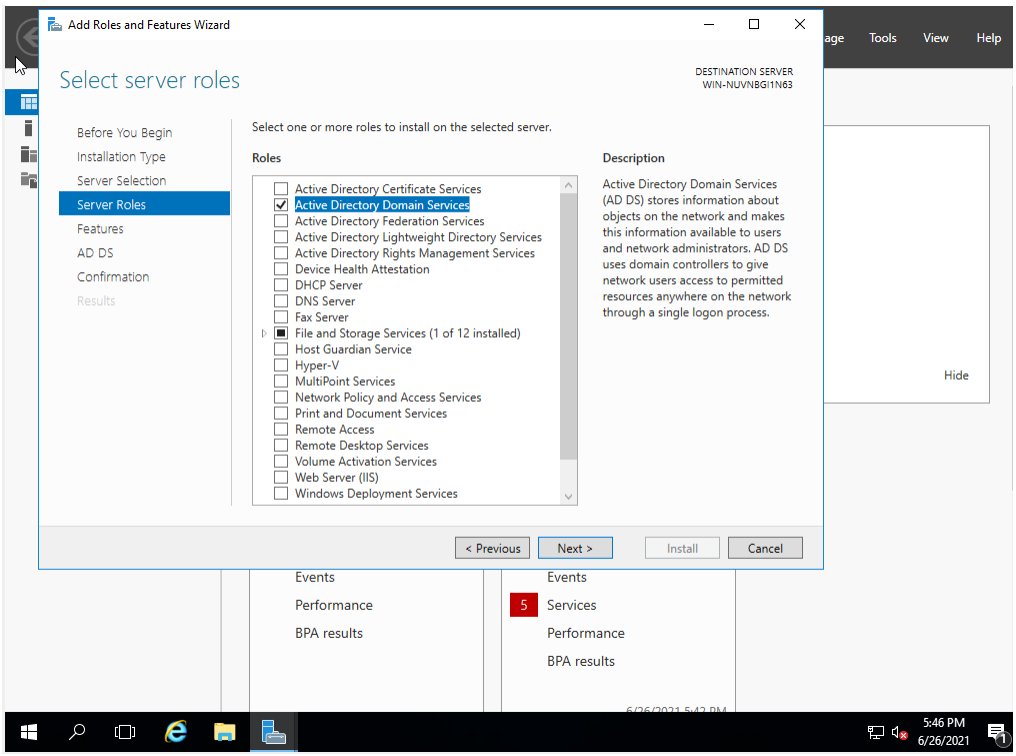

Figura 8. Roles de Windows Server 2016

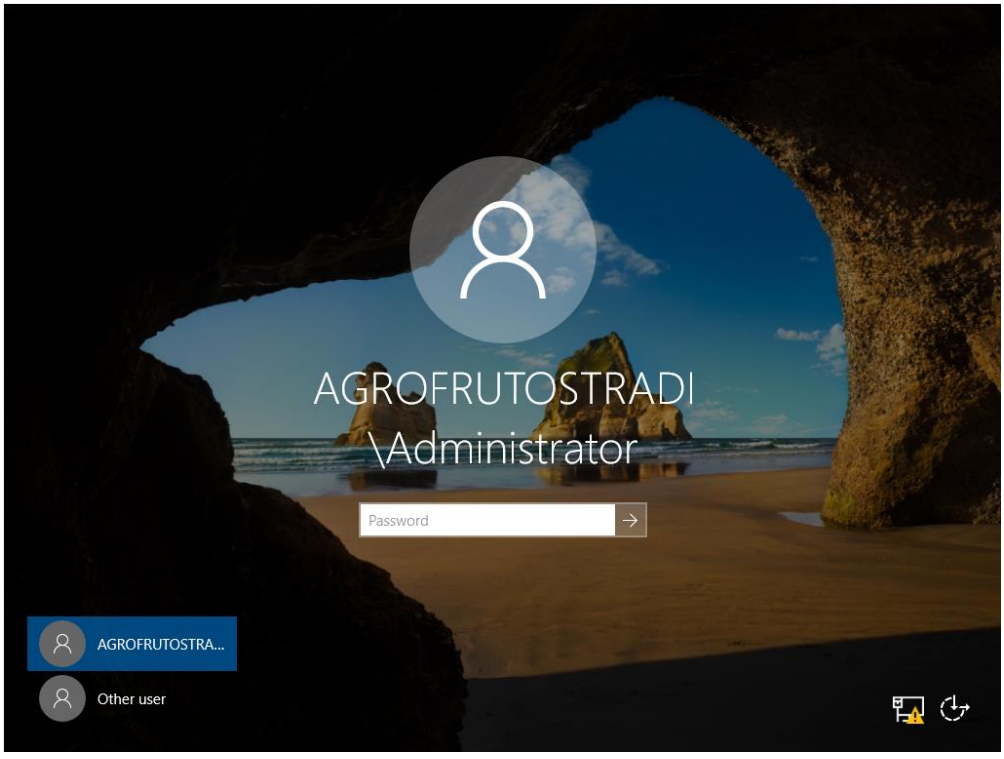

Figura 9. Dominio Windows Server 2016

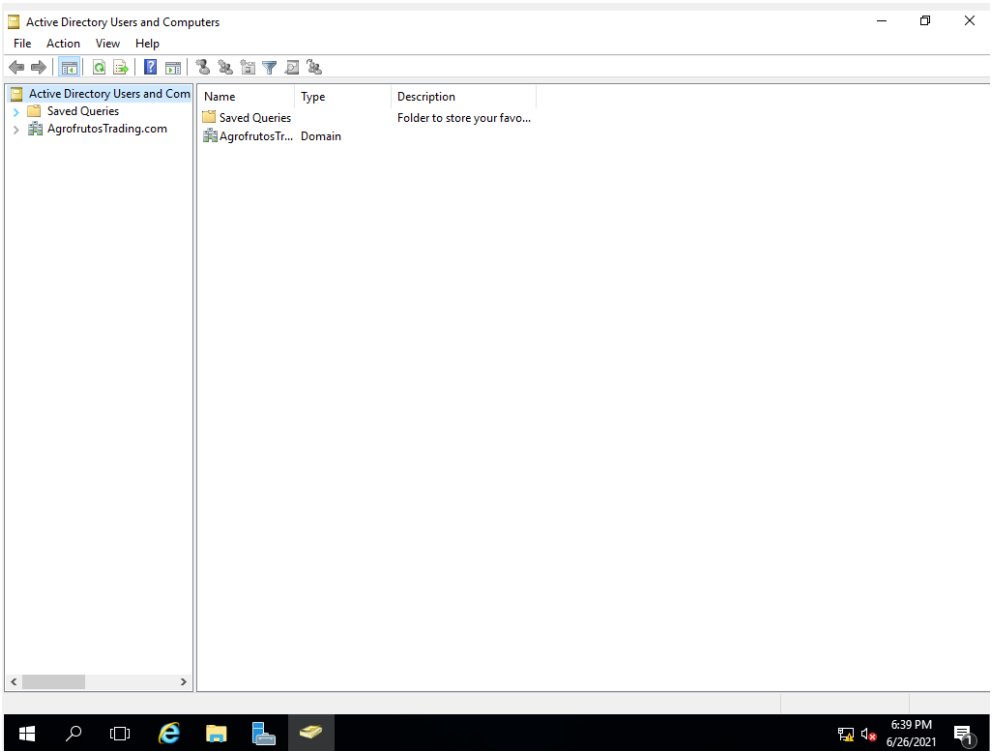

Figura 11. Unidades organizativas de la empresa

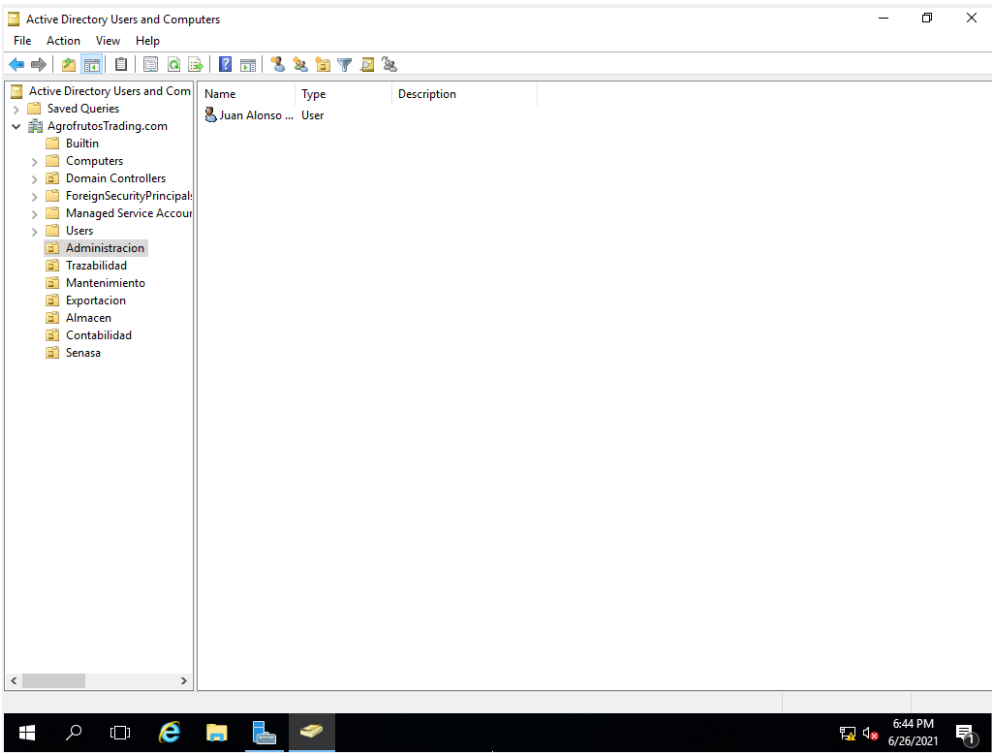

Figura 10. Usuarios y computadoras del directorio activo

4.1.3. Fase 3: Implementación

Defensa de datos

Se creó la política para la creación de usuarios, esto para permitir y controlar el acceso el personal que requiera información. Se implementó un servidor con directorio activo, con el dominio AgrofrutosTrading.com, asignandose una ruta de trabajo a los usuarios, con restricciones y privilegios de acuerdo a los grupos creados en cada unidad organizacional del controlador principal. Se consideró VPN a los usuarios flotantes que interactuan entre la red LAN.

Defensa de la aplicación

Se realizó mediante la actualización de licencia del antivirus de la empresa Agrofrutos Trading S.A, pues cubre necesidades principales, como el control de dispositivos desde plataformas en la nube. Asegurando características gráficos de analisis de virus, ejecucón de consola en la nueb, descarga de actualizaciones, control de contenido para acceder a la web, atraves de listas de acceso proporcionando un consumo adecuado de datos.

Defensa de host

Se creo la politica de hardening(aseguramiento) con el proposito de minimizar las vulnerabilidades de seguridad, considerando depurar aplicaciones en forma periodica, usuarios inactivos o retirados, asimismo auditoria permanente a los puertos, iniciando su apertura conforme las aplicaciones lo requieran y los que no son requeridos se mantiene cerrados. Adicionalmente se programo un sistema de actualizaciones automaticos en horarios de menor carga laboral para no sobrecargar a los sistemas. Ademas desde controlador del dominio, se creo politicas de grupo (GPO) que bloquean a los componentes de los dispositivos de acuerdo a las restricciones de los usuarios según horarios de trabajo. Finalmente un seguimientos a los logs que genera los antivirus, con el objetivo de bloquear las brechas de seguridad en hardware y en software.

Defensa en red

En cuanto a la implementación de la red, se realizó configuraciones, los equipos de software y hardware para su seguridad.

Seguridad perimetral y física

En lo que respecta a la protección del perimetro de las instalaciones, debido a que pueden generar brechas de seguridad se planteó un circuito cerrado, monitoreado en forma permanente. La configuración sugerida, fue por detección de movimientos y con el fin de garantizar que no se sature la capacidad del disco almacenar las grabaciones de 30 dias autoescribibles, con el fin de garantizar que no se sature la capacidad del disco. En cada esquina se sugirió camaras con un angulo de 90° y el resto de ubicaciones camaras con sistemas de domo.

Configuraciones de firewall y bloqueo de paginas

En esta etapa se realizo las configuraciones de firewall y bloqueo de algunas paginas serealizo de la siguiente manera:

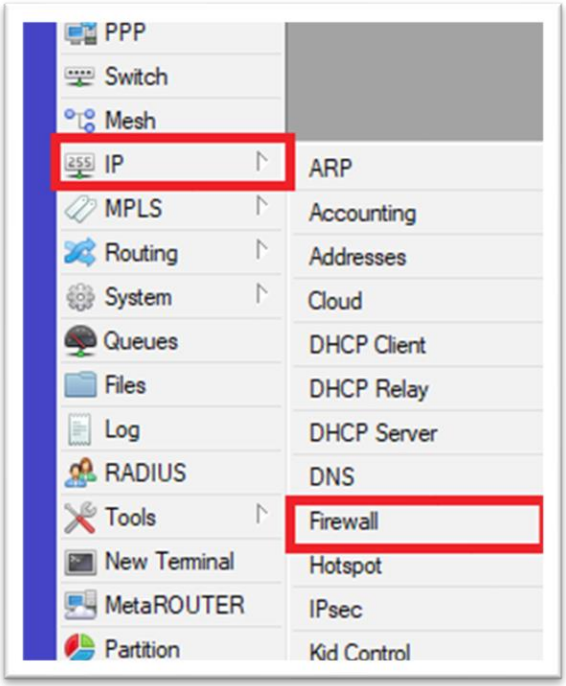

Figura 12. Configuraciones de firewall

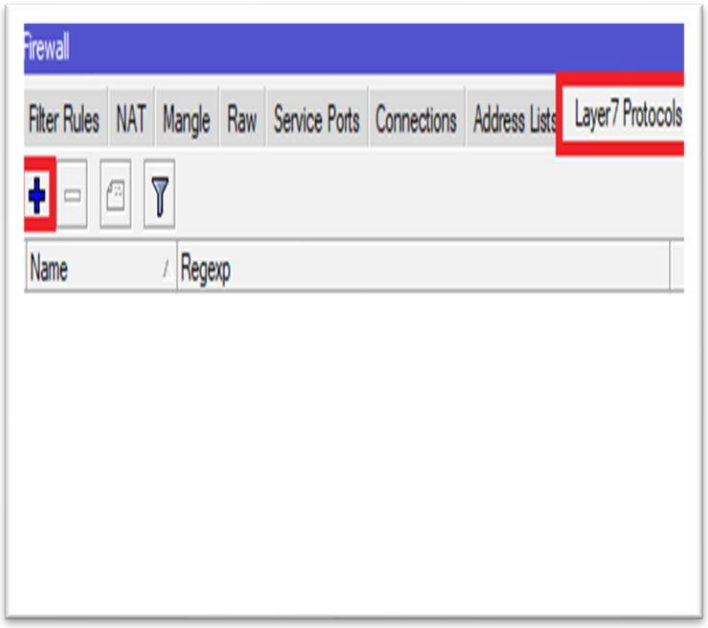

Figura 14. Configuración de protocolos

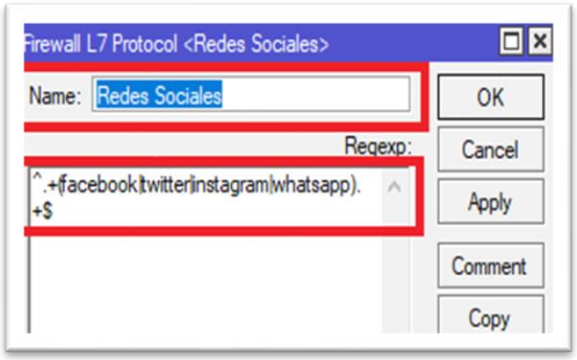

Figura 13. Configuración de reglas

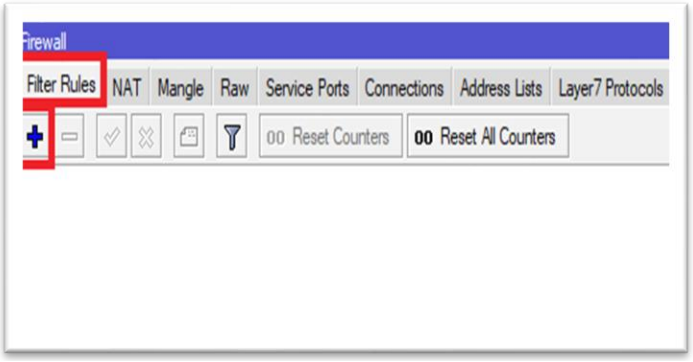

Figura 15**.** Filtrado de páginas

Configuraciones básicas de mikrotik como es agregar las direcciones IP y Mac de todas más Máquinas

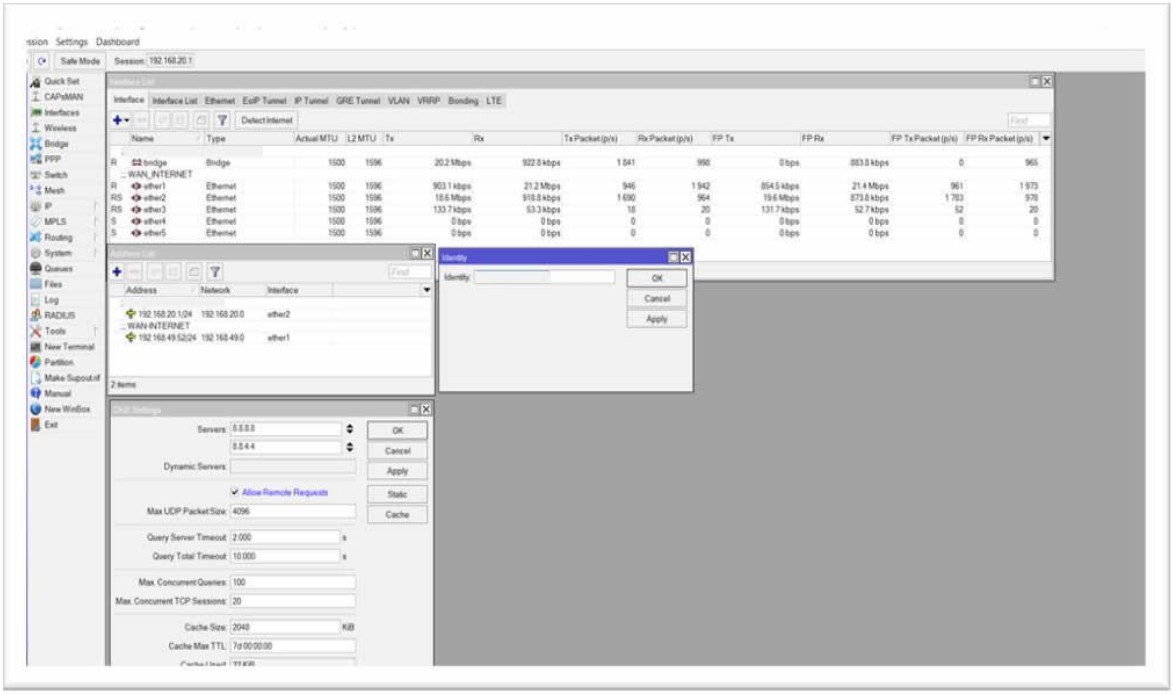

Figura 16. Configuración de Mikrotik

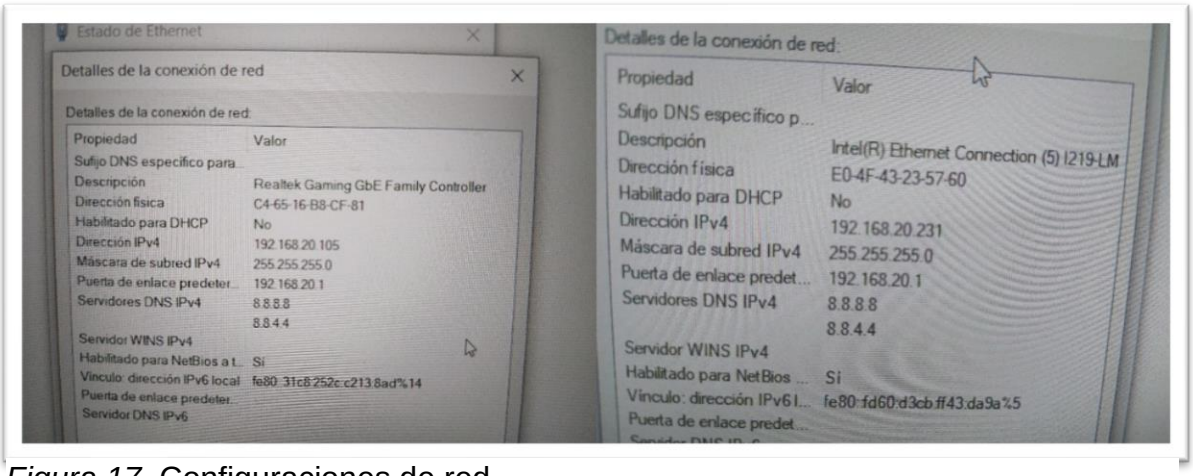

*Figura 17***.** Configuraciones de red

4.1.4. Fase 4: Operación

Monitorear la infraestructura implementada para mitigar el riesgo.

Figura 18. Monitoreo del ancho de banda de la red

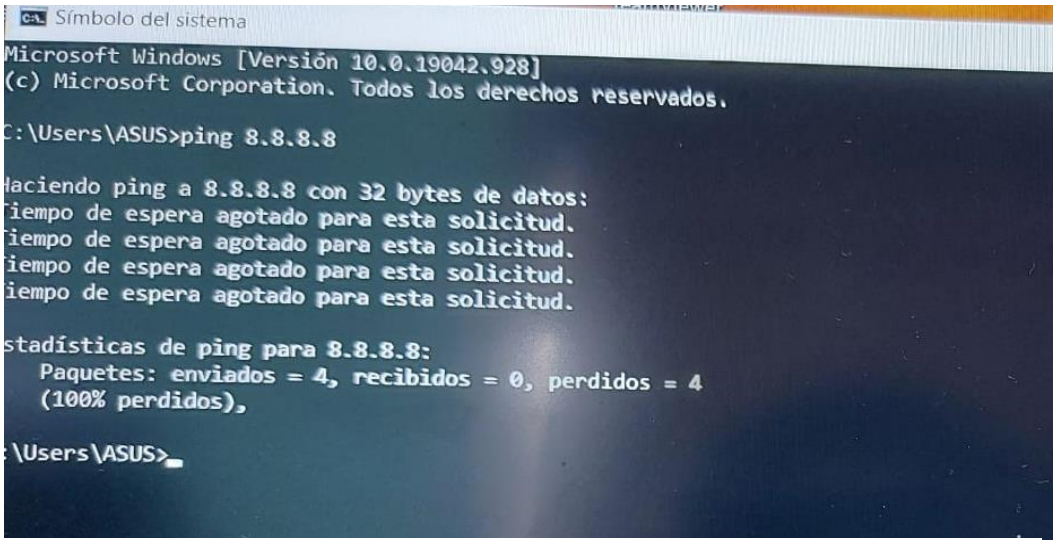

Figura 19. Aplicación Ping a DNS

Reglas de filtrado mediante direcciones IP

Tabla 13. *Reglas de filtraje direcciones IP*

Regla	IP Origen	IP Destino	Acción
1	75.32.152.*	198.125.12.*	Permitir
2	198.125.12.*	75.32.152.*	Permitir
3	*	*	Negar

Reglas de filtrado mediante IP y puertos TCP/UDP

Tabla 14. *Reglas de filtraje direcciones IP y puertos TCP/UDP*

Regla	Conexión	Tipo	IP Origen	IP Destino	Puerto fuente	Puerto Destino	Acción
1	entrada	tcp	externa	interna	>=1024	25	permitir
2	entrada	tcp	interna	externa	25	>=1024	permitir
3	salida	tcp	interna	externa	>=1024	25	permitir
4	entrada	tcp	externa	interna	25	>=1024	permitir
5	*	*	*	*	*	*	negar

4.1.5. Fase 5: Optimización

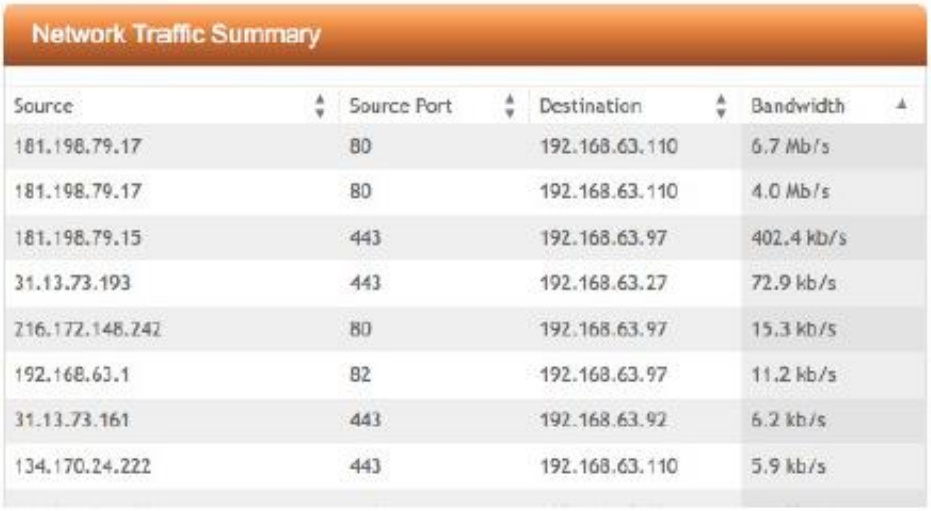

Figura 20. Optimización de Ancho de banda de IP

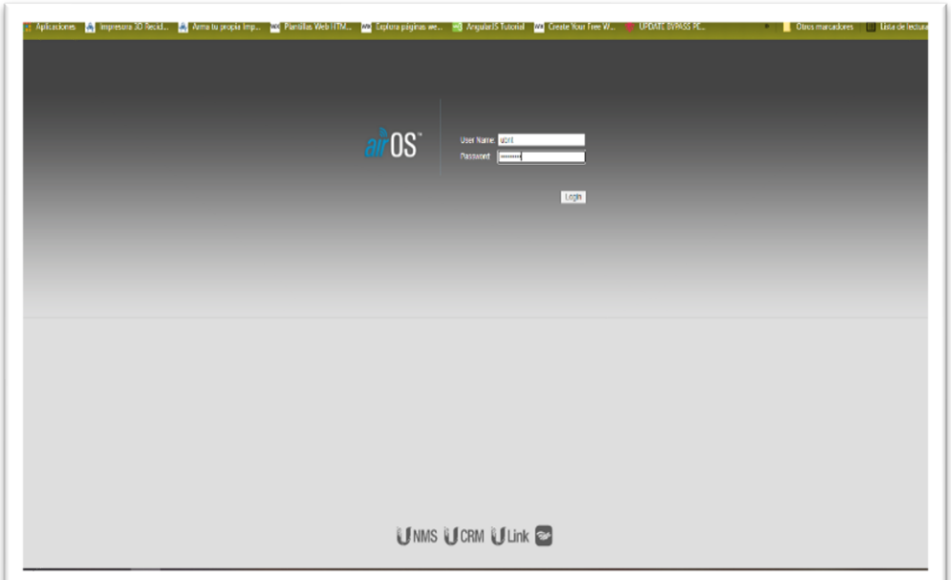

Figura 21. Optimización de indicadores de red en el Router

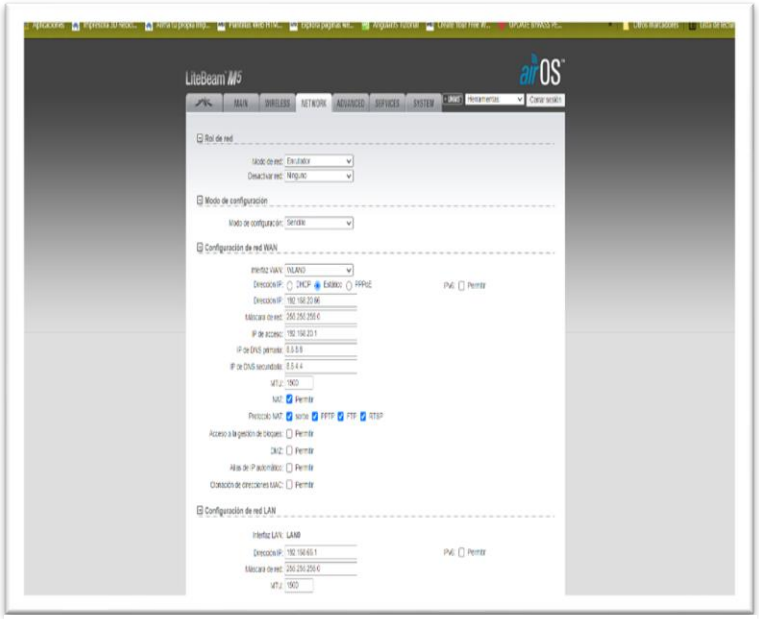

Figura 23. Optimización parámetros de red

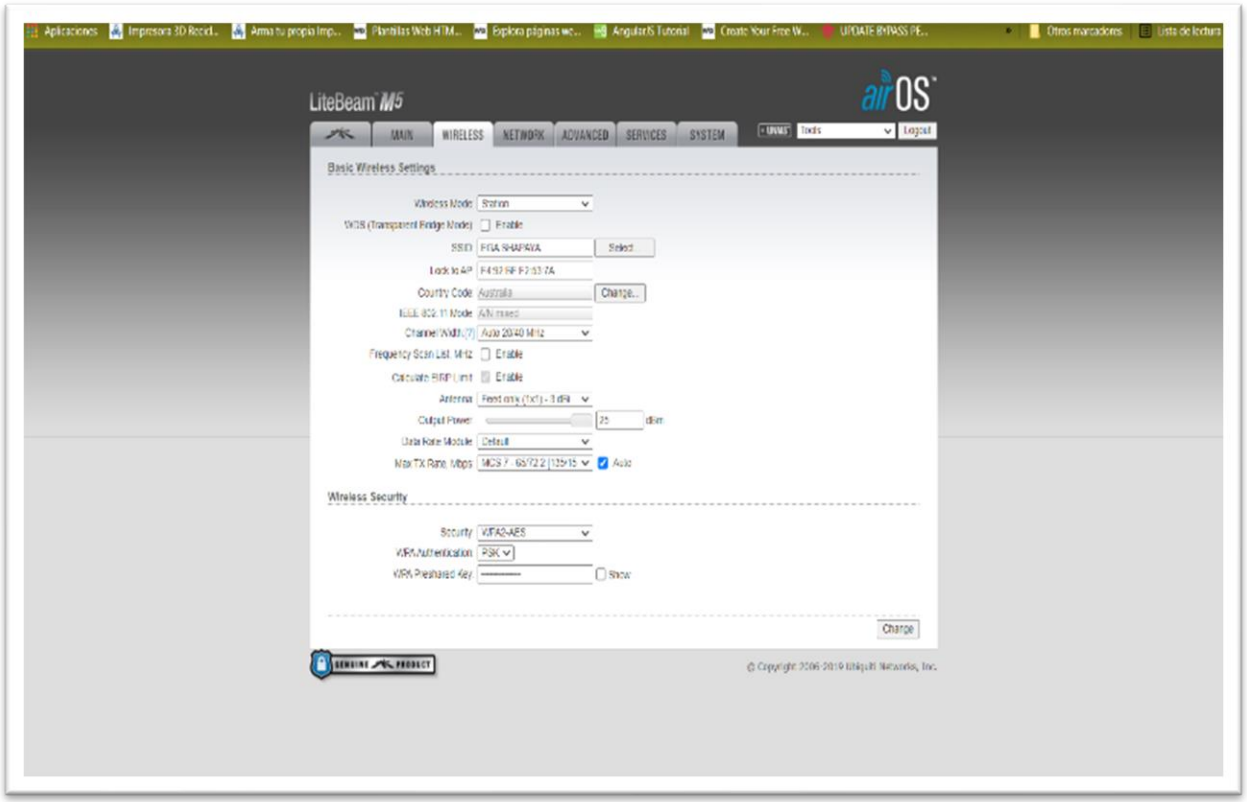

Figura 22. Configuración y optimización de Wireless

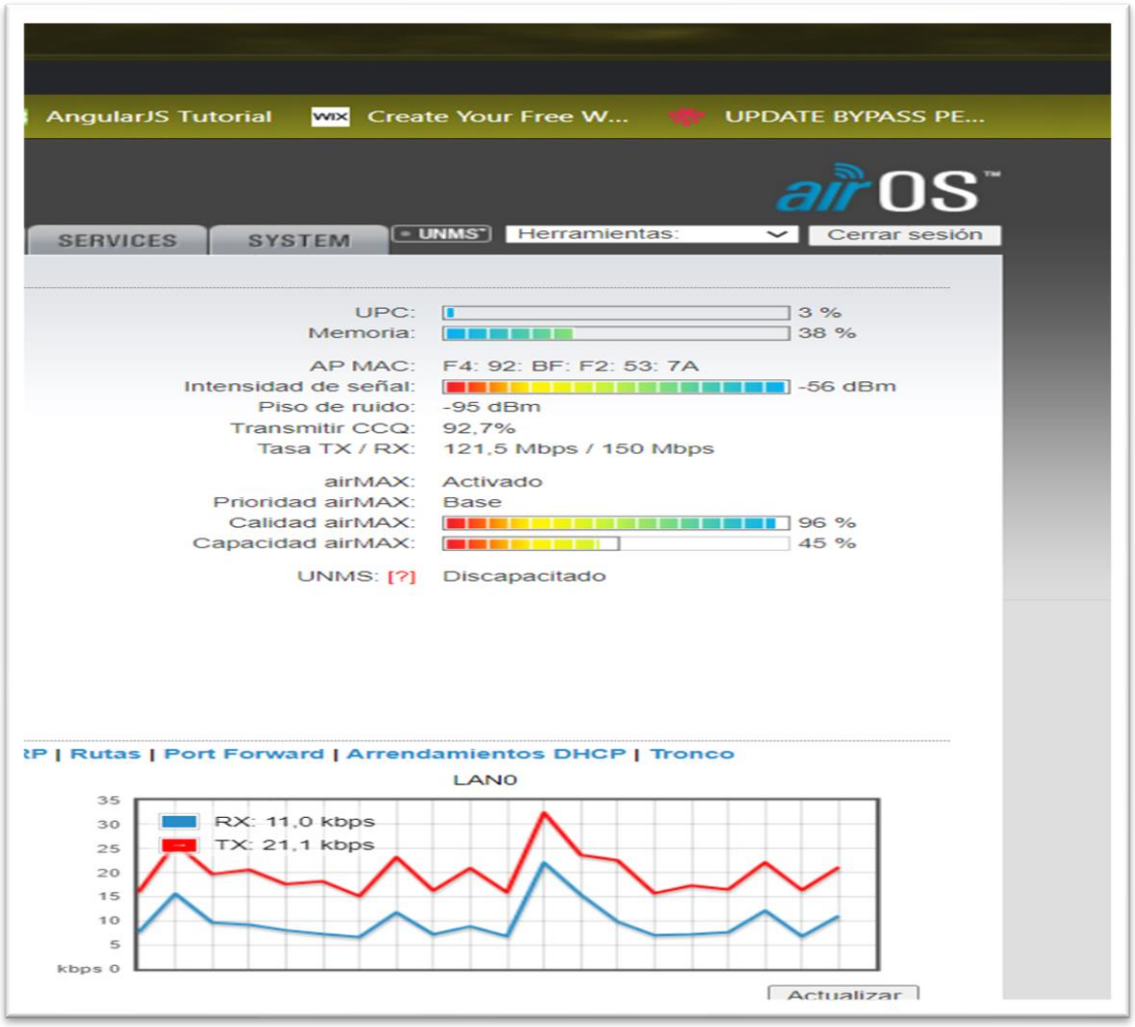

Figura 24. Configuración sistema operativo airOS

4.2 Resultados

En esta sección se detallan

A continuación se muestran los valores de los indicadore del Pre y Post del G.

Tabla 15. *Resultados de los indicadores del Pre y Post del G.*

Número	**I1: Tiempo de ida y vuelta (milisegundos)**		**I2: Perdida de paquetes (Porcentaje)**		**I3: Número de intrusiones(Veces x dia)**		**I4: Número de vulnerabilidades**	
	Post-test Gc	Post-test Ge	Post-test Gc	Post-test Ge	Post-test Gc	Post-test Ge	Post-test Gc	Post-test Ge
1	35	22	8,5	0,4	13	4	25	4
2	31	21	5,0	0,2	11	5	22	2
3	31	19	10,2	0,7	15	3	28	3
4	34	21	7,4	0,5	8	2	16	2
5	29	20	8,2	0,0	10	4	20	4
6	35	25	5,0	0,5	7	1	14	1
7	33	21	7,5	0,7	10	4	20	4
8	31	24	6,2	0,2	8	2	15	2
9	29	19	10,5	0,4	13	4	25	4
10	31	21	8,5	0,0	11	5	22	5
11	33	20	5,6	0,5	9	3	18	3
12	31	22	9,5	0,1	9	3	18	3
13	34	23	7,6	0,0	5	0	10	0

14	30	21	9,0	0,4	8	2	15	2
15	31	23	8,6	0,3	6	0	12	0
16	35	22	10,0	0,1	8	2	15	2
17	38	21	5,5	0,3	12	6	24	6
18	33	20	8,0	0,5	8	2	16	2
19	34	21	5,6	0,7	5	0	10	0
20	31	22	7,0	0,8	9	3	18	3
21	37	23	10,0	0,6	7	1	14	1
22	33	22	8,0	0,3	14	3	28	3
23	38	19	5,0	0,9	13	7	25	5
24	33	21	9,4	0,4	11	5	22	3
25	39	20	5,0	0,2	15	3	28	5
26	37	23	8,5	0,0	8	2	16	2
27	33	22	11,0	0,6	11	5	22	5
28	32	21	9,5	0,4	8	2	15	2
29	35	23	7,0	0,6	10	4	20	3
30	33	23	10,0	0,2	7	1	14	1

4.3 Prueba de Normalidad

Se realizo mediante la prueba de Anderson-Darling, la cual compara la distancia acumulada teorica de datos de la muestra con la que se esperaba, con el fin de establecer la normalidad de los datos.

4.3.1 I1: Tiempo de ida y vuelta

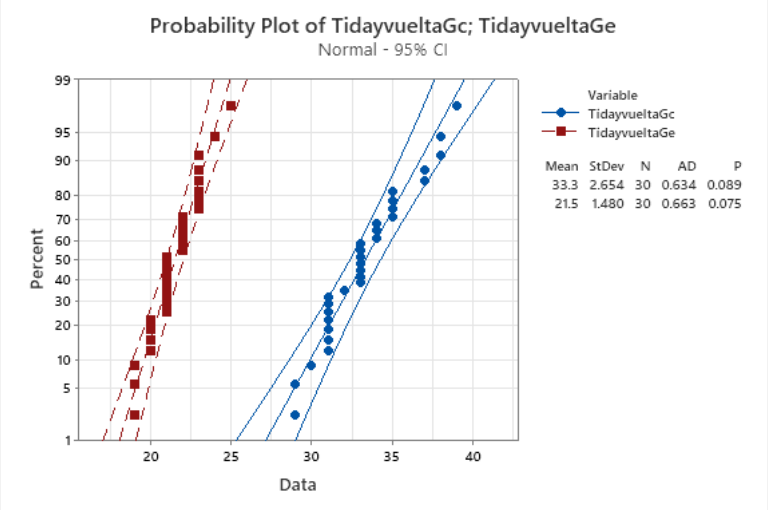

Figura 25. Probabilidad normal de tiempo de ida y vuelta

Como se muestra en la Figura 25, en PostPrueba Ge y PostPrueba Gc del indicador I1, sus valores de p son 0.089 y 0.075, los mismos que mayores a 0.05. Por lo que se infiere que los valores concernientes al tiempo de ida y vuelta tienen un comportamiento normal.

4.3.2 I2: Perdida de paquetes

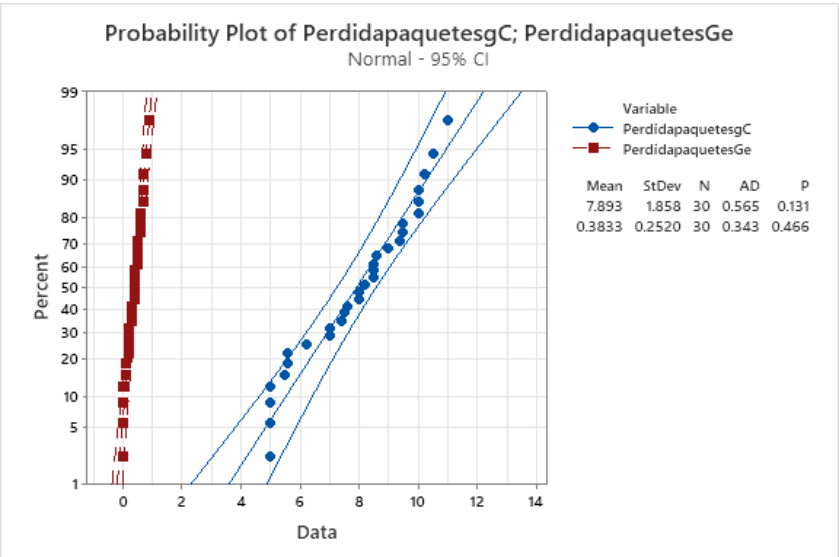

Figura 26. Probabilidad normal de perdida de paquetes

Como se aprecia en la Figura 26, en PostPrueba Ge y PostPrueba Gc del indicador I2, sus valores de p son 0.131 y 0.466, los mismos que mayores a 0.05. Por lo que se infiere que los valores concernientes a la perdida de paquetes tienen un comportamiento normal.

4.3.3 I3: Número de intrusiones

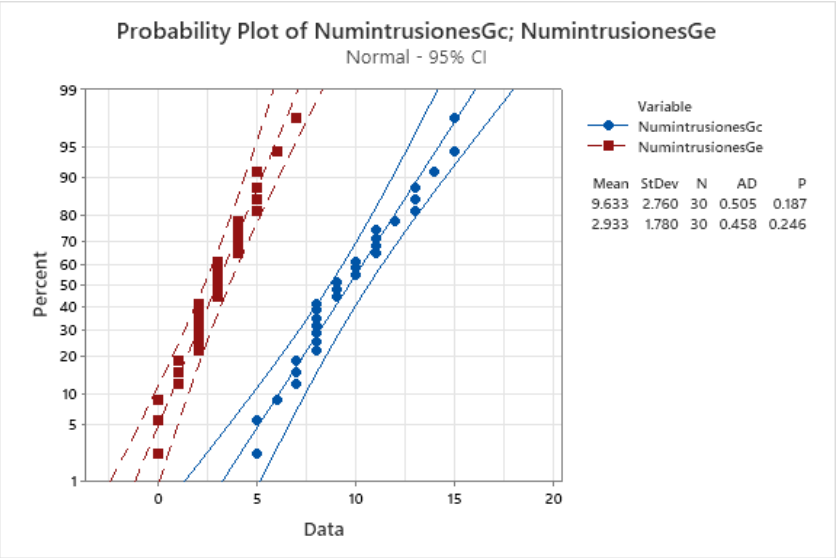

Figura 27. Probabilidad normal de número de intrusiones

Como se aprecia en la Figura 27, en PostPrueba Ge y PostPrueba Gc del indicador I3, sus valores de p son 0.187 y 0.246 los mismos que mayores a 0.05. Por lo tanto los valores concernientes al número de intrusiones posee un comportamiento normal.

4.3.4 I4: Número de vulnerabilidades

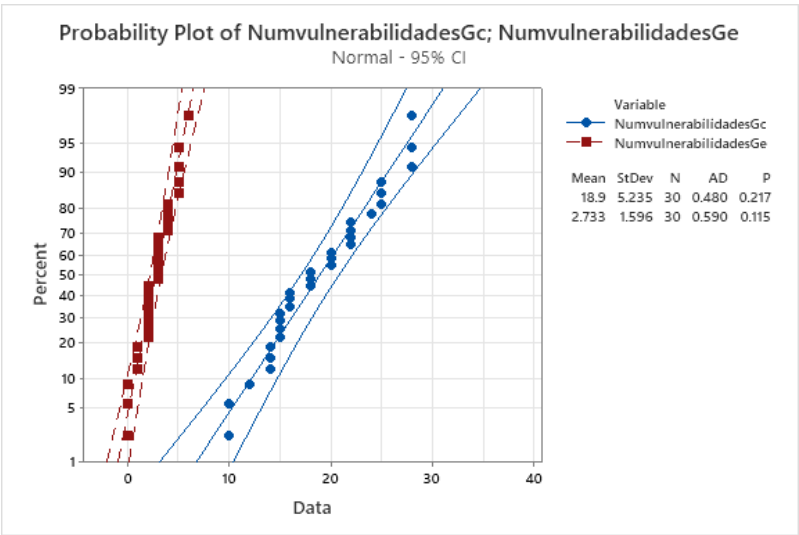

Figura 28. Probabilidad normal de número de vulnerabiliades

En la Figura 28, se aprecia, en PostPrueba Ge y PostPrueba Gc del indicador I4, sus valores de p son 0.217 y 0.115, los mismos que mayores a 0.05. Por lo que se infiere que los valores concernientes al número de vulnerabilidades tienen un comportamiento normal.

4.4 Analisis de Resultados

En las siguienttes tablas se visuzalizan los resultados de la PostPrueba del Gc y PostPrueba del Ge. Ademas se pone enfasis en los valores de la PostPrueba del Ge, que resultaron mejores, menores o mayores de acuerdo al contexto, que los promedios en la PostPrueba del Ge resaltados de fondo verde, los mismos que mejores que la meta planteada, resaltado de fondo azul , y los mismos que son menores que los promedios en la PostPrueba del Gc resaltados de fondo rojo.

Se realiza, a continuación, un análisis detallado de los datos de cada unas de las tablas.

4.4.1. Indicador **Tiempo de ida y vuelta: I_1**

Tabla 16. *Analisis detallado de indicador Tiempo de ida y vuelta*

	Post-test Gc	**Post-test Ge**		
	35	22	22	22
	31	21	21	21
	31	19	19	19
	34	21	21	21
	29	20	20	20
	35	25	25	25
	33	21	21	21
	31	24	24	24
	29	19	19	19
	31	21	21	21
	33	20	20	20
	31	22	22	22
	34	23	23	23
	30	21	21	21
	31	23	23	23
	35	22	22	22
	38	21	21	21

	33	20	20	20
	34	21	21	21
	31	22	22	22
	37	23	23	23
	33	22	22	22
	38	19	19	19
	33	21	21	21
	39	20	20	20
	37	23	23	23
	33	22	22	22
	32	21	21	21
	35	23	23	23
	33	23	23	23
Promedio	**33.3**	21.5		
Meta Planteada			22	
N° menor a Promedio		18	16	30
%° menor a Promedio		60.00	53.33	100

- El 60% de los **Tiempos de ida y vuelta** en la PostPrueba de Ge fueron menores que su tiempo promedio.
- El 53.33% de los **Tiempos de ida y vuelta** en la PostPrueba de Ge fueron menores que la meta planteada..
- El 100% de los **Tiempos de ida y vuelta** en la PostPrueba de Ge fueron menores que el tiempo promedio en la PostPrueba del Gc.

4.4.2. Indicador **Perdida de paquetes: l_2**

Tabla 17. *Analisis detallado de indicador perdida de paquetes*

	Post-test Gc	**Post-test Ge**		
	8.5	0.4	0.4	0.4
	5	0.2	0.2	0.2
	10.2	0.7	0.7	0.7
	7.4	0.5	0.5	0.5
	8.2	0	0	0
	5	0.5	0.5	0.5
	7.5	0.7	0.7	0.7
	6.2	0.2	0.2	0.2
	10.5	0.4	0.4	0.4
	8.5	0	0	0
	5.6	0.5	0.5	0.5
	9.5	0.1	0.1	0.1
	7.6	0	0	0
	9	0.4	0.4	0.4
	8.6	0.3	0.3	0.3
	10	0.1	0.1	0.1
	5.5	0.3	0.3	0.3
	8	0.5	0.5	0.5
	5.6	0.7	0.7	0.7
	7	0.8	0.8	0.8
	10	0.6	0.6	0.6
	8	0.3	0.3	0.3
	5	0.9	0.9	0.9
	9.4	0.4	0.4	0.4
	5	0.2	0.2	0.2
	8.5	0	0	0
	11	0.6	0.6	0.6
	9.5	0.4	0.4	0.4
	7	0.6	0.6	0.6
	10	0.2	0.2	0.2
Promedio	**7.893333333**	0.383333333		
Meta Planteada			0.1	
N° menor a Promedio		13	13	30
%° menor a Promedio		43.33	43.33	100

- El 43.33% de los **paquetes perdidos** en la PostPrueba de Ge fueron menores que los paquetes perdidos en promedio.
- El 43.33% de **paquetes perdidos** en la PostPrueba de Ge fueron menores que la meta planteada..
- El 100% de **paquetes perdidos** en la PostPrueba de Ge fueron menores que la perdida de paquetes promedio en la PostPrueba del Gc.

4.4.2. Indicador **Número de intrusiones: I_3**

Tabla 18. *Análisis detallado de indicador número de intrusiones*

	Post-test Gc	Post-test Ge		
	13	4	4	4
	11	5	5	5
	15	3	3	3
	8	2	2	2
	10	4	4	4
	7	1	1	1
	10	4	4	4
	8	2	2	2
	13	4	4	4
	11	5	5	5
	9	3	3	3
	9	3	3	3
	5	0	0	0
	8	2	2	2
	6	0	0	0
	8	2	2	2
	12	6	6	6
	8	2	2	2
	5	0	0	0
	9	3	3	3
	7	1	1	1
	14	3	3	3
	13	7	7	7
	11	5	5	5
	15	3	3	3
	8	2	2	2
	11	5	5	5

	8	2	2	2
	10	4	4	4
	7	1	1	1
Promedio	**9.633333333**	2.933333333		
Meta Planteada			3	
N° menor a Promedio		16	13	30
%° menor a Promedio		53.33	43.33	100

- El 53.33% de los **número de intrusiones** en la PostPrueba de Ge fueron menores que el numero de intrusiones promedio.
- El 43.33% de los **número de instrusiones** en la PostPrueba de Ge fueron menores que la meta planteada..
- El 100% de los **número de intrusiones** en la PostPrueba de Ge fueron menores que el numero de intrusiones promedio en la PostPrueba del Gc.

4.4.2. Indicador **Numero de vulnerabilidades: I_4**

Tabla 19. *Análisis detallado de indicador número de vulnerabilidades*

	Post-test Gc	**Post-test Ge**		
	25	4	4	4
	22	2	5	5
	28	3	3	3
	16	2	2	2
	20	4	4	4
	14	1	1	1
	20	4	4	4
	15	2	2	2
	25	4	4	4
	22	5	5	5
	18	3	3	3
	18	3	3	3
	10	0	0	0
	15	2	2	2
	12	0	0	0
	15	2	2	2
	24	6	6	6
	16	2	2	2
	10	0	0	0
	18	3	3	3

	14	1	1	1
	28	3	3	3
	25	5	7	7
	22	3	5	5
	28	5	3	3
	16	2	2	2
	22	5	5	5
	15	2	2	2
	20	3	4	4
	14	1	1	1
Promedio	**18.9**	2.733333333		
Meta Planteada			3	
N° menor a Promedio		16	14	30
%° menor a Promedio		53.33	46.67	100

- El 53.33% del **número de vulnerabilidades** en la PostPrueba de Ge fueron menores que el numero de vulnerabilidades promedio.
- El 46.67% del **número de vulnerabilidades** en la PostPrueba de Ge fueron menores que la meta planteada..
- El 100% del **número de vulnerabilidades** en la PostPrueba de Ge fueron menores que el número de vulnerabilidades en la PostPrueba del Gc.

4.5 Contrastación de hipótesis

4.5.1. Contrastación de la H1 (I1: Tiempo de ida y vuelta)

H1: Si se diseña un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO disminuye el tiempo de ida y vuelta

Hi: El diseño de un sistema de seguridad perimetral, disminuye el tiempo de ida y vuelta (PostPrueba del Ge) con respecto a la muestra a la que no se aplicó (PostPrueba del Gc)

Se realizó una medición sin el diseño de un sistema de seguridad perimetral (PostPrueba del Gc) y otro con el diseño de un sistema de seguridad perimetral (PostPrueba del Ge)

Tabla 20. *Valores de indicador tiempo de ida y vuelta PostPrueba Ge*

PostPrueba Ge	22	21	19	21	20	25	21	24	19	21	20	22	23	21	23
	22	21	20	21	22	23	22	19	21	20	23	22	21	23	23

Tabla 21. *Valores de indicador tiempo de ida y vuelta PostPrueba Gc*

PostPrueba Gc	35	31	31	34	29	35	33	31	29	31	33	31	34	30	31
	35	38	33	34	31	37	33	38	33	39	37	33	32	35	33

a) Planteamiento de la hipótesis nula y alterna

H_0 El diseño de un sistema de seguridad perimetral, aumenta el tiempo de ida y vuelta (PostPrueba del Ge) con relación a la muestra a la que no se aplicó (PostPrueba del Gc)

H_a El diseño de un sistema de seguridad perimetral, disminuye el tiempo de ida y vuelta (PostPrueba del Ge) con relación a la muestra a la que no se aplicó (PostPrueba del Gc)

μ_1=Media poblacional del tiempo de ida y vuelta en la PostPrueba del Gc

μ_2=Media poblacional del tiempo de ida y vuelta en la PostPrueba del Ge

H_0: $\mu_1 < \mu_2$

H_a: $\mu_1 \geq \mu_2$

b) Decisión estadística basado en los resultados obtenidos de la prueba t para medias de las 02 muestras del indicador1

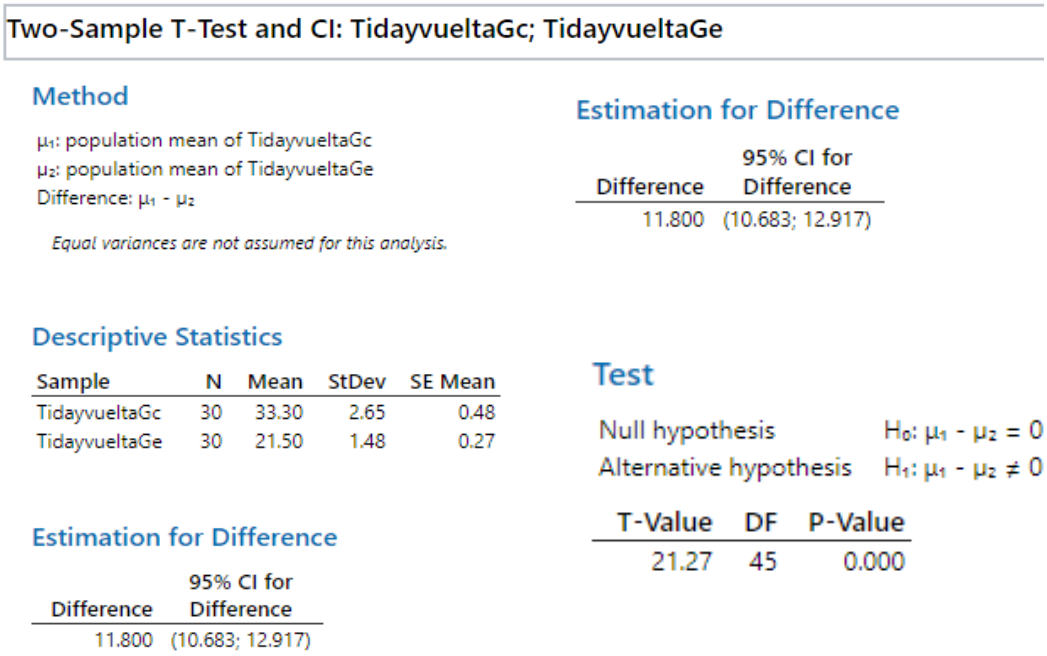

Figura 29. Prueba Two-Sample T-Test de tiempo de ida y vuelta

Debido a que el valor de p es 0.000, al ser este valor menor a 0.05, se infiere, que los resultados evidencian prueba suficiente para rechazar la hipótesis nula (Ho) y considerar la hipótesis alterna (Ha) como verdadera. Por lo que se concluye que prueba es significativa.

4.5.2. Contrastación de la H2 (I2: Perdida de paquetes)

H2: Si se diseña un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO disminuye la perdida de paquetes

Hi: El diseño de un sistema de seguridad perimetral, disminuye la perdida de paquetes (PostPrueba del Ge) con respecto a la muestra a la que no se aplicó (PostPrueba del Gc)

Se realizó una medición sin el diseño de un sistema de seguridad perimetral (PostPrueba del Gc) y otro con el diseño de un sistema de seguridad perimetral (PostPrueba del Ge)

Tabla 22. *Valores de indicador perdida de paquetes PostPrueba Ge*

PostPrueba Ge	8.5	5	10.2	7.4	8.2	5	7.5	6.2	10.5	8.5	5.6	9.5	7.6	9	8.6
	10	5.5	8	5.6	7	10	8	5	9.4	5	8.5	11	9.5	7	10

Tabla 23. *Valores de indicador perdida de paquetes PostPrueba Gc*

PostPrueba Gc	0.4	0.2	0.7	0.5	0	0.5	0.7	0.2	0.4	0	0.5	0.1	0	0.4	0.3
	0.1	0.3	0.5	0.7	0.8	0.6	0.3	0.9	0.4	0.2	0	0.6	0.4	0.6	0.2

a) Planteamiento de la hipótesis nula y alterna

H_0 El diseño de un sistema de seguridad perimetral, aumenta los paquetes perdidos (PostPrueba del Ge) con relación a la muestra a la que no se aplicó (PostPrueba del Gc)

H_a El diseño de un sistema de seguridad perimetral, disminuye los paquetes perdidos (PostPrueba del Ge) con relación a la muestra a la que no se aplicó (PostPrueba del Gc)

μ_1=Media poblacional de paquetes perdidos en la PostPrueba del Gc

μ_2=Media poblacional de paquetes perdidos en la PostPrueba del Ge

H_0: $\mu_1 < \mu_2$

H_a: $\mu_1 \geq \mu_2$

b) Decisión estadística basado en los resultados obtenidos de la prueba t para medias de las 02 muestras del indicador2

Two-Sample T-Test and CI: PerdidapaquetesgC; PerdidapaquetesGe

Method

μ_1: population mean of PerdidapaquetesgC
μ_2: population mean of PerdidapaquetesGe
Difference: $\mu_1 - \mu_2$

Equal variances are not assumed for this analysis.

Estimation for Difference

Difference	95% CI for Difference
7.510	(6.811; 8.209)

Descriptive Statistics

Sample	N	Mean	StDev	SE Mean
PerdidapaquetesgC	30	7.89	1.86	0.34
PerdidapaquetesGe	30	0.383	0.252	0.046

Test

Null hypothesis H_0: $\mu_1 - \mu_2 = 0$
Alternative hypothesis H_1: $\mu_1 - \mu_2 \neq 0$

T-Value	DF	P-Value
21.94	30	0.000

Figura 30. Prueba Two-Sample T-Test de perdida de paquetes

Debido a que el valor de p es 0.000, al ser este valor menor a 0.05, se infiere, que los resultados evidencian prueba suficiente para rechazar la hipótesis nula (Ho) y considerar la hipótesis alterna (Ha) como verdadera. Por lo que se concluye que prueba es significativa.

4.5.3. Contrastación de la H3 (I3: Número de intrusiones)

H3: Si se diseña un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO disminuye el número de intrusiones

Hi: El diseño de un sistema de seguridad perimetral, disminuye el número de intrusiones (PostPrueba del Ge) con respecto a la muestra a la que no se aplicó (PostPrueba del Gc)

Se realizó una medición sin el diseño de un sistema de seguridad perimetral (PostPrueba del Gc) y otro con el diseño de un sistema de seguridad perimetral (PostPrueba del Ge)

Tabla 24. *Valores de indicador número de intrusiones PostPrueba Gc*

PostPrueba Gc	4	5	3	2	4	1	4	2	4	5	3	3	0	2	0
	2	6	2	0	3	1	3	7	5	3	2	5	2	4	1

Tabla 25. *Valores de indicador número de intrusiones PostPrueba Ge*

PostPrueba Ge	13	11	15	8	10	7	10	8	13	11	9	9	5	8	6
	8	12	8	5	9	7	14	13	11	15	8	11	8	10	7

a) Planteamiento de la hipótesis nula y alterna

H_0 El diseño de un sistema de seguridad perimetral, aumenta el número de intrusiones (PostPrueba del Ge) con respecto a la muestra a la que no se aplicó (PostPrueba del Gc)

H_a El diseño de un sistema de seguridad perimetral, disminuye el número de intrusiones (PostPrueba del Ge) con respecto a la muestra a la que no se aplicó (PostPrueba del Gc)

μ_1=Media poblacional del número de intrusiones en la PostPrueba del Gc

μ_2=Media poblacional del número de intrusiones en la PostPrueba del Ge

H_0: $\mu_1 < \mu_2$

H_a: $\mu_1 \geq \mu_2$

b) Decisión estadística basado en los resultados obtenidos de la prueba t para medias de las 02 muestras del indicador3

Two-Sample T-Test and CI: NumintrusionesGc; NumintrusionesGe

Method

μ_1: population mean of NumintrusionesGc
μ_2: population mean of NumintrusionesGe
Difference: $\mu_1 - \mu_2$

Equal variances are not assumed for this analysis.

Estimation for Difference

Difference	95% CI for Difference
6.700	(5.495; 7.905)

Descriptive Statistics

Sample	N	Mean	StDev	SE Mean
NumintrusionesGc	30	9.63	2.76	0.50
NumintrusionesGe	30	2.93	1.78	0.32

Test

Null hypothesis	H_0: $\mu_1 - \mu_2 = 0$
Alternative hypothesis	H_1: $\mu_1 - \mu_2 \neq 0$

T-Value	DF	P-Value
11.17	49	0.000

Figura 31. Prueba Two-Sample T-Test de número de intrusiones

Debido a que el valor de p es 0.000, al ser este valor menor a 0.05, se infiere, que los resultados evidencian prueba suficiente para rechazar la hipótesis nula (Ho) y considerar la hipótesis alterna (Ha) como verdadera. Por lo que se concluye que prueba es significativa

4.5.4. Contrastación de la H4 (I4: Número de vulnerabilidades)

H4: Si se diseña un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO disminuye el número de vulnerabilidades

Hi: El diseño de un sistema de seguridad perimetral, disminuye el número de vulnerabilidades (PostPrueba del Ge) con respecto a la muestra a la que no se aplicó (PostPrueba del Gc)

Se realizó una medición sin el diseño de un sistema de seguridad perimetral (PostPrueba del Gc) y otro con el diseño de un sistema de seguridad perimetral (PostPrueba del Ge)

Tabla 26. *Valores de indicador número de vulnerabilidades PostPrueba Ge*

PostPrueba Ge	4	2	3	2	4	1	4	2	4	5	3	3	0	2	0
	2	6	2	0	3	1	3	5	3	5	2	5	2	3	1

Tabla 27. *Valores de indicador número de vulnerabilidades PostPrueba Ge*

PostPrueba Gc	25	22	28	16	20	14	20	15	25	22	18	18	10	15	12
	15	24	16	10	18	14	28	25	22	28	16	22	15	20	14

Planteamiento de la hipótesis nula y alterna

H_0 El diseño de un sistema de seguridad perimetral, aumenta el número de vulnerabilidades (PostPrueba del Ge) con respecto a la muestra a la que no se aplicó (PostPrueba del Gc)

H_a El diseño de un sistema de seguridad perimetral, disminuye el número de vulnerabilidades (PostPrueba del Ge) con respecto a la muestra a la que no se aplicó (PostPrueba del Gc)

μ_1=Media poblacional del número de vulnerabilidades en la PostPrueba del Gc

μ_2=Media poblacional del número de vulnerabilidades en la PostPrueba del Ge

H_0: $\mu_1 < \mu_2$

H_a: $\mu_1 \geq \mu_2$

b) Decisión estadística basado en los resultados obtenidos de la prueba t para medias de las 02 muestras del indicador4

Debido a que el valor de p es 0.000, al ser este valor menor a 0.05, se infiere, que los resultados evidencian prueba suficiente para rechazar la hipótesis nula (Ho) y considerar la hipótesis alterna (Ha) como verdadera. Por lo que se concluye que prueba es significativa.

Two-Sample T-Test and CI: NumvulnerabilidadesGc; NumvulnerabilidadesGe

Method

μ_1: population mean of NumvulnerabilidadesGc
μ_2: population mean of NumvulnerabilidadesGe
Difference: $\mu_1 - \mu_2$

Equal variances are not assumed for this analysis.

Descriptive Statistics

Sample	N	Mean	StDev	SE Mean
NumvulnerabilidadesGc	30	18.90	5.23	0.96
NumvulnerabilidadesGe	30	2.73	1.60	0.29

Estimation for Difference

Difference	95% CI for Difference
16.167	(14.136; 18.197)

Test

Null hypothesis H_0: $\mu_1 - \mu_2 = 0$
Alternative hypothesis H_1: $\mu_1 - \mu_2 \neq 0$

T-Value	DF	P-Value
16.18	34	0.000

Figura 32. Prueba Two-Sample T-Test de número de vulnerabilidades

V. DISCUSIÓN

Debido a las brechas existentes en cuanto a seguridad en las redes de datos, en los dispositivos que se utilizan diariamente, el avance tecnológico, las comunicaciones móviles, hacen que estos conceptos de seguridad lógica, se implanten un sistema de seguridad integro que fusione las formas de acceso tanto físicos como lógicos. Cabe resaltar que la metodología SAFE de Cisco está conformada por una estructura metodológica que permite un proceso de fácil adaptabilidad, enfocada en la escalabilidad y aseguramiento de flexibilidad en la red. Ante esto, se diseñó una solución que gestione la infraestructura de redes y comunicaciones, a través de la mejora de los siguientes indicadores:

Indicador1: Tiempo de ida y vuelta

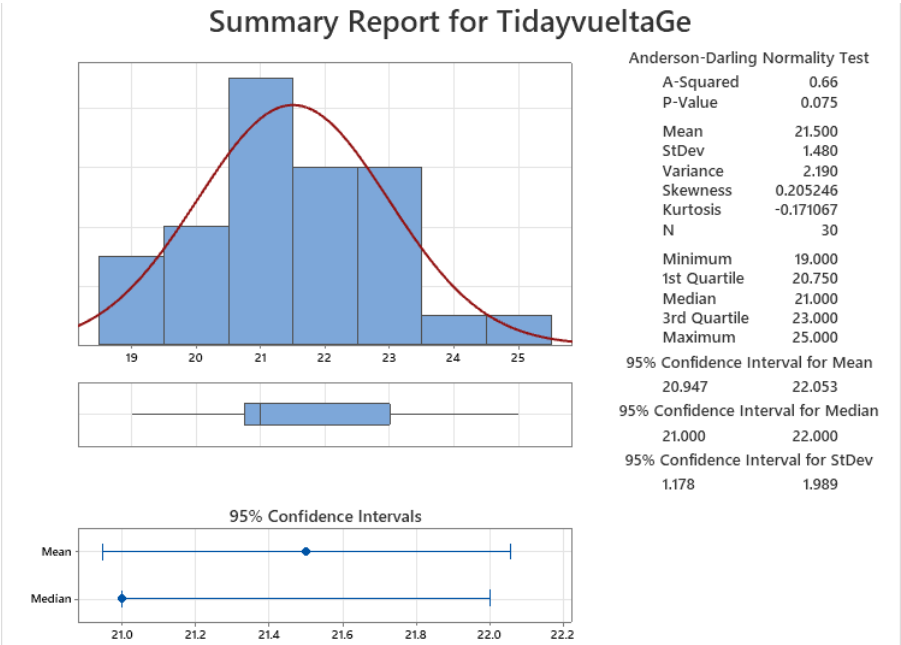

Figura 33. Informe resumido de tiempo de ida y vuelta

Los Tiempos de ida y vuelta del paquete en el grupo de experimentación fueron significativamente menores que los resultados del grupo control. Las diferencias de las observaciones individuales de los tiempos de ida y vuelta en relación a la media son 21.5 milisegundos

Aproximadamente el 95% de los tiempos de ida y vuelta caen entre la desviación estándar de 20.947 y 22.053 milisegundos.

La kurtosis=-0.17 evidencia que existen valores de tiempos con picos muy bajos

La asimetría=0.205246 indica que la mayoría de los tiempos de ida y vuelta son bajos.

El 1er Cuartil (Q1) = 20.750 milisegundos indica que el 25% de los tiempos de ida y vuelta es menor que o igual que este valor.

El 3er Cuartil (Q3) = 23.000 milisegundos indica que el 75% de los tiempos de ida y vuelta es menor que o igual que este valor.

Al ejecutar el comando ping en el CMD, el tiempo de ida y vuelta, considera el tiempo mínimo y máximo para la media, siendo estos hallazgos coherentes con la investigación de Toapanta (2019) que a pesar de que solo realiza estas pruebas hacia un servidor de la red, obtiene un valor promedio 22 milisegundos, pero con la diferencia que en esta investigación se ha ejecutado pruebas desde distintos host, diferentes vlans a los diferentes dispositivos de comunicación de la red y se obtiene un promedio significativamente inferior.

Indicador 2: Paquetes perdidos

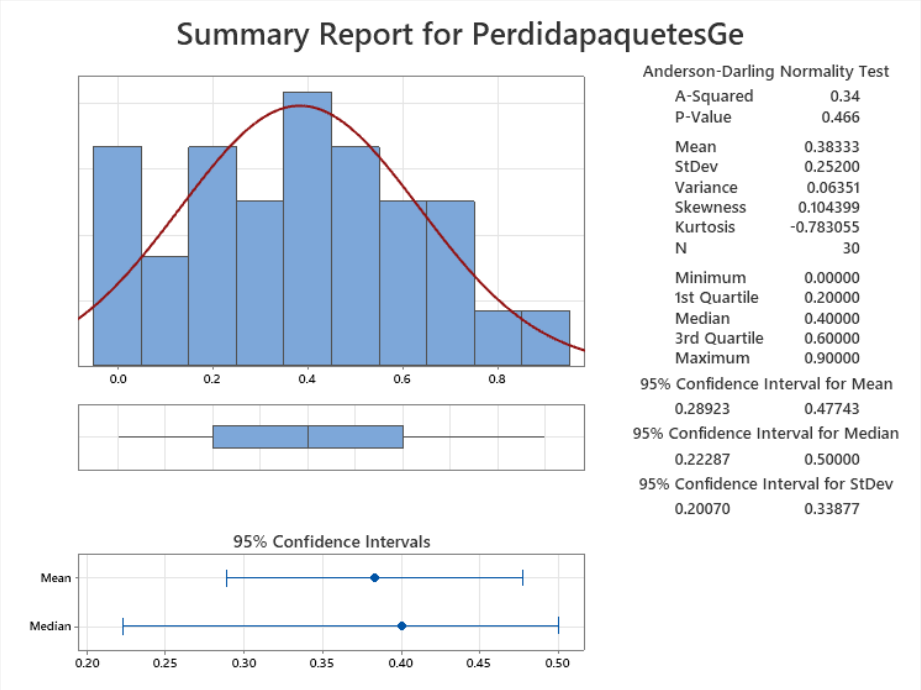

Figura 34. Prueba Two-Sample T-Test de perdida de paquetes

Los paquetes perdidos en el grupo de experimentación fueron significativamente menores a los resultados del grupo control

Las diferencias de las observaciones individuales de paquetes perdidos caen entre la desviación estándar de 0.38 paquetes

Aproximadamente el 95% de los paquetes perdidos caen entre la desviación estándar de 0.28923 y 0.47743 paquetes.

La kurtosis=-0.78 evidencia que existen valores de paquetes perdidos con picos muy bajos

La asimetría=0.104399 evidencia que la mayoría de paquetes perdidos son bajos.

El primer Cuartil (Q1) = 0.20000 evidencia que el 25% de paquetes perdida es menor que o igual que este valor.

El tercer Cuartil (Q3) = 0.60000 evidencia que el 75% de paquetes perdidos es menor que o igual que este valor.

Estos resultados son similares a lo obtenido por Pilacuán(2016) donde realiza la selección de la mejor ruta para el envío de los paquetes, considerando filtros de paquetes o firewalls y filtros basados en direcciones IP; logrando reducir la perdida de paquetes a 0%, siendo esta meta lo ideal tal como se logra en la presente investigación reducir a 0.38%, que aunque son tasas bajas se tienden a reducir a lo largo de la implantación del sistema de seguridad perimetral.

Indicador 3: Número de intrusiones

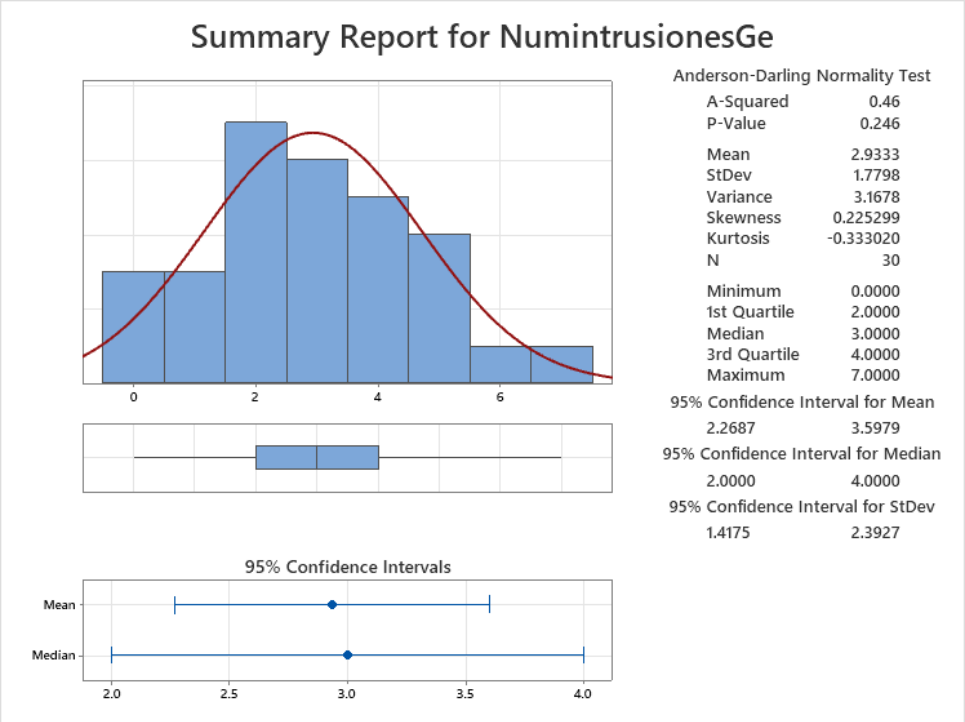

Figura 35. Prueba Two-Sample T-Test de número de intrusiones

El número de intrusiones en el grupo experimentación fue significativamente menor a los resultados del grupo control.

Las diferencias de las observaciones individuales del número de intrusiones en relación a la media fueron de 2.93 intrusiones.

Aproximadamente el 95% del número de intrusiones caen entre la desviación estándar de 2.2687 y 3.5979 milisegundos.

La kurtosis=-0.33 evidencia que existen valores de intrusiones con picos muy bajos

La asimetría=0.225299 evidencia que la mayoría del número de intrusiones son bajos.

El primer Cuartil (Q1) = 20.750 evidencia que el 25% del número de intrusiones es menor que o igual que este valor.

El tercer Cuartil (Q3) = 23.000 evidencia que el 75% del número de intrusiones es menor que o igual que este valor.

Los resultados son coherentes con lo encontrado por Toapanta (2019), pues en su investigación en la prueba de bloqueos para streaming, bloqueos por malware, bloqueos de páginas no permitidas, existen un promedio de 05 ataques controlados, el mismo que es superior al resultado de esta investigación. Asimismo, es semejante a los resultados de Ruiz Vieira, y otros (2018) que, mediante la implementación del firewall, de 152 ataques, 10 intentos fueron exitosos, lo que representa el 6.6% y 1 intento exitoso en los servicios, siendo el valor obtenido en esta investigación significativamente inferior al obtenido por el mencionado autor, reduciendo significativamente el número de intrusiones en la red.

Indicador 4: Numero de vulnerabilidades

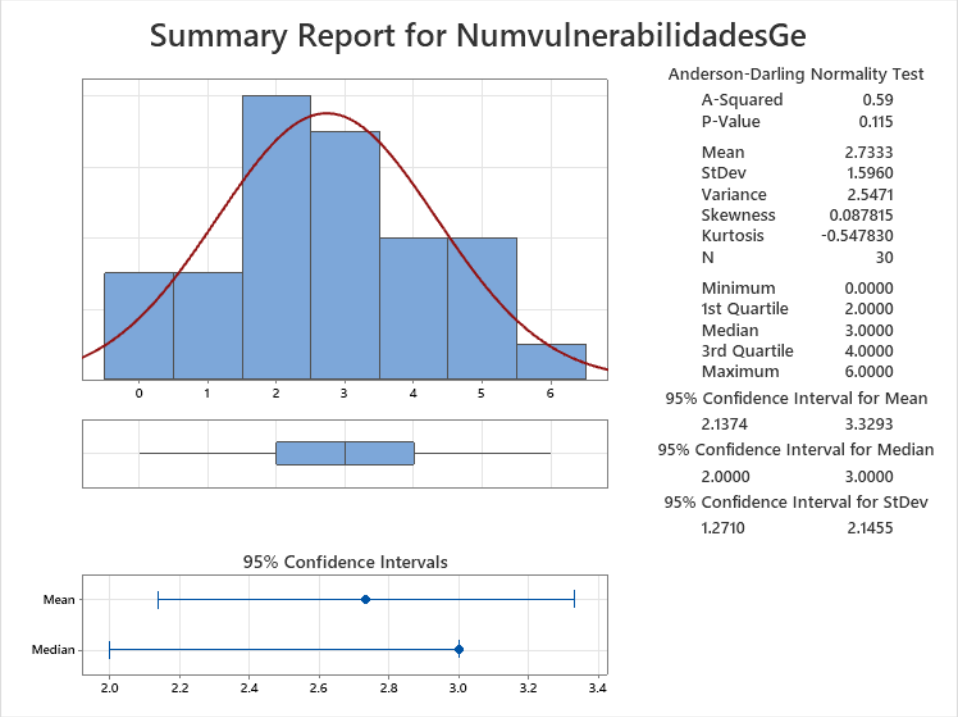

Figura 36. Prueba Two-Sample T-Test de número de vulnerabilidades

La cantidad de vulnerabilidades en el grupo de experimentación fue significativamente menor a los resultados del grupo control.

Las diferencias de las observaciones individuales del número de vulnerabilidades en relación a la media son de 21.5 veces.

Aproximadamente el 95% del número de vulnerabilidades caen entre la desviación estándar de 20.947 y 22.053 vulnerabilidades.

La kurtosis=-0.17 evidencia que existen valores de vulnerabilidades con picos muy bajos

La asimetría=0.205246 evidencia que la mayoría del número de vulnerabilidades son bajos.

El primer Cuartil (Q1) = 20.750 evidencia que el 25% número de vulnerabilidades es menor que o igual que este valor.

El tercer Cuartil (Q3) = 23.000 evidencia que el 75% del número de vulnerabilidades es menor o igual que este valor.

Estos hallazgos evidencian coherencia con el estudio de Calderón Diáz, y otros (2019) en cuanto a la seguridad de la utilización de los recursos tecnológicos, al establecer políticas de seguridad, se disminuyó el riesgo de sufrir ataques en un promedio de 5 vulnerabilidades en la red controlada mediante una honeynet, siendo este valor significativamente mayor a los resultados de esta investigación. En ese sentido se corresponde a lo obtenido por Toapanta(2019), pues mediante políticas y reglas de permisos implantados en el sistema firewall perimetral mejora la seguridad actual en lo que respecta a integridad, confidencialidad y disponibilidad, con una vulnerabilidad de 2.83 según los Check Point aplicados a la red, el mismo que es semejante a lo obtenido en la presente investigación. Finalmente concuerda con Da Silva (2016) al implementar el sistema PfSense determinó que, el promedio de vulnerabilidades sin la implementación fue de 104,6 ingresos, mientras que con la implementación fue de 3,3 con desviación estándar de 1,8 ingresos; los mismos que concuerdan con los hallazgos presentados en este indicador de la investigación.

VI. CONCLUSIONES

a) Se comprobó que un sistema de seguridad perimetral, fundamentado en el modelo SAFE de CISCO mejora la gestión de la infraestructura de redes y comunicaciones en la empresa Agrofrutos Trading S.A.
b) Se observa que un sistema de seguridad perimetral, fundamentado en el modelo SAFE de CISCO disminuye el tiempo de ida y vuelta
c) Se aprecia que un sistema de seguridad perimetral, fundamentado en el modelo SAFE de CISCO disminuye los paquetes perdidos
d) Se evidencia que un sistema de seguridad perimetral, fundamentado en el modelo SAFE de CISCO disminuye el número de intrusiones
e) Es notorio que un sistema de seguridad perimetral, fundamentado en el modelo SAFE de CISCO disminuye el número de vulnerabilidades

VII. RECOMENDACIONES

a) Se recomienda usar herramientas de monitoreo certificadas para la medición constante de los indicadores de la infraestructura de red
b) Se propone para futuras investigaciones considerar el almacenamiento dinámico para las grabaciones en los circuitos cerrados de televisión
c) Se recomienda la revisión de amenazas y vulnerabilidades a la infraestructura de la redes y comunicaciones
d) Se sugiere considerar indicadores de estados de seguridad como guías de revisión para una mejora continua

REFERENCIAS

Andres Bohorquez, Marcel y Paez Cuadros, Luis Angelo. 2017. *Diseño de un sistema de seguridad perimetral en las instalaciones del consorcio Expansión PTAR Salitre, sede Bogotá D.C.* Bogotá, Colombia : Universidad Católica de Colombia

ANTONIO ÁNGEL, RAMOS VARÓN y CARLOS A., BARBERO MUÑOZ. 2014. *Seguridad perimetral, monitorización y ataques en redes.* s.l. : RA-MA.

Arias, Fidias G. 2012. *El Proyecto de Investigación.* Caracas, Venezuela : Ediciones El Pasillo, 2012. 980-07-8529-9.

Benguría Puebla, Claudia, y otros. 2010. *Investigación: Métodos de investigación en educación especial.*.

Bolaños Botina, Jesús. 2018. *Diseño de la arquitectura de seguridad perimetral de la red informática en la industria de licores del Valle*.

Calderón Diáz, Daniel Eduardo, Tovar Semanate, Jhon Freddy y García Cuellar, Leonardo. 2019. *Sistema de seguridad perimetral en la empresa JFC Electrical Engineering S.A.S.* Colombia : Universidad Cooperativaa de Colombia.

Camacho Contreras, Andrés Fernando y López Rodríguez, John Steven. 2017. *Diseño de un sistema de seguridad perimetral e interna para la empresa Américas Business Process Services, en Bogotá D.C.* Bogotá, Colombia : s.n.

Campos Morales, Estela. 2014. *Internet y Sociedad: Relación y compromiso de beneficios colectivos e individuales.* Revista Digital Universitaria.

Castillo Palomino, Renzo Giancarlo, Dominguez Chavez, Miguel Angel y Sulca Galarza, Carlos Iván. 2017. *Implementación de un firewall TMG Forefront para la seguridad perimetral de la red de datos de la Clínica Aliada.* Lima, Perú : s.n..

Costas Santos, Jesús. 2015. *Seguridad y alta disponibilidad.* s.l. : Ra-Ma, 2015.

Defaz Calvopiña, Manuel Fernando. 2015. *La seguridad perimetral y su incidencia en la calidad de servicio de la red informática para el gobierno autónomo descentralizado de la provincia de Cotopaxi.* Ambato, Ecuador : s.n.

Delgado Zambrano, Pablo Ricardo y Loor Loor, Luis Antonio. 2017. *Sistema perimetral firewall y fortalecimiento de la seguridad en el data center de la ESPAM MFL*.

Fidias G., Arias. 2016. *El proyecto de investigación*. 7ma Edición.

Freire Aragón, Freddy Alejandro. 2018. *Análisis y propuesta de mejoramiento del sistema de seguridad perimetral aplicable a institución pública de seguridad social.* Quito, Ecuador : s.n..

Gómez Vieites, Álvaro. 2015. *Seguridad en equipos informáticos.* España : Ra-Ma.

Guevara Tinoco, Roberto Carlos y López López, Willy Lleison. 2016. *Implementación de un sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de una red informática*.

Hernández Escobar, Arturo Andrés, y otros. 2018. *Metodología de la Investigación Cinetifíca.* 2018. 978-84-948257-0-5.

Hernández Sampieri, Roberto, y otros. 2017. *Fundamenstos de Investigación.* México : Mc Graw Hill Education, 2017. 978-607-15-1395-3.

Hernández-Sampieri, R., Fernández-Collado, R. y Baptista-Lucio, P.,. 2017. *Selección de la muestra*.

Jarita, Coyla y Yony. 2019. *Implementación de un sistema de detección y prevención de intrusos (IDS/IPS), basado en la norma ISO 27001, para el monitoreo perimetral de la seguridad informática, en la red de la Universidad Peruana Unión – Filial Juliaca*.

López Paredes, Gabriela Janeth. 2015. *Sistema de seguridad perimetral para la red de datos de la industria Floralp S.A en la ciudad de Ibarra, basado en la plataforma de software libre.* Ibarra : s.n.

Manosalvas Rivas, Erick David y Rosales Garay, Julián Ramiro. 2016. *Diseño e implementación de un sistema de seguridad perimetral para la granja de la UDLA.* Ecuador : s.n..

Morales, Flavio, Toapanta, Sergio y Toasa, Renaato M. 2020. *Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información.* s.l. : Risti.

Morales, Flavio, Toapanta, Sergio y Toasa, Renato M. 2020. *Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información.* Quito, Ecuador : Universidad Tecnológica Israel.

Paredes López, Javier Paolo. 2015. *Modelo de seguridad de informática perimetral para reducir los riesgos de ataque al RENIEC*.

Pilacuán Erazo, Edgard Rubén. 2015. *Implementación de un sistema de seguridad perimetral para las empresas Teamsourcing Cia. Ltda. Con software libre (ClearOS) y desarrollo de las políticas de seguridad basadas en el estándar ISO-27001.* Sangolqui - Ecuador : s.n..

Ruiz Vieira, Kenny Esleyther y Delgado Ramos, Wilson. 2018. *Implementación de una solución de seguridad perimetral Open Source en La Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.* Chiclayo, Perú : s.n..

Silva Ledesma, Jony Rene y Da Silva de Oliveira Diaz, Renzo Giancarlos. 2016. *Efecto de la Implementación del Sistema PfSense en la Seguridad Perimetral Lógica en los Servicios de la Red Troncal de la Universidad Nacional de la Amazonía Peruana, Iquitos-2016*.

Toapanta Viracocha, Sergio Euclides. 2019. *Implementación de un sistema de seguridad perimetral para seguridad de la información de contratación pública.* Quito, Ecuador : s.n..

Torres Bolaños, Rodrigo Javier. 2015. *Seguridad Perimetral de la red de distribución de la Universidad Técnica del Norte de la ciudad de Ibarra.* Ibarra. Ecuador : s.n..

—. 2017. *Diseño de un sistema de seguridad perimetral en las instalaciones del consorcio Expansión PTAR Salitre, sede Bogotá D.C.* Colombia : Universidad Católica ade Colombia.

ANEXOS:

Anexo 1: Conformidad y aceptación del proyecto

AGROFRUTOS Trading S.A.

Sullana, 05 de Diciembre de 2020

Señor:
Dra. Lily Doris Salazar Chávez
Directora de la Escuela de Ingeniería de Sistemas
Universidad César Vallejo
PRESENTE.-

ASUNTO : **CONFORMIDAD DEL PROYECTO**

Es grato dirigirme a usted para saludarlo cordialmente en nombre de la empresa **AGROFRUTOS TRADING S.A**, que me honro en dirigir y a la vez, hacer de su conocimiento que el señor **Justiniano Tello, Eddie Armando Paul,** estudiante de la experiencia curricular de Practicas Pre Profesionales Terminales I de la carrera de **INGENIERIA DE SISTEMAS** de vuestra casa de estudios, aplicó en nuestra empresa sus conocimientos e investigaciones del caso y entre otras actividades, desarrolló el proyecto **"Implementación de un sistema de seguridad perimetral para mejorar la infraestructura de redes y comunicaciones en la empresa AGROFRUTOS TRADING S.A"**; el cual fue presentado en esta dependencia para las pruebas respectivas de su funcionamiento.

En tal sentido, hago de su conocimiento que el señor **Justiniano Tello, Eddie Armando Paul**, ha culminado satisfatoriamente su perido de prácticas pre-profesionales. Por lo que estamos ofreciendo la **CONFORMIDAD Y ACEPTACION DEL PROYECTO** desarrollado de acuerdo al compromiso definido.

Sin otro particular, quedo de ud.

Atentamente,

SILUPU MUNAR ERIC GUILLERMO
Jefe de Sistemas
Ing. Eric Silupu Munar
DEPARTAMENTO DE SISTEMAS

Anexo 2: Matriz de consistencia

PROBLEMA GENERAL	OBJETIVOS GENERAL	HIPÓTESIS GENERAL	VARIABLES	INDICADORES	TIPO DE INVESTIGACIÓN: • Aplicada NIVEL DE INVESTIGACIÓN: • Descriptiva • Experimental MÉTODOS DE INVESTIGACIÓN UNIVERSO: Todos los procesos de la gestión de Infraestructura de redes y comunicaciones de las empresas agro exportadoras.
¿En qué medida la implementación de un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO mejora la gestión de la infraestructura de redes y comunicaciones en la	Implementar un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO para la mejora de la gestión de la infraestructura de redes y comunicaciones	Si se implementa un sistema de seguridad perimetral, basado en el modelo SAFE de CISCO mejora de la gestión de la infraestructura de	**Variable Independiente** Sistema de seguridad perimetral	• Presencia_Ausencia	

empresa Agrofrutos Trading S.A.	en la empresa Agrofrutos Trading S.A.	redes y comunicaciones en la empresa Agrofrutos Trading S.A..	**Variable Dependiente** Infraestructura de redes y comunicaciones	• Tiempo de ida y vuelta • Paquetes perdidos • Número de intrusiones • Número de vulnerabilidades	**MUESTRA:** Procesos de la gestión de la Infraestructura de redes y comunicaciones de la empresa Agrofrutos Trading S.A. N=30
VARIABLES	**INDICADORES**		**ÍNDICES**	**UNIDADES DE OBSERVACIÓN**	**FÓRMULA**
Variable Independiente Sistema de seguridad perimetral	• Presencia_Ausencia		• [0-80]	Observación directa e indirecta	$\sum_1^n \text{TIV/n}$ TIV=Tiempo de ida y vuelta n= número de envíos
Variable Dependiente Infraestructura de redes y comunicaciones	• Tiempo de ida y vuelta • Paquetes perdidos • Número de intrusiones • Número de vulnerabilidades		• [0-100 • [0-100] • [0-50]		$\sum_1^n \frac{PE - PR}{n}$ PE=Paquetes enviados PR=Paquetes recibidos n= número de envíos

Anexo 3: Instrumentos

UNIVERSIDAD CÉSAR VALLEJO

Ficha de Registro 1			
Investigador	JUSTINIANO TELLO EDDIE ARMANDO PAUL	**Tipo de prueba**	**PRE / POST**
Institución	AGROFRUTOS TRADING S.A.		
Variable	INFRAESTRUCTURA DE REDES Y COMUNICACIONES		
Dimensión	DISPONIBILIDAD		
Periodo	II		

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Tiempo de ida y vuelta		Observación	Dispositivos	$\sum_{1}^{n} \text{TIV}$
				TIV=Tiempo de ida y vuelta

ÍTEM	Nombre de Host	IP de origen	Tiempo de ida y vuelta mínimo	Tiempo de ida y vuelta máximo	Media
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

UNIVERSIDAD CÉSAR VALLEJO

Ficha de Registro 2			
Investigador	JUSTINIANO TELLO EDDIE ARMANDO PAUL	**Tipo de prueba**	**PRE / POST**
Institución	AGROFRUTOS TRADING S.A.		
Variable	INFRAESTRUCTURA DE REDES Y COMUNICACIONES		
Dimensión	DISPONIBILIDAD		
Periodo	II		

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Perdida de paquetes		Observación	Dispositivos	$\sum_{1}^{n} \frac{PP}{n}$
				PP=Paquetes perdidos

ÍTEM	Nombre de Host	IP de origen	Paquetes enviados	Paquetes recibidos	% Paquetes perdidos
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

UNIVERSIDAD CÉSAR VALLEJO

Ficha de Registro 3			
Investigador	JUSTINIANO TELLO EDDIE ARMANDO PAUL	**Tipo de prueba**	**PRE / POST**
Institución	AGROFRUTOS TRADING S.A.		
Variable	INFRAESTRUCTURA DE REDES Y COMUNICACIONES		
Dimensión	EFICIENCIA		
Periodo	II		

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Tasa de transferencia		Observación	Dispositivos	$\sum_{1}^{n} \frac{AB}{T}$
				AB=Ancho de banda **T=**Tiempo

ÍTEM	Nombre de Host	IP de origen	IP de destino	Velocidad de transferencia
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

UNIVERSIDAD CÉSAR VALLEJO

Ficha de Registro 4			
Investigador	JUSTINIANO TELLO EDDIE ARMANDO PAUL	**Tipo de prueba**	**PRE / POST**
Institución	AGROFRUTOS TRADING S.A.		
Variable	INFRAESTRUCTURA DE REDES Y COMUNICACIONES		
Dimensión	RENDIMIENTO		
Periodo	II		

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Redes VLAN		Observación	Dispositivos	$\sum_{1}^{n} \frac{RV}{n}$
				RV=Redes VLAN

ÍTEM	Código de la VLAN	Nombre	Descripción	Funcionalidad
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

UNIVERSIDAD CÉSAR VALLEJO

Ficha de Registro 5			
Investigador	JUSTINIANO TELLO EDDIE ARMANDO PAUL	**Tipo de prueba**	**PRE / POST**
Institución	AGROFRUTOS TRADING S.A.		
Variable	INFRAESTRUCTURA DE REDES Y COMUNICACIONES		
Dimensión	ESCALABILIDAD		
Periodo	II		

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Nivel de escalabilidad		Observación	Dispositivos	$\sum_{1}^{n} \frac{PPC}{PPT}$
				PPS= Políticas y procedimientos cumplidos **PPT=** Políticas y procedimientos totales

ÍTEM	Código de la política / procedimiento	Nombre de la política/ procedimiento	Descripción
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

UNIVERSIDAD CÉSAR VALLEJO

Ficha de Registro 6			
Investigador	JUSTINIANO TELLO EDDIE ARMANDO PAUL	**Tipo de prueba**	**PRE / POST**
Institución	AGROFRUTOS TRADING S.A.		
Variable	INFRAESTRUCTURA DE REDES Y COMUNICACIONES		
Dimensión	FUNCIONALIDAD		
Periodo	II		

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Nivel de satisfacción		Observación	Dispositivos	$\sum_{1}^{n} \frac{RCC}{RCN}$
				RCC=Requerimientos de control cumplidos en la empresa
				RCN= Requerimientos de control de la norma

ÍTEM	Código del requerimiento	Nombre del requerimiento	Descripción
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

UNIVERSIDAD CÉSAR VALLEJO

Ficha de Registro 7			
Investigador	JUSTINIANO TELLO EDDIE ARMANDO PAUL	**Tipo de prueba**	**PRE / POST**
Institución	AGROFRUTOS TRADING S.A.		
Variable	INFRAESTRUCTURA DE REDES Y COMUNICACIONES		
Dimensión	ANALISIS		
Periodo	II		

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Cantidad de vulnerabilidades		Observación	Dispositivos	$\sum_{1}^{n} V$
				V=Vulnerabilidades

ÍTEM	Código del servicio	Nombre del servicio	Descripción
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

UNIVERSIDAD CÉSAR VALLEJO

Ficha de Registro 8			
Investigador	JUSTINIANO TELLO EDDIE ARMANDO PAUL	**Tipo de prueba**	**PRE / POST**
Institución	AGROFRUTOS TRADING S.A.		
Variable	INFRAESTRUCTURA DE REDES Y COMUNICACIONES		
Dimensión	DISEÑO		
Periodo	II		

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Nivel de cumplimiento de los Requerimientos de la empresa		Observación	Dispositivos	$\sum_{1}^{n} EM$ **RC=**Requerimientos cumplidos **RTE**=Requerimientos totales de la empresa

ÍTEM	Código del evento	Nombre del evento	Descripción del evento
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

UNIVERSIDAD CÉSAR VALLEJO

Ficha de Registro 9			
Investigador	JUSTINIANO TELLO EDDIE ARMANDO PAUL	**Tipo de prueba**	**PRE / POST**
Institución	AGROFRUTOS TRADING S.A.		
Variable	INFRAESTRUCTURA DE REDES Y COMUNICACIONES		
Dimensión	IMPLEMENTACIÓN		
Periodo	II		

Indicador	Descripción	Técnica	Unidad de Medida	Fórmula
Alertas de indisponibilidad		Observación	Dispositivos	$\sum_{1}^{n} AD$
				AD=Alertas de disponibilidad

ÍTEM	Código de la alerta	Nombre de la alerta	Descripción de la alerta
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			