UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

ESCUELA DE TECNOLOGÍA DE LA INFORMACIÓN Y LA COMUNICACIÓN

TEMA

INFRAESTRUCTURA DE RED PARA MEJORAR LA SEGURIDAD Y EFICIENCIA OPERATIVA EN LA EMPRESA "AGROQUÍMICOS SAN ANTONIO" DEL SECTOR MATA DE CACAO, Y SU IMPACTO EN LA CALIDAD DE SERVICIOS DE SUS USUARIOS

EGRESADO

ORELLANA SOUZZA ELIAS ALEXANDER

TUTOR

ING. IVÁN RUIZ PARRALES

PERIODO

ABRIL 2024 – AGOSTO 2024

DEDICATORIA

Este proyecto está dedicado a mis padres que son las personas que me impulsaron todos los días a seguir adelante, a esforzarme constantemente y a siempre mantener la motivación. A familiares y amigos cercanos que aportaron con su granito de arena en todo momento desde el inicio de mis estudios universitarios para que hoy en día este proyecto esté en su término y así lograr obtener el título tan mencionado.

Con mucho aprecio.

Elías Alexander Orellana Souzza

AGRADECIMIENTO

Mi agradecimiento primeramente va dirigido a Dios, que me dios las fuerzas para avanzar durante toda esta etapa de estudio, al ING. Jorge Isaac Souza que me permitió realizar mi proyecto dentro de su empresa con toda la comodidad y hospitalidad posible, a mi tutor, el ING. Iván Ruíz Parrales por el acompañamiento ofrecido y su colaboración durante la elaboración de mi proyecto y, a todos los demás docentes que compartieron sus conocimientos para poder convertirme en gran parte el profesional que soy ahora, en especial al ING. Carlos Soto, que siempre estuvo compartiéndonos sus experiencias, conocimientos e inspirándonos de muchas maneras a seguir adelante, por todas las charlas emotivas y las oportunidades de siempre aprender algo nuevo.

A cada uno de ustedes, mis más grandes y sinceros agradecimientos.

Autorización de la auditoría intelectual

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICACARRERA SISTEMAS DE INFORMACION

AUTORIZACION DE ACTA DE AUTORIA INTELECTUAL

Yo, **ELIAS ALEXANDER ORELLANA SOUZZA,** portador de número de cédula **120833246-8** en calidad de autor del Informe Final del Proyecto de Investigación, previo a laobtención del título de Ingeniero en Sistemas de Información, declaro ser autor del presentetrabajo de investigación, el mismo que es original y personal, con el tema:

"INFRAESTRUCTURA DE RED PARA MEJORAR LA SEGURIDAD Y EFICIENCIA OPERATIVA EN LA EMPRESA "AGROQUÍMICOS SAN ANTONIO" DEL SECTOR MATA DE CACAO, Y SU IMPACTO EN LA CALIDAD DE SERVICIOS DE SUS USUARIOS"

Por la presente autoriza a la Universidad Técnica de Babahoyo, hacer uso de todos los contenidos que me pertenecen.

ELIAS ALEXANDER ORELLANA SOUZZA

CI: 1208332468

Informe final del sistema Anti plagio

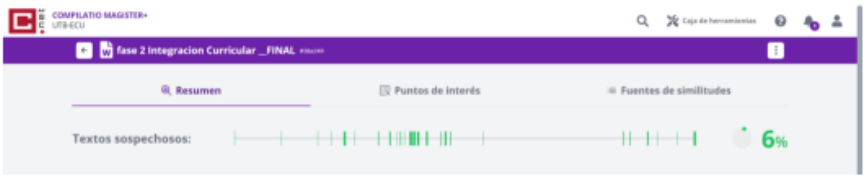
UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE INGENIERIA EN SISTEMAS DE INFORMACION

Babahoyo, 7 de agosto del 2024

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutor del Trabajo de la Investigación de: la Srta.: **ORELLANA SOUZZA ELIAS ALEXANDER**, cuyo tema es: **INFRAESTRUCTURA DE RED PARA MEJORAR LA SEGURIDAD Y EFICIENCIA OPERATIVA EN LA EMPRESA "AGROQUÍMICOS SAN ANTONIO" DEL SECTOR MATA DE CACAO, Y SU IMPACTO EN LA CALIDAD DE SERVICIOS DE SUS USUARIOS,** , certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Compilatio, obteniendo como porcentaje de similitud de **[6 %]**, resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.



Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

ING. IVAN RUIZ PARRALES, Msg
DOCENTE DE LA FAFI.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE FIGURAS

RESUMEN

En un mundo donde los avances tecnológicos son cada vez más acelerados, la seguridad de la información se ha convertido en una preocupación urgente, tanto a nivel mundial como local. En este contexto, el presente proyecto aborda el tema de las infraestructuras tecnológicas que hoy en día son importantes para todas las organizaciones sin importar el tamaño de las mismas.

El constante crecimiento de amenazas y ciberataques que ha surgido en estas áreas ha requerido soluciones que sean eficientes y se encuentren altamente preparadas para mitigar este tipo de inconvenientes que afectan de manera significativa a las empresas. Este proyecto no solo aborda conceptos teóricos sobre la seguridad, eficiencia, operatividad y riesgos, sino también sobre cómo mejorar mediante soluciones innovadoras estos inconvenientes haciendo uso de herramientas tecnológicas que posibiliten la creación de infraestructuras de red eficientes. Se toman en consideración los aspectos éticos y desafíos que conlleva el diseño de esta solución.

Está investigación contribuirá en la creación de un entorno más seguro y confiable para la empresa, generando un impacto positivo en la calidad del servicio de sus usuarios.

Palabras claves: Infraestructura de red, seguridad, riesgos, operatividad, tecnología, herramientas.

ABSTRACT

In a world where technological advances are accelerating, information security has become an urgent concern, both globally and locally. In this context, this project addresses the issue of technological infrastructures that are nowadays important for all organizations regardless of their size.

The constant growth of threats and cyber-attacks that have arisen in these areas has required solutions that are efficient and highly prepared to mitigate these types of problems that significantly affect companies. This project not only addresses theoretical concepts on security, efficiency, operability and risks, but also on how to improve these issues through innovative solutions using technological tools that enable the creation of efficient network infrastructures. The ethical aspects and challenges involved in the design of this solution are taken into consideration.

This research will contribute to the creation of a more secure and reliable environment for the company, generating a positive impact on the quality of service for its users.

Key words: Network infrastructure, security, risks, operability, technology, tools.

INTRODUCCIÓN

Las tecnologías de información y comunicación (TI) son esenciales para cualquier organización sin importar su tamaño, ya que no solo permiten la gestión eficiente de sus actividades diarias, sino que también se han convertido en un activo estratégico que impulsa la toma de decisiones y mejora la productividad. La información, es el activo más importante de cualquier empresa, y su protección al igual que su disponibilidad son cruciales para su éxito.

Hoy en día, en un mundo cada vez más interconectado, las amenazas cibernéticas se han vuelto más sofisticadas y frecuentes. Tanto a nivel internacional como nacional, el aumento de los ataques informáticos ha puesto en evidencia las vulnerabilidades que poseen gran parte de las infraestructuras tecnológicas en diferentes empresas, poniendo en riesgo datos críticos, interrumpiendo operaciones y causando pérdidas financieras que pueden ser significativas.

Por tanto, en el caso de la empresa "Agroquímicos San Antonio", ubicada en el sector Mata de Cacao, contar con una infraestructura de red eficiente y segura no solo es una necesidad operativa, sino también un factor determinante para garantizar la calidad de los servicios.

CAPÍTULO I

1. CONTEXTUALIZACIÓN PROBLEMÁTICA

1.1. Contexto internacional

A nivel internacional, el incremento de ataques informáticos se ha convertido en una preocupación central para gobiernos y empresas de todos los tamaños. La extensa capacidad de conexión ha facilitado que las amenazas cibernéticas tengan un mayor alcance, afectando a infraestructuras de manera crítica, servicios y la privacidad de la información de muchos usuarios.

1.2. Contexto nacional

En el contexto nacional, en Ecuador los ataques informáticos también han mostrado un crecimiento considerable. Según la Asociación Ecuatoriana de Ciberseguridad (AECI), durante el año 2023 hubo un incremento del 40% en incidentes de seguridad cibernética que afectaron tanto a entidades gubernamentales como a empresas privadas. Según el diario ecuatoriano “El Comercio”, la mañana del 16 de abril del 2022, la infraestructura tecnológica de la Dirección Metropolitana de Informática (DMI) del Municipio de Quito, fue objeto de un ciberataque. El origen fue un malware (software hostil intrusivo, virus informático) de tipo Ransomware la cual tuvo como consecuencia que se afectarán los servicios automatizados con los cuales la municipalidad atiende a la ciudadanía. Las pequeñas y medianas empresas (PyMEs) han sido particularmente vulnerables debido a la falta de infraestructuras de redes eficientes que implementen medidas de seguridad adecuadas para prevenir y mitigar ataques informáticos.

1.3. Contexto local

En este contexto, la empresa "Agroquímicos San Antonio" presentó un ataque informático el 5 de septiembre de 2023, debido a la deficiente infraestructura de red con la que cuenta para realizar la gestión de sus actividades, lo que dio origen a una intrusión dentro de su red, ocasionando que por medio de una ataque informático se pierda la operatividad de un servicio tecnológico que se encontraba disponible en ese instante, resultando en la pérdida de información, lo que incluía datos de clientes y registros de facturas, los cuales elementos fundamentales para la empresa.

1.4. Planteamiento del problema

¿Cómo la empresa Agroquímicos San Antonio puede prevenir fallos en su infraestructura de red asegurando la operatividad de sus servicios tecnológicos y seguridad de su información?

1.5. Justificación

La seguridad informática es esencial para todas las empresas, independientemente de su tamaño, ya que asegura la continuidad operativa y resguarda la información de posibles amenazas. Este proyecto aborda el problema identificado en la empresa "Agroquímicos San Antonio" mediante la propuesta de una infraestructura de red adecuada para mitigar intrusiones dentro de su red, asegurando la operatividad de sus servicios tecnológicos, ya que la falta de una adecuada y correcta segmentación permitió un acceso no autorizado a dispositivos que deberían ser exclusivo para la administración, lo que dio origen y facilitó un ataque informático que resultó en la detención de la operatividad de un servicio tecnológico y la pérdida de datos relevantes para la empresa, lo que incluía datos de clientes y facturas registradas. Para corregir estas vulnerabilidades y prevenir futuros incidentes, es crucial identificar la infraestructura actual, los puntos

débiles en equipos de administración, estaciones de trabajo, exposición y vulnerabilidades de los servicios disponibles y otros aspectos clave que posibiliten la acción de intrusión.

1.6. Objetivos

1.6.1. Objetivo general

Diseñar una infraestructura de red que permita mejorar la seguridad y operatividad de los servicios tecnológicos en la empresa "Agroquímicos San Antonio" del Sector Mata de Cacao.

1.6.2. Objetivos específicos

1. Identificar los activos de la infraestructura de red mediante lineamientos de control de la norma ISO/IEC 27001:2022.
2. Determinar los factores de vulnerabilidad y amenaza asociados con la infraestructura de red.
3. Realizar un plan de seguridad y medidas efectivas para mitigar el riesgo en la infraestructura de red de la empresa.

1.7. Hipótesis

Con la implementación de medidas efectivas y correctivas en la infraestructura de red en la empresa "Agroquímicos San Antonio", se disminuirá el riesgo y los accesos no autorizados, asegurando la información y la operatividad de sus servicios tecnológicos.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Antecedentes

En el estudio de Pérez et al. (2023), titulado "Impacto de la transformación digital en la cadena de suministro de la industria agroalimentaria: un estudio de caso en México", se analiza cómo la implementación de tecnologías de la información y la comunicación (TIC), incluyendo la optimización de la infraestructura de red, ha mejorado la eficiencia operativa y la trazabilidad de los productos en una empresa agroalimentaria. Los autores destacan la importancia de la conectividad y la seguridad de la red para garantizar la integridad de los datos y la continuidad de las operaciones.

Rodríguez y Gómez (2022), en su artículo "Seguridad de la información en empresas del sector agropecuario: desafíos y estrategias", examinan los principales riesgos y vulnerabilidades a los que se enfrentan las empresas agropecuarias en el ámbito de la seguridad de la información. Los autores proponen un marco de referencia para el diseño e implementación de políticas y medidas de seguridad, haciendo hincapié en la necesidad de contar con una infraestructura de red robusta y actualizada para proteger los activos de información de la empresa.

2.2. Bases teóricas

2.2.1. Redes informáticas

Estas son un conjunto de dispositivos que están conectados entre sí, los cuales crean una red y permiten que, a través de medios de transmisión y dispositivos de comunicación, los usuarios puedan establecer conexión a través de diferentes herramientas o servicios tecnológicos. Estos pueden ser un conjunto de computadoras, servidores, dispositivos móviles, entre otros, que se comunican entre sí para compartir recursos y transmitir datos. (Jiménez, 2020)

2.2.2. Tipos de redes informáticas

Las redes informáticas pueden clasificarse de varias formas, sin embargo, hay dos clasificaciones que destacan de manera importante a lo que refieren: la tecnología de transmisión y la escala. (Portal, 2022)

2.2.3. Red basada en escala

La tecnología de redes basada en escala o también conocida como basada en dispersión se refiere a la distancia a la que se encuentran los distintos nodos o redes que conecta. (Inforolot, 2021)

2.2.4. Redes LAN

Es un grupo de dispositivos que comparten una misma línea de comunicación en común o un enlace inalámbrico a un servidor dentro de una zona específica. (Hwang, 2021)

Esta se comprende en al menos dos dispositivos finales, pero también puede vincular varios dispositivos entre sí, conectar computadoras, teléfonos, impresoras, etc. (Susan, 2021)

2.2.5. Redes MAN

Una red de área metropolitana (MAN) es una red informática que conecta los ordenadores de un área metropolitana, esta misma puede ser una o varias ciudades o cualquier zona grande con varios edificios. (Perez, 2023)

2.2.6. Redes WAN

Una red de área mundial (WAN) es una red que puede ser empleada por empresas privadas, organizaciones gubernamentales o proveedores de internet para abarcar grandes distancias y soportar una enorme cantidad de tráfico o gran volumen de información. (Enríquez, 2022)

2.2.7. Infraestructura de red

Son un conjunto de recursos de hardware y software que permiten conectividad, comunicación, operaciones y la administración de una red. Esta se encuentra interconectada y puede usarse para comunicaciones, sean internas o externas, proporcionando la ruta de comunicación y servicios entre usuarios, procesos, aplicaciones, servicios y redes externas. (Eviciti, 2024)

Una infraestructura de red se encuentra conformadas principalmente por dos recursos o factores importantes:

- **Componentes físicos**

  Siendo el conjunto de hardware como computadoras, servidores, routers, centros de datos, cables y cualquier otro equipo que adopte una forma corpórea. (Aguirre, 2020)

- **Componentes lógicos**

  Siendo el conjunto de aplicaciones o programas que gestionan el hardware, permitiendo administrar los recursos de los componentes físicos de manera que

realicen la ejecución de tareas y el funcionamiento de los servicios tecnológicos. (Wrobel, 2023)

2.2.8. Puertos

Un puerto es aquel que permite la comunicación y el intercambio de datos a través de una red. Estos puertos son lógicos y se encuentran clasificados por rangos e identificadores únicos. (Jesús, 2024)

Los puertos se clasifican en diferentes tipos, tales como:

- **Puertos Bien Conocidos:** Estos puertos del 0 al 1023 se los utiliza en protocolos y aplicaciones estandarizadas.
- **Puertos Registrados:** Estos puertos del 1024 a 49151 son menos conocidos, pero están asignados para usos específicos.
- **Puertos Dinámicos o Privados:** Puerto desde 49152 a 65535 que son asignados a aplicativos de cliente cuando es necesario, lo que facilita múltiples sesiones de comunicación simultáneas.

2.2.9. Protocolos de red

Proporcionar un lenguaje común para que dispositivos pertenecientes a una red puedan transmitir información. Estas reglas incluyen pautas que regulan características como el método de acceso, topologías físicas, tipos de cableado y velocidad de transferencia de datos. (Bermúdez, 2024)

Entre los protocolos más comunes se encuentra la siguiente clasificación:

- **TCP/IP:** Es un protocolo base de la comunicación de redes encargado de la transmisión de datos y el manejo del direccionamiento y enrutamiento de los dispositivos.
- **UDP:** Es un protocolo de comunicación sin conexión que realiza el establecimiento de una sesión de comunicación antes de enviar datos.

- **HTTP/HTTPS:** Es un protocolo que hace uso del modelo de cliente-servidor para cuando los clientes realizan peticiones hacia un servidor y este proporciona una respuesta compuesta con diferentes parámetros.
- **SMTP**: Es un protocolo utilizado para el envío de correos electrónicos.
- **FTP:** Es un protocolo que se usa para la transferencia de archivos entre sistemas.
- **TLS:** Protocolos de seguridad para comunicaciones cifradas en la web.

2.2.10. Vulnerabilidad informática

Es una debilidad que puede ser explotada por medio de un ataque cibernético para obtener acceso o realizar acciones no autorizadas dentro de un sistema informático. Estas vulnerabilidades pueden permitir a los usuarios ejecutar código, acceder a la memoria de un sistema, instalar softwares, instalar malware o modificar datos confidenciales. (Aurora, 2022)

2.2.11. Tipos de vulnerabilidades

Entre las vulnerabilidades, se puede diferenciar los siguientes tipos: (Abanca, 2023)

- **Vulnerabilidades humanas**: Son realizados de manera física y ponen en riesgo la información, ya sean intencionados, por el desconocimiento o por no ser conocer el riesgo que trae realizar dichas acciones.
- **Vulnerabilidades físicas**: Originadas en el propio lugar en el que se gestiona la información, como fallas eléctricas, cables dañados, etc.
- **Vulnerabilidades del hardware**: Defectos que comprometa un dispositivo físico, sea por una mala administración o ubicación del mismo.
- **Vulnerabilidades de software**: Mal configuración, versiones viejas o usos abusivos en los recursos tras configurar mal algún programa.

2.2.12. CVE

Son una lista única de identificadores de vulnerabilidades que tiene como objetivo revelar brechas de seguridad en software y sistemas. De modo que usuarios y diferentes organizaciones o empresas puedan acceder a información adecuada y actualizada sobre las vulnerabilidades de seguridad que se presenten en su entorno. (Villanueva, 2023)

2.2.13. Amenaza

Una amenaza es la explotación de una vulnerabilidad o brechas que se utilizan para afectar la operatividad de un sistema, sea con la intención de obtener información de manera maliciosa. (Hernandez, 2022)

2.2.14. Riesgo

Es la posibilidad de que ocurra un evento no deseado, esto implica identificar, evaluar y mitigar riesgos potenciales para así minimizar la probabilidad de que se conviertan en ataques reales. (García, 2023)

2.2.15. Tipos de riesgo

Son cualquier tipo de amenazas que puedan comprometer la confidencialidad, integridad de los datos y disponibilidad de sistemas informáticos. (Toapanta, 2024)

Estos pueden estar divididos en dos tipos; riesgos físicos y riesgos lógicos, en los que:

- **Riesgos físicos:** Son eventos o circunstancias del mundo real que pueden causar algún daño a equipos, sistemas o datos, como fallas en el suministro eléctrico, desastres naturales, etc. (Jurado, 2023)
- **Riesgos lógicos:** Se originan en el software por configuraciones o el uso inadecuado de los sistemas, como virus, malware o accesos que no son autorizados. (España, 2021)

2.2.16. Seguridad de la Información

Conjunto de medidas preventivas y técnicas que se utilizan para gestionar y salvaguardar los datos que se manejan dentro de una organización y asegurar que estos no salgan del sistema establecido. (Toro, 2024)

Así mismo, se define como un conjunto de medidas y procedimientos que se aplican para proteger la confidencialidad de los datos en una empresa u organización. (Spasojevic, 2024)

2.2.17. Firewall

Es un dispositivo de seguridad que monitorea el tráfico entrante y saliente de una red y gestiona sus permisos, sea permitiendo o bloqueando tráfico específico en función al conjunto de reglas de seguridad definidas. (Albarrán, 2023)

Puede estar basado en un software o hardware que funciona como puerta de seguridad entre redes ya que logra filtrar el contenido y la comunicación que se considere dañina o potencialmente no deseada. (ESET, 2024)

2.2.18. Firewall de software

Software que se puede instalar y utilizar libremente en computadoras o dispositivos tecnológicos que los permitan. Se basa en instalaciones que permiten monitorear y bloquear el tráfico de red. (Navarro, 2023)

2.2.19. Pfsense

Es una distribución de FreeBSD creada para ser usada como sistema operativo principal de servidores o dispositivos que se desempeñen como cortafuegos, tanto como soluciones empresariales a gran escala como pequeñas. (Ashtreelane, 2024)

Este se puede emplear como solución de:

- Enrutador
- Cortafuegos

- Portal cautivo
- Servidor de servicios elementales en redes como: NTP, DHCP, Forwarder, VPN, etc.

2.2.20. Firewall de hardware

Es un dispositivo físico que protege la red de amenazas externa el cual se instala entre el punto de conexión de la institución e Internet. Se encarga de monitorear e inspeccionar y gestionar los paquetes de tráfico en base a reglas predefinidas. (Pathak, 2024)

2.2.21. Escaneo de red

Se emplea para detectar errores que tienen que remediarse para restaurar la seguridad ya que permite mapear todos los puertos y servicios que se encuentran disponibles para evitar posibles ataques o brechas de seguridad que pasan desapercibidas de otras formas. (Kullick, 2024)

2.2.22. Escaneo de puertos

Es utilizado para conocer los puertos disponibles o puntos débiles que se encuentran en una red debido a que, por medio de esto, usuarios malintencionados pueden interceptar datos que se transmiten y capturar la información. (Ahijon, 2023)

Esto puede proporcionar información como:

- Servicios que se están ejecutando
- Usuarios que poseen servicios
- Si se permiten inicios de sesión anónimos
- Servicios de red requieren autenticación

2.2.23. Herramientas de escaneo de red

Son aplicaciones que pueden descubrir fallos en la red y protegerla de comportamientos que amenazan a los sistemas. (Lorenzo Williams, 2024)

Se utiliza para analizar y evaluar un dispositivo, red o aplicación para detectar vulnerabilidades y amenazas conocidas. (Nicole, 2024)

2.2.24. NMAP

Es un software utilizado para realizar escaneo de una red y sus puertos con el objetivo de obtener información sobre la misma, con el fin de controlar y gestionar su seguridad. (Abrie, 2022)

Permite realizar actividades como mapeo para identificar los diferentes componentes físicos y lógicos que se encuentran funcionando dentro de ella, servicios en ejecución con sus versiones, vulnerabilidades y sistemas operativos en los que se ejecutan.

2.2.25. Nessus

Es un escáner de vulnerabilidades de red que se diseñó para identificar y resolver brechas de seguridad con el fin de proteger a la información, procesos y servicios contra diferentes riesgos de seguridad. Entre las principales funciones se encuentra el descubrimiento de activos, escaneo web, priorización y evaluación de vulnerabilidades. (Sepulveda, 2023)

2.2.26. Wireshark

Proporciona la visibilidad del tráfico que se realiza en una determinada red o dispositivos, permitiendo examinar diferentes detalles de tráfico a varios niveles: desde el nivel de la conexión hasta los bits que conforman a un paquete y los datos que contiene. (Abba, 2023)

2.2.27. Servicio tecnológico

Son aquellos que facilitan las tareas de los usuarios en todo tipo de entornos, desde las herramientas tecnológicas hasta las aplicaciones, programas y softwares de todo tipo que permiten realizar tareas de gestión a través de los datos. (Rojas, 2024)

Entre ellos se puede encontrar servicios tecnológicos cómo:

- **Servicios en la nube:** Permiten a empresas u organizaciones almacenar datos y aplicaciones en línea, sin la necesidad de contar con algún servidor físico dentro de sus instalaciones.
- **Servicios de seguridad informática:** Se encuentran enfocados en la seguridad de tal manera que resguardan a las empresas y usuarios de una gran variedad de amenazas en línea, como lo son virus, malware o ataques cibernéticos.
- **Servicios de software:** Se encuentran encargados de proporcionar aplicaciones que son empleadas y aplicadas por personas o individuos para con el fin de ejecutar determinadas tareas.

2.2.28. Virus informático

Son diseñados con la intención de infiltrarse en un ordenador sin el permiso del usuario, teniendo la capacidad de auto replicarse, de tal manera que obtiene el acceso para realizar copias de sí mismo y se adhiere a otros archivos o documentos. (Latto, 2022)

2.2.29. Tipos de virus informáticos

Tienen como finalidad infectar, interferir o interrumpir servicios u operaciones que se realizan o ejecutan a través de un conjunto de elementos conectados entre sí. (Gonzalez, 2023)

Entre los tipos de virus informáticos más conocidos se encuentran:

- **Spyware:** Es un programa espía cuyo objetivo es robar toda la información de un ordenador.
- **Ransomware:** Es un tipo de software malintencionado o malware que amenaza a una víctima con destruir o bloquear el acceso a sistemas o datos críticos.

- **Troyanos:** Son un tipo de malware que, para lograr infectar un equipo, se camufla como un software legítimo para acceder a los sistemas de los usuarios de manera no autorizada.

2.2.30. Norma ISO

Son un conjunto de reglas y estándares que proporcionan a las empresas u organizaciones un conjunto de procedimientos para que se realice una gestión adecuada en todos sus ámbitos. Componen de guías relacionadas con sistemas y herramientas específicas de gestión aplicables en cualquier tipo de organización. (Rodríguez, 2023)

2.2.31. Controles

Son medidas que las organizaciones deben considerar y tomar a través de políticas, procesos y procedimientos para cumplir con requisitos de seguridad estandarizados. (Manuel, 2023)

2.2.32. CID

Es un modelo que constituye bases para el desarrollo de sistemas de seguridad, utilizado para encontrar vulnerabilidades y métodos para crear soluciones, siendo crucial para la operación de un negocio porque ayuda a guiar a los equipos y otros recursos a aplicar medidas de seguridad. (Stic, 2023)

Esta se encuentra conformada por:

- **Confidencialidad (C)**: Garantiza que la información solo sea accesible para personas autorizadas.

Tabla 1

Confidencialidad

Confidencialidad	Criterio
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la institución.

Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución.
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución.

Fuente: *Autor.*

- **Integridad (I)**: Asegura que la información sea precisa y confiable, y que no haya sido modificada o alterada sin autorización.

Tabla 2

Integridad

Integridad	Criterio
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución.
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución.
Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución.

Fuente: *Autor.*

- **Disponibilidad (D)**: Garantiza que la información esté disponible y accesible cuando sea necesario para usuarios autorizados.

Tabla 3

Disponibilidad

Disponibilidad	Criterio
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución.
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
Bajo (1)	La interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

Fuente: *Autor.*

2.2.33. Plan de seguridad

Detalla un conjunto de medidas y procedimientos que se deben seguir para proteger los activos, sean físicos o lógicos de una organización, cumpliendo con los requisitos de seguridad establecidos. Debe estar claramente vinculado a los procedimientos de trabajo relacionados con la seguridad de los activos. (It, 2024)

2.2.34. Virtualización

Permite la creación de múltiples entornos virtuales simulados o recursos dedicados a partir de un único sistema de hardware físico disponible, distribuyendo las cargas de trabajo entre varias máquinas, maximizando así la eficiencia y reduciendo los costos de aplicación. (Muñoz, 2024)

2.2.35. Entorno virtual

Es una tecnología que permite la capacidad de crear múltiples sistemas operativos y aplicaciones independientes en un solo ordenador físico. Este se comporta como un ordenador independiente, con su propio sistema operativo, aplicaciones y recursos asignados. (León, 2020)

2.2.36. Máquinas virtuales

Es un software que simula un sistema y que permite ejecutar programas o servicios como si fuera un ordenador real, lo que permite que varias máquinas virtuales puedan llegar a ejecutarse simultáneamente en un solo equipo físico. (Arsys, 2024)

2.2.37. EVE-NG

Es un entorno de virtualización que permite crear topologías de redes complejas y realistas para fines de pruebas y desarrollo. Cuenta con una plataforma flexible y escalable para simular diferentes dispositivos de red, sistemas operativos y protocolos, asegurando un entorno seguro y controlado, además de permitir la exportación de configuraciones realizadas y establecidas dentro del entorno para su implementación en otro dispositivo. (César, 2021)

Entre las principales características se encuentra:

- Aceleración de hardware KVM.
- Diseñador de topología.
- Configuración de importación y exportación de configuraciones.

- Formato de archivo XML de laboratorios.
- Importación de imágenes y mapas.
- Soporte de kernel personalizado para protocolos L2.
- Optimización de memoria (UKSM).
- Monitoreo de la CPU.
- Interfaz de usuario HTML5 completa.
- Capacidad de uso sin herramientas adicionales.
- Multiusuarios.
- Interacción con red real totalmente compatible.
- Instancias de laboratorio simultáneas.
- Derivado del servidor Ubuntu LTS 20.04 para soporte a largo plazo.

CAPÍTULO III

3. Metodología

3.1. Tipo y diseño de la investigación

Según el nivel de estudio:

Aplicada

La investigación aplicada se encuentra enfocada en utilizar el conocimiento científico para resolver problemas específicos o concretos y mejorar situaciones actuales, buscando aplicar resultados de investigación para desarrollar soluciones prácticas en diferentes campos como lo es la medicina, la ingeniería y la agricultura (Ortega, 2024)

Según el lugar:

Bibliográfica

Es un proceso organizado y sistemático que implica la búsqueda, selección y evaluación de información relevante que se encuentre sobre un tema específico, con el fin de adquirir un conocimiento profundo y actualizado sobre sobre el mismo. (Zorrilla, 2023)

La investigación bibliográfica es una técnica de investigación en la que se explora lo que se ha escrito y publicado antes acerca un determinado tema. (Parrales, 2023)

Según el método:

Método cualitativo

Es un método para recopilar y evaluar datos no estandarizados. Se emplea una muestra pequeña y no representativa para comprender más profundamente los criterios de decisiones. (Qualtrics, 2023)

Así mismo, es un proceso que permite extraer conclusiones de datos no estructurados y heterogéneos que no se expresan de manera numérica o cuantificable. (Ekon, 2023)

Método cuantitativo

Se basa en la recolección y el análisis de datos para responder preguntas de investigación y probar hipótesis establecidas previamente, utilizando la medición numérica, el conteo y frecuentemente el uso de estadísticas para determinar patrones de comportamiento en una población. (Canive, 2020)

Este método, se dedica a la recopilación y análisis sistemáticos de datos, utilizando técnicas estadísticas para extraer conclusiones de diferentes instrumentos de recolección de información. (Alam, 2023)

3.2. Operacionalización de las variables

Tabla 4

Operacionalización de las variables

	Variables	**Definición conceptual**	**Definición operacional**	**Dimensión**	**Indicadores**	**Escala de Medición**	**Instrumentos**
V. Dependiente	Seguridad	Conjunto de procedimientos y herramientas de seguridad que protegen la información confidencial de la empresa frente al uso indebido, acceso no autorizado o intrusiones, interrupción o destrucción.	Nivel de protección de los activos de información de la empresa.	Escaneo de vulnerabilidades	Vulnerabilidades de servicio Vulnerabilidad de hardware CVE Nivel de vulnerabilidad	Escala de razón	Herramientas de escaneo de vulnerabilidades Tablas de datos estructurada
				Riesgo de operatividad tecnológica	Confidencialidad. Integridad. Disponibilidad. Amenaza. Vulnerabilidad.	Escala nominal	Matriz de valoración de activo. Tablas de datos estructuradas.
	Eficiencia operativa	Capacidad de los servicios para funcionar de manera	Los servicios responden correctamente a las	Disponibilidad	Tiempo de actividad Tiempo de inactividad	Escala de nominal	Tablas de datos estructurada

		correcta y sin interrupciones.	peticiones de los usuarios internos.				
	Impacto de los usuarios	Se refiere al efecto de experimentación que tienen los usuarios de un sistema, servicio o producto en su entorno o contexto específico.	Grado de satisfacción y percepción de los usuarios sobre la calidad y eficiencia de los servicios tecnológicos.	Tiempo de respuesta Seguridad Eficiencia	Calidad del Servicio. Grado de satisfacción. Eficiencia del Servicio.	Escala Likert	Encuesta a los miembros de la empresa.
V. Independiente	Empresa Agroquímicos “San Antonio”	Empresa dedicada a la compra y venta de insumos agrícolas al por mayor y menor.	Empresa dedicada a la compra y venta de insumos agrícolas, con ofrecimiento crediticio a sus clientes.	Empresa	Empleados	Escala nominal	Entrevista estructura a miembros de la empresa con conocimientos en el área
	Infraestructura de red	Conjunto organizado y estructurado de elementos físicos y lógicos que permiten la comunicación y transferencia de datos dentro de una empresa.	Componentes físicos y lógicos de la red, que posibilitan las actividades de la empresa.	Componentes físicos Componentes lógicos	Topología de la red. Dispositivos en la red. Servicios tecnológicos.	Escala nominal	Escaneo de red.

Fuente: *Autor*.

3.3. Población y muestra de la investigación

3.3.1. Población

Representante y personal de la empresa con conocimiento en el área (3 personas).

3.3.2. Muestra

Debido a que la población es pequeña y específica a un grupo de personas, toda la población será la muestra.

3.4. Técnicas e instrumentos de medición

3.4.1. Técnicas

Entrevista

Se emplea la entrevista como técnica de recolección de información cualitativa para conocer en detalle los problemas y carencias de seguridad presentados en la empresa.

Encuesta

Se emplea el uso de la encuesta como técnica para la recolección de información cuantitativa respecto a la satisfacción y calidad de la nueva infraestructura.

3.4.2. Instrumentos

Cuestionario

En el caso de la entrevista, se diseña un cuestionario con preguntas estructuradas para obtener datos cualitativos de los miembros de la empresa.

En el caso de la encuesta, se diseña un cuestionario con preguntas basadas en la escala de Likert para conocer el grado de satisfacción referente a los aspectos de seguridad y calidad en respuesta a la infraestructura tecnológica.

Herramienta de escaneo de red

Se emplea para analizar y mapear los dispositivos presentes en la infraestructura de red de Agroquímicos “San Antonio”, lo que permite identificar todos los equipos conectados, sistemas operativos y servicios instalados. Se usa la herramienta de mapeo NMAP para efectuar un análisis a la red e identificar los activos que posee, tanto de hardware como de software, representándose de la siguiente manera:

Identificación de activos de la infraestructura de red

Tabla 5

Identificación de activos de la infraestructura de red según consideración de la Norma ISO 27001:2022 Controles del Anexo A.8.

N° Activo	Nombre de activo	Descripción del activo	Sistema involucrado	Tipo de activo	Tipo de ubicación	Propietario del activo
1°				Software	Física	
				Físico		
				Personas	Lógica	
				Servicios		

Fuente: *Autor*.

Valoración de activos

La valoración de activos (CID) se emplea para conocer el valor de los activos, lo cual permite tomar decisiones sobre su protección y manera de gestionarlos.

Identificación del valor del activo mediante CID

Tabla 6

Valoración de valor de activo según Norma ISO 27001:2022 Controles del Anexo A.8.

N° Activo	Nombre de activo	C	I	D	VA	Nivel de tasación

Fuentes: *Autor.*

Haciendo uso de la siguiente fórmula:

$$Valor\ Activo\ (VA) = Confidencialidad\ (C) * Integridad\ (I) *\ Disponibilidad\ (D)$$

Herramienta de escaneo de vulnerabilidades

La herramienta de escaneo de vulnerabilidades se emplea para identificar puntos débiles que puedan ser vulnerables o brechas de seguridad en la infraestructura de red de la empresa. Se usa la herramienta Nessus para escanear la red de manera que realice una búsqueda completa e identifique vulnerabilidades de componentes lógicos.

Identificación de vulnerabilidades de componentes físicos y lógicos de la infraestructura de red.

Tabla 7

Identificación de vulnerabilidades.

Tipo de vulnerabilidad	N° Activo	Nombre de activo	CVE	Vulnerabilidad	Amenaza	Nivel de vulnerabilidad (1-10)
Lógica						
Número de vulnerabilidades						

Fuente: *Autor.*

Elaboración de plan de seguridad y medidas para mitigar riesgo de la información.

Tabla 8

Plan de Seguridad y Medidas para mitigar el riesgo de la información basado en Norma ISO 27001:2022

1. **Contexto de la Organización** Detalla el contexto de la organización o empresa.
2. Objetivo Detalla el objetivo del plan
3. **Medidas de Control** Describe las medidas técnicas y organizativas para proteger la infraestructura de red.
4. Políticas de Seguridad Establece las reglas y directrices que rigen el uso de los recursos.
5. Plan de Respuesta a Incidentes Establece los procedimientos para detectar y responder incidentes. (firewall, bloqueo de IP)
6. Monitoreo y Revisión Detalla los mecanismos de monitoreo continuo de la seguridad de la red. (Análisis de los recursos del servidor y tráfico)
7. Formación y Concienciación del Personal Describe las acciones para capacitar al personal en materia de seguridad de la información. (Recomendaciones de capacitaciones)

Fuente: *Autor.*

Se determina un plan de seguridad y medidas efectivas para asegurar la infraestructura de red a través de un enfoque que abarque capas de seguridad y se emplee buenas prácticas para reducir el riesgo a incidentes no deseados.

EVE-NG

Se usa la plataforma de EVE-NG de manera virtualizada por medio del software de VMWare para crear un laboratorio virtual donde se diseña la infraestructura de red en base a consideraciones de mejoras de la infraestructura de red actual, se usa distintos softwares de sistemas operativos de estaciones de trabajo, de servidores, de firewalls, entre otros.

- Se realiza la instalación de EVE-NG en un equipo tecnológico dedicado, configurado para soportar la simulación de la infraestructura de red.
- Se cargan imágenes como Routers, Switches, Firewalls y sistemas operativos basadas en los componentes de mejoras de la infraestructura de red actualmente.
- Se diseña la nueva infraestructura de red asegurando el uso correcto de los componentes lógicos que proporcionan un mayor nivel de seguridad.
- Se realizan pruebas de la accesibilidad por los usuarios de la empresa para prevenir los accesos no autorizados.

3.5. Procesamiento de datos

El procesamiento de datos se realiza en varias etapas, utilizando tanto el método cualitativo como cuantitativo para analizar la información recopilada a través de entrevistas y encuestas. En primer lugar, se transcribe la entrevista realizada a personal y representante de la empresa Agroquímicos “San Antonio”, convirtiendo las grabaciones en texto para facilitar su análisis. Luego, se exportan los datos recopilados a través de la encuesta en línea que serán realizadas con Google Forms a una hoja de cálculo de Excel para llevar a cabo una limpieza de los datos. Se corrigen errores de transcripción, se eliminan datos incompletos o inconsistentes para garantizar la calidad y coherencia de la información.

3.6. Aspectos éticos

Se garantiza la privacidad y confidencialidad de los datos obtenidos, asegurando un manejo y uso adecuado de la información sensible y evitando su divulgación sin autorización expresa de los participantes.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Resultados

Durante las entrevistas dirigidas hacia personal seleccionado y representante de la empresa se obtuvieron las siguientes respuestas:

Tabla 9

Preguntas de entrevista dirigida hacia el representante de la empresa.

Nro.	Preguntas	Respuestas
1	¿Cómo podría describir el impacto que tuvo el problema de seguridad presentado en la empresa?	"Como algo a considerar debido a que por faltas de seguridad, se llevó a cabo la realización de aquella acción de manera indirecta."
2	¿Qué tipo de información se vio comprometida durante el ataque informático que presentó la empresa?	"No era ningún tipo de información que podría poner en exposición datos importantes de los clientes, solo fueron algunas facturas antiguas y algunos registros, nada comprometedor."
3	¿Qué medidas de seguridad considera que se deberían aplicar para proteger la información de la empresa?	"Considero que tras el problema que se presentó, es esencial mejorar la seguridad de la red."
4	¿Considera usted la posibilidad de que sucedan futuros ataques informáticos como el ya experimentado?	"Si no se aplican medidas de seguridad que impidan efectuar nuevamente lo mismo, es probable."

Fuente: *Autor*.

Tabla 10

Preguntas de entrevista dirigida hacia personal con conocimientos sobre el área de la empresa.

Nro.	Preguntas	Respuestas	Responsable
1	¿Cuáles son los problemas que se presentaron en su trabajo durante el incidente informático?	"La interrupción de algunos servicios porque no respondían a las peticiones que se les realizaba."	Sistemas
		"Se interrumpieron servicios y funciones de las que se requería para el funcionamiento de otros sistemas."	
2	¿Qué tipo de información de la que hace uso durante su trabajo se vio afectada por el incidente presentado en la empresa?	"Información que provenía de otros servicios, no respondían a las peticiones, por lo tanto no se podían visualizar."	Sistemas
		"Información de la que dependía otra."	
3	¿Cuánto tiempo cree que se perdió debido a la interrupción de los servicios causada por el incidente informático?	"Fueron algunas horas de inactividad porque no podíamos establecer conexión."	Sistemas
		"Fue un par de horas, no se podía realizar acceso por la inactividad."	
4	¿Cree que la falta de aplicar medidas de seguridad hacia la red o establecer configuraciones inadecuadas en los dispositivos contribuyeron en la posibilidad del incidente informático?	"Sí, la red de la empresa no cuenta con una segmentación muy adecuada por lo que posiblemente fue lo que en gran parte posibilitó que se manifestara aquel incidente."	Sistemas
		"Sí, hace falta aplicar algunas medidas de seguridad en los dispositivos y la red."	
5	¿Qué medidas de seguridad cree que serían necesarias para proteger la red de la empresa y prevenir futuros incidentes como el ya experimentado?	"Las medidas de seguridad que considero necesarias aplicar son firewall, con reglas que ayuden a filtrar contenidos o host no deseados y políticas para mantener segura la información de las sesiones de los demás compañeros de trabajo."	Sistemas

		"Medidas como sesiones, segmentación y control de accesos."

Fuente: *Autor*.

Empleando la herramienta de escaneo en la infraestructura de red de la empresa, se obtuvo el siguiente resultado:

Tabla 10

Resultado de inventario de activos

N° Activo	Nombre de activo	Descripción del activo	Sistema involucrado	Tipo de activo	Tipo de ubicación	Propietario del activo
1.	VMware	Máquina virtual	Red interna	Software	Lógico	Empresa
2°	Dell-1	Servidor	Red interna	Físico	Físico	Empresa
3°	Dell-2	Estación de trabajo	Red interna	Físico	Físico	Empresa
4°	Dell-3	Estación de trabajo	Red interna	Físico	Físico	Empresa
5°	Dell-4	Estación de trabajo	Red interna	Físico	Físico	Empresa
6°	Dell-5	Estación de trabajo	Red interna	Físico	Físico	Empresa
7°	TP-LINK	Switch	Red interna	Físico	Físico	Empresa
8°	ESP_ECCC 8E	Impresora	Red interna	Físico	Físico	Empresa
9°	FN-Link-1	Cámara IP	Red interna	Físico	Físico	Empresa
10°	FN-Link-2	Cámara IP	Red interna	Físico	Físico	Empresa
11°	FN-Link-3	Cámara IP	Red interna	Físico	Físico	Empresa
12°	HTTP	Servicio web	Red interna	Servicios	Lógica	Empresa

13°	HTTPS	Servicio web seguro	Red interna	Servicios	Lógica	Empresa
14°	MSRPC	Servicio de Microsoft RPC	Red interna	Servicios	Lógica	Empresa
15°	Microsoft-DS	Servicio de Microsoft	Red interna	Servicios	Lógica	Empresa
16°	NetBIOS-SSN	Servicio NetBIOS	Red interna	Servicios	Lógica	Empresa
17°	WSDAPI	Servicio de dispositivos web	Red interna	Servicios	Lógica	Empresa
18°	IRC	Servicio de chat IRC	Red interna	Servicios	Lógica	Empresa
19°	Zebra	Servicio Zebra	Red interna	Servicios	Lógica	Empresa
20°	Windows SMB	Servicio de Windows	Red interna	Servicios	Lógica	Empresa

Fuente. *Autor*.

Obtenido el inventario de activos y aplicando la valoración de activos a cada uno de ellos se obtuvo el siguiente resultado:

Tabla 11

Resultado de valoración de activos

N° Activo	Nombre de activo	C	I	D	VA	Nivel de tasación
1°	VMware	3	3	3	27	Crítico
2°	Dell-1	2	2	2	8	Medio
3°	Dell-2	2	2	2	8	Medio
4°	Dell-3	2	1	2	4	Medio
5°	Dell-4	2	1	2	4	Medio
6°	Dell-5	2	2	2	8	Medio
7°	TP-LINK	3	3	3	27	Crítico

8°	ESP_ECCC8E	1	1	2	2	Bajo
9°	FN-Link-1	2	2	2	8	Medio
10°	FN-Link-2	2	2	2	8	Medio
11°	FN-Link-3	2	2	2	8	Medio
12°	HTTP	2	2	2	8	Medio
13°	HTTPS	2	2	2	8	Medio
14°	MSRPC	2	2	2	8	Medio
15°	Microsoft-DS	3	3	3	27	Crítico
16°	NetBIOS-SSN	3	3	3	27	Crítico
17°	WSDAPI	2	2	2	8	Medio
18°	IRC	2	2	2	8	Medio
19°	Zebra	2	2	2	8	Medio
20°	Windows SMB	2	2	3	12	Alto

Fuente. *Autor*.

Obtenida la valoración de activos y aplicando el análisis de vulnerabilidades a los activos lógicos, se obtuvo el siguiente resultado:

Tabla 12

Resultado de identificación de vulnerabilidades.

Tipo de vulnerabilidad	**N° Activo**	**Nombre de activo**	**CVE**	**Vulnerabilidad**	**Amenaza**	**Nivel de vulnerabilidad (0-10)**
Lógica	1°	VMware	CVE-2021-21994	Omisión de autenticación	Control completo del sistema ESXi afectado.	10
			CVE-2021-21995	Acceso OpenSLP en VMware ESXi	Lectura en el servicio OpenSLP y ataque de denegación de servicio (DoS)	7
	12°	HTTP	Ninguna	Ninguna	Ninguna	0
	13°	HTTPS	Ninguna	Ninguna	Ninguna	0

	14°	MSRPC	Ninguna	Ninguna	Ninguna	0
	15°	Microsoft-DNS	CVE-2022-21984	Desbordamiento de búfer basado en pila	Uso del servidor para lanzar ataques a otros sistemas en la red.	7
	16°	NetBIOS-SSN	CVE-2017-0161	Ejecución remota de código (RCE)	Control total del sistema afectado.	7
	17°	WSDAPI	Ninguna	Ninguna	Ninguna	0
	18°	IRC	Ninguna	Ninguna	Ninguna	0
	19°	Zebra	Ninguna	Ninguna	Ninguna	0
	20°	Windows SMB	CVE-2022-24500	Ejecución remota de código (RCE)	Control total del sistema afectado.	8
Número de vulnerabilidades					4	

Fuente. *Autor.*

Tomando puntos claves de la seguridad informática, se obtiene como resultado un plan de seguridad y medidas efectivas que ayuda a prevenir posibles incidentes de seguridad en la infraestructura de la empresa.

Tabla 13

Resultado de plan de seguridad y medidas para mitigar riesgos.

1. **Contexto de la Organización** **Nombre de la institución:** Agroquímicos “San Antonio” **Representante legal:** Ing. Jorge Isaac Souza Orellana.
2. Objetivo Estructurar un plan de seguridad y medidas efectivas que contribuya a la mejora de la seguridad de la infraestructura de red en la empresa Agroquímicos “San Antonio”.
3. **Medidas de Control** **Medidas técnicas**

- **Firewall:** Aplicar un firewall para controlar el tráfico entrante y saliente de la infraestructura, bloqueando a accesos no autorizados en la red.
- **Portal cautivo:** Aplicar un portal cautivo para mantener el acceso de los dispositivos a la red y puedan hacer consumo de paquetes en sesiones específicas
- **Cierre de sesión por inactividad:** Aplicar medidas o reglas que desconecten a usuarios de la red por tiempo de inactividad.
- **Segmento de red:** Aplicar segmentación adecuada a la red para gestionar el tráfico entre los dispositivos administrativos.

Medidas Organizativas

- **Autorías:** Realizar auditorías internas de forma periódica para verificar el cumplimiento de las políticas de seguridad..

4. Políticas de Seguridad

- **Políticas de contraseñas:** Establecer contraseñas seguras de 8 dígitos que incluyan caracteres especiales, mayúsculas, minúsculas y números.
- **Sesiones de usuarios:** Realizar el cierre de sesión de la estación de trabajo en el tiempo que no se la utilice.
- **Políticas para conectividad de dispositivos externos a la red:** Establecer una cantidad máxima de conectividad a dispositivos que no pertenezcan a la red.

5. Plan de Respuesta a Incidentes

- **Análisis de tráfico:** Efectuar medidas de seguridad que bloqueen las direcciones de dispositivos que realicen tráfico no deseado.

6. Monitoreo y Revisión

- **Análisis de logs:** Aplicar análisis a la red por medio de los logs o registros que se realizan para identificar acciones o tráfico sospechoso.

7. Formación y Concienciación del Personal

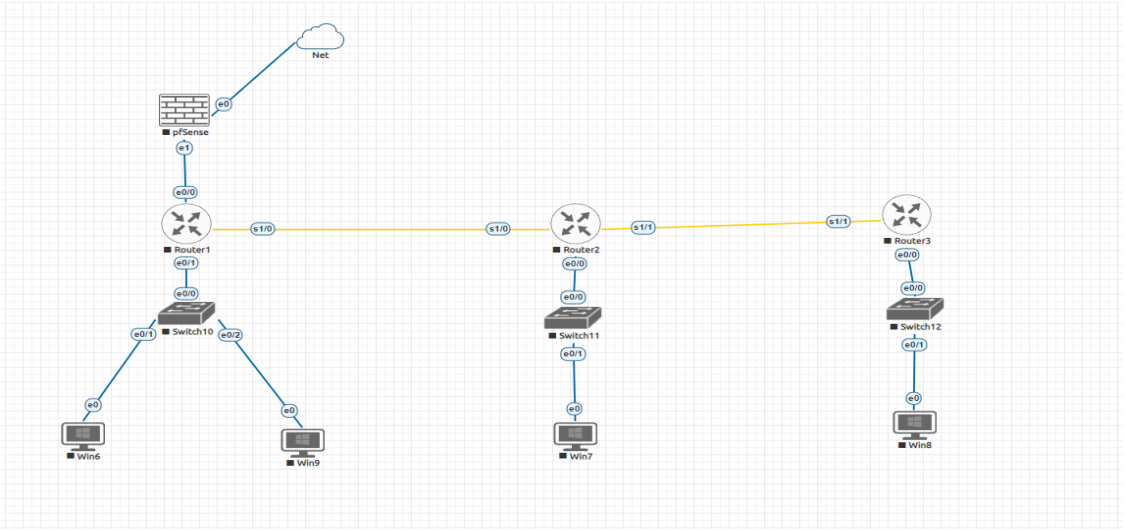
- **Capacitaciones:** Brindar capacitaciones al personal de la empresa sobre la importancia de la seguridad informática y los riesgos que conlleva no aplicarla.

Fuente: *Autor*.

Luego de tomar todos los puntos clave de la investigación, se obtiene como resultado el diseño de la nueva infraestructura de red de la empresa.

Ilustración 1

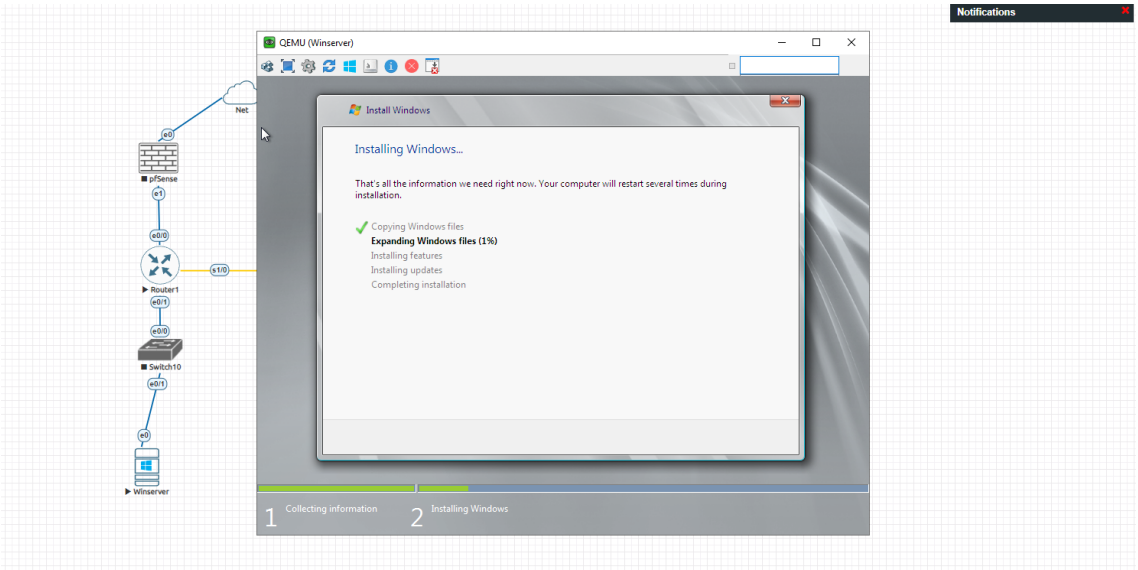
Infraestructura de red virtualizada de la empresa Agroquímicos "San Antonio"



Fuente. *Autor*.

Ilustración 2

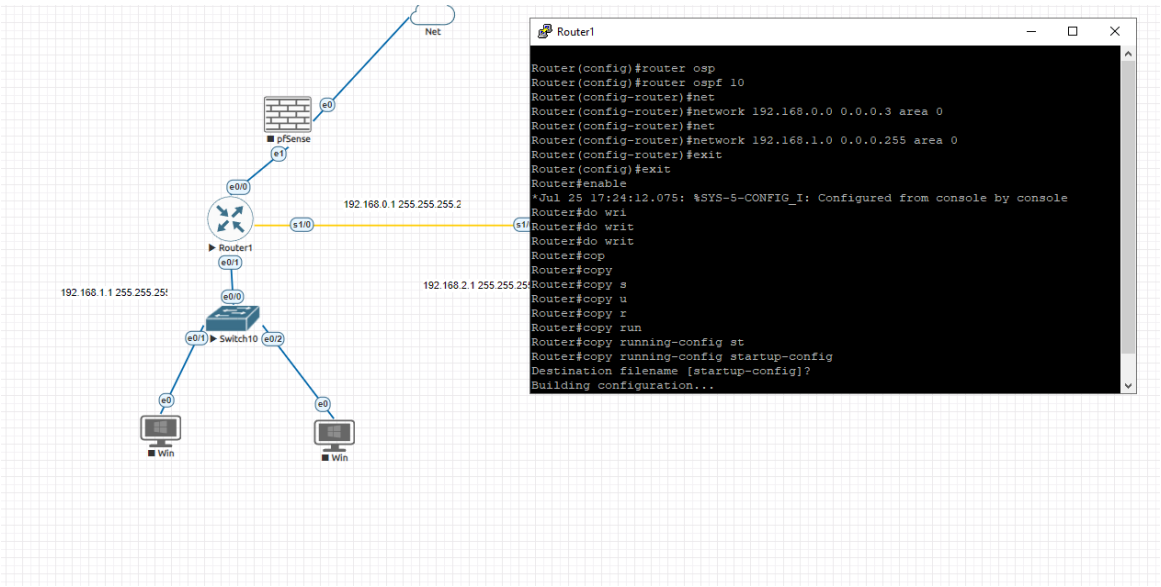
Instalación de sistemas operativos en los nodos virtuales,



Fuente. *Autor*.

Ilustración 3

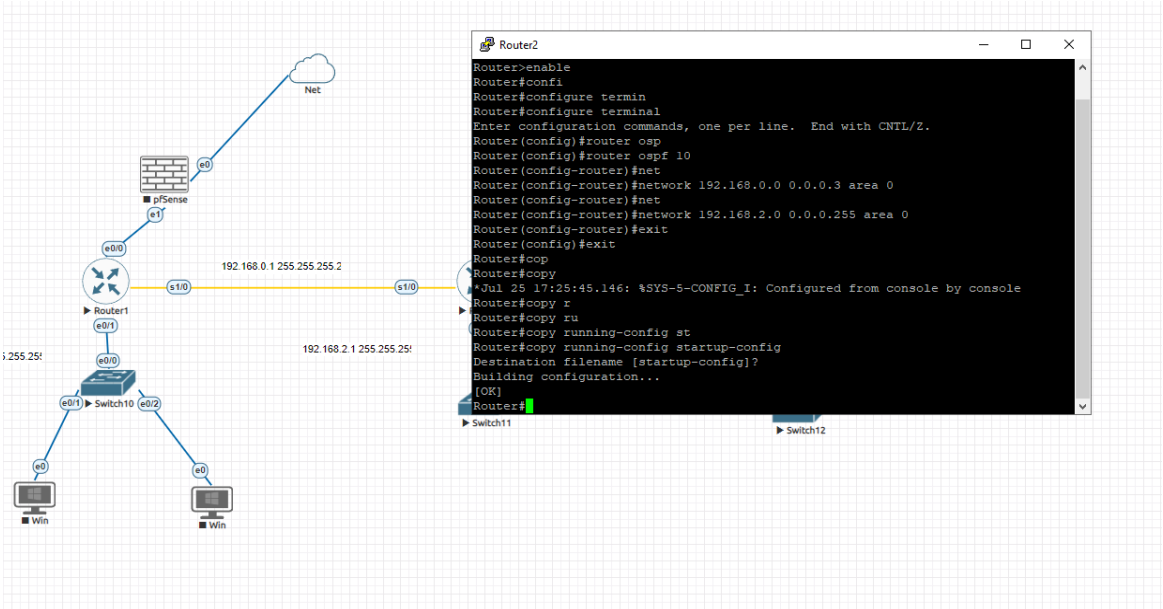
Configuración de enrutamiento OSPF en Routers IOL de cisco



Fuente. *Autor.*

Ilustración 4

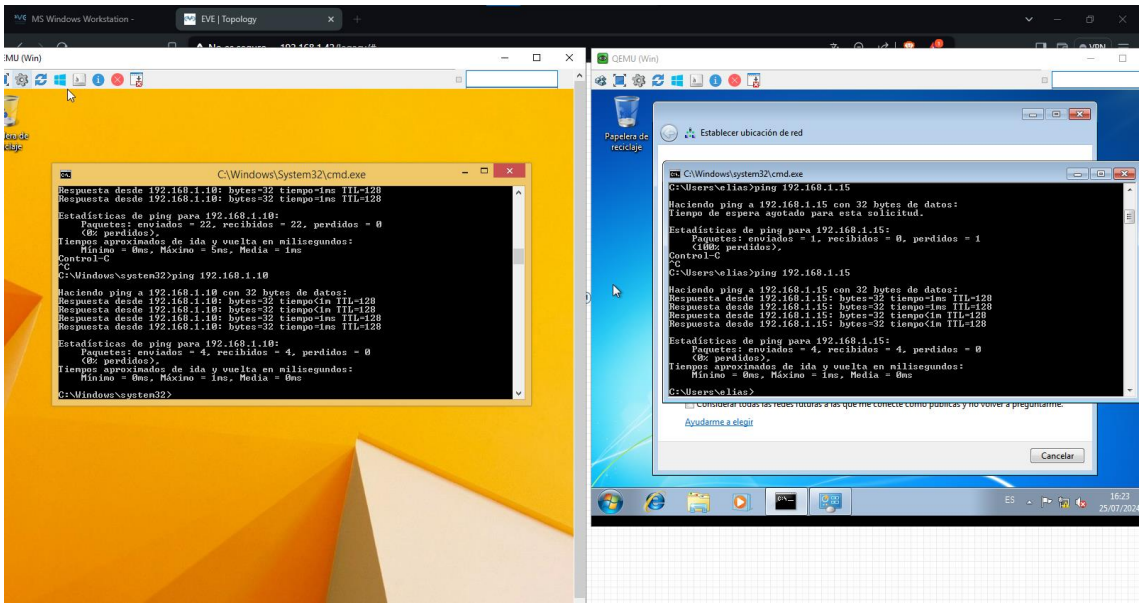
Configuración de enrutamiento OSPF en Routers IOL de cisco



Fuente. *Autor.*

Ilustración 5

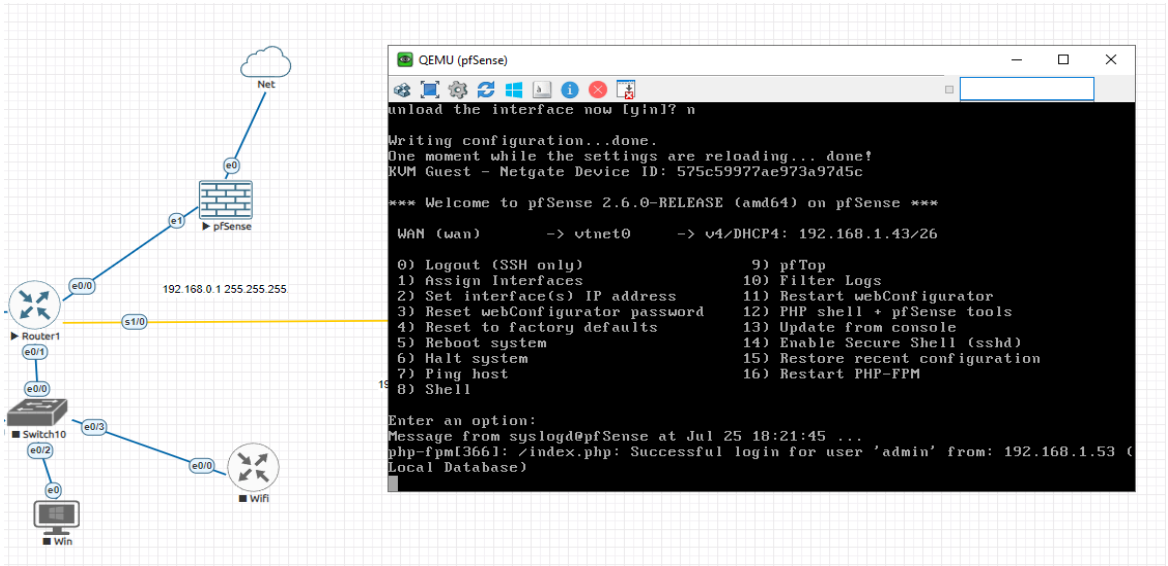
Ping entre diferentes nodos de Windows enrutados en la red.



Fuente. *Autor.*

Ilustración 6

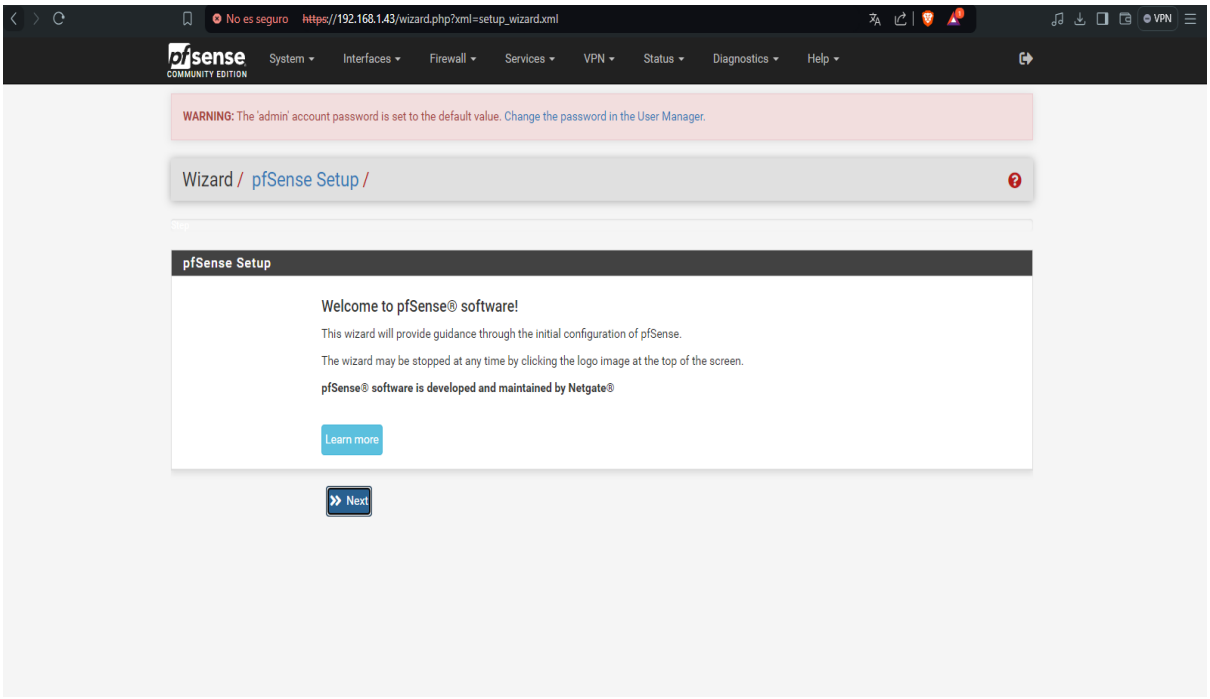
Instalación y configuración de Firewall Pfsense



Fuente. *Autor,*

Ilustración 7

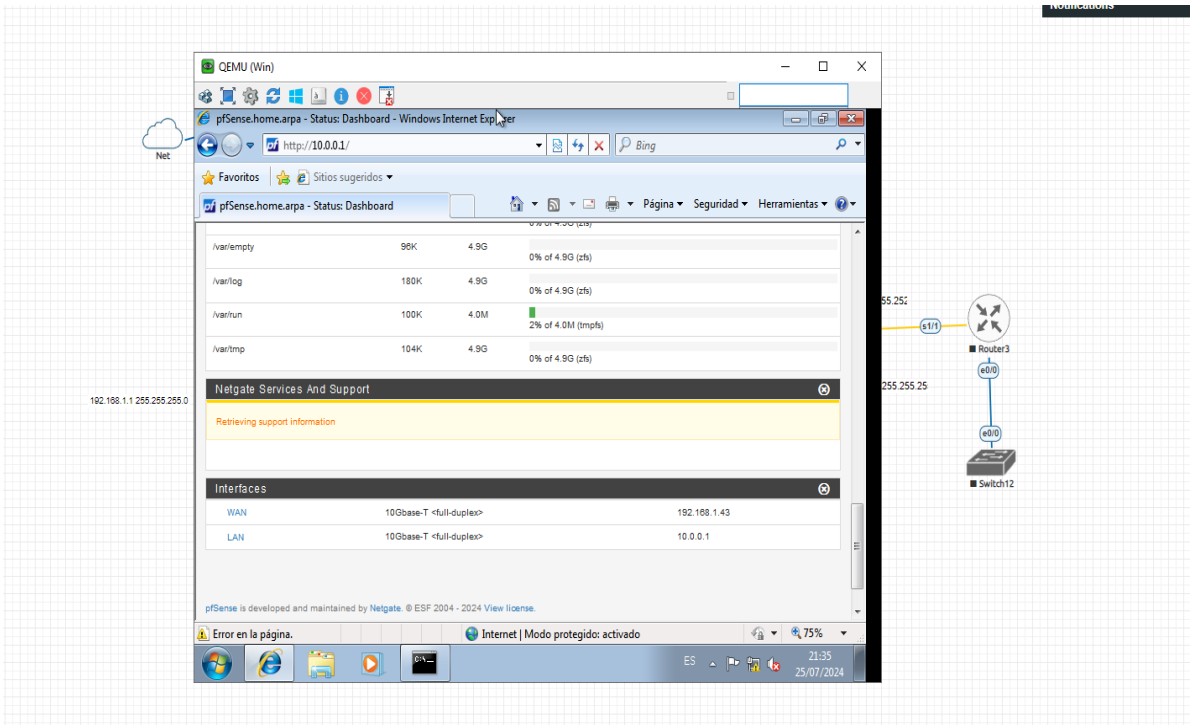
Pantalla GUI de inicio de Pfsense.



Fuente. *Autor.*

Ilustración 8

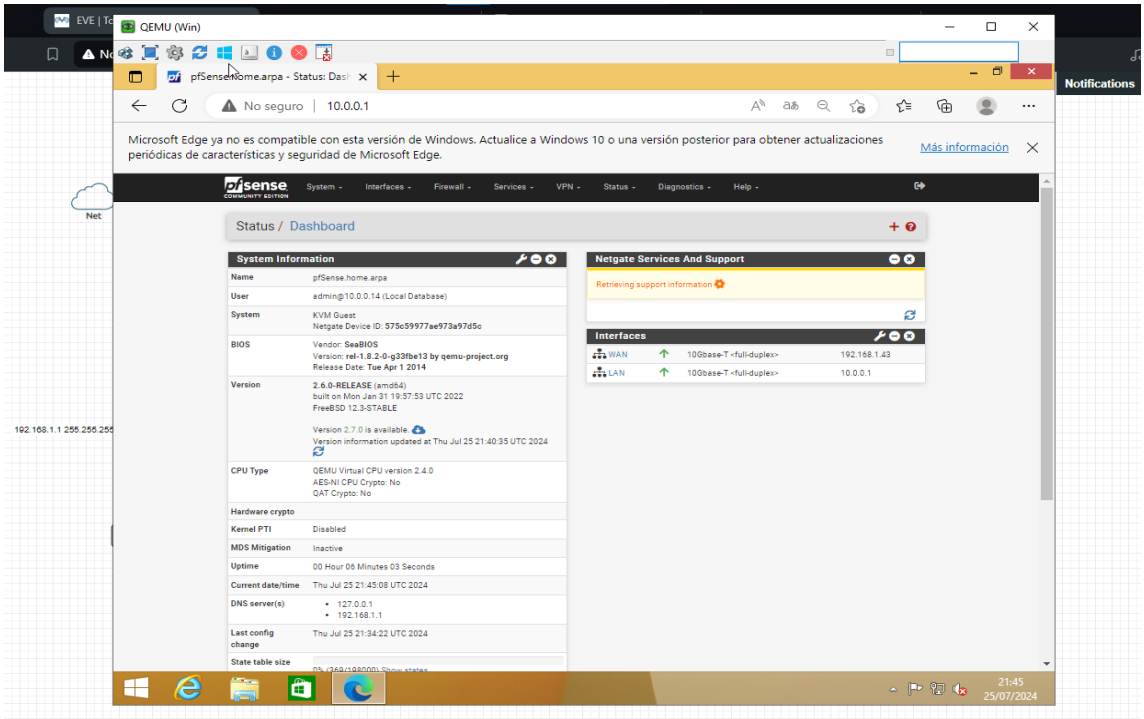
Pantalla GUI de recursos del nodo en Pfsense.



Fuente. *Autor.*

Ilustración 9

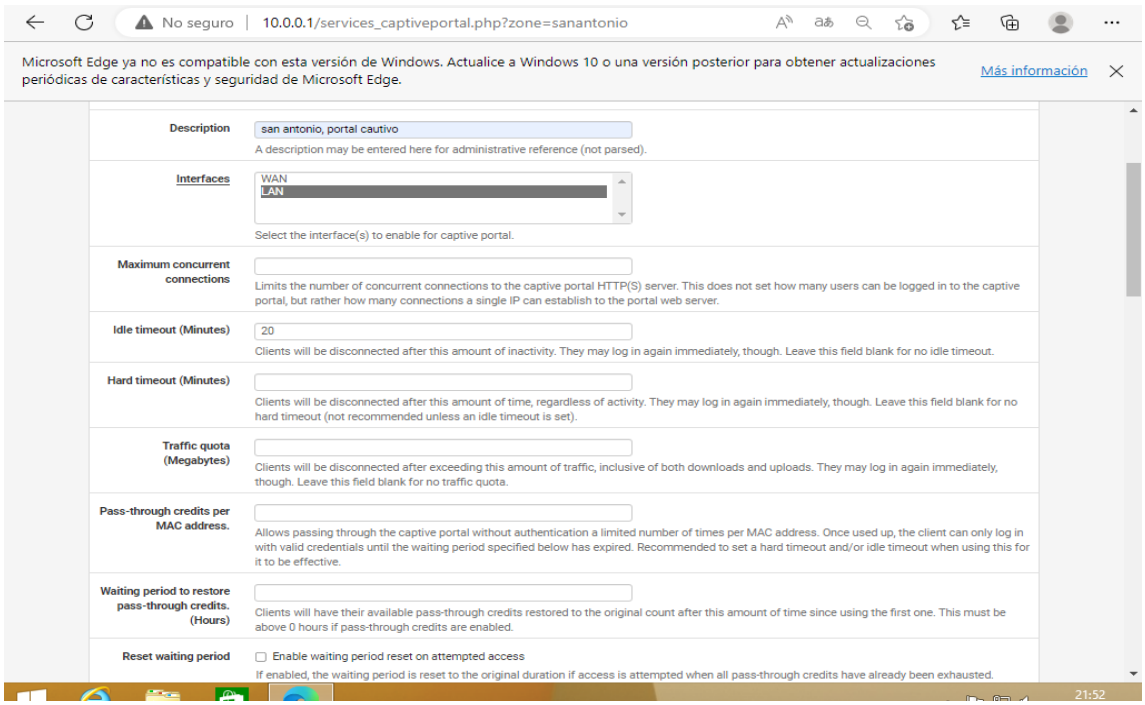
Pantalla GUI de información e interfaces de Pfsense.



Fuente. *Autor.*

Ilustración 10

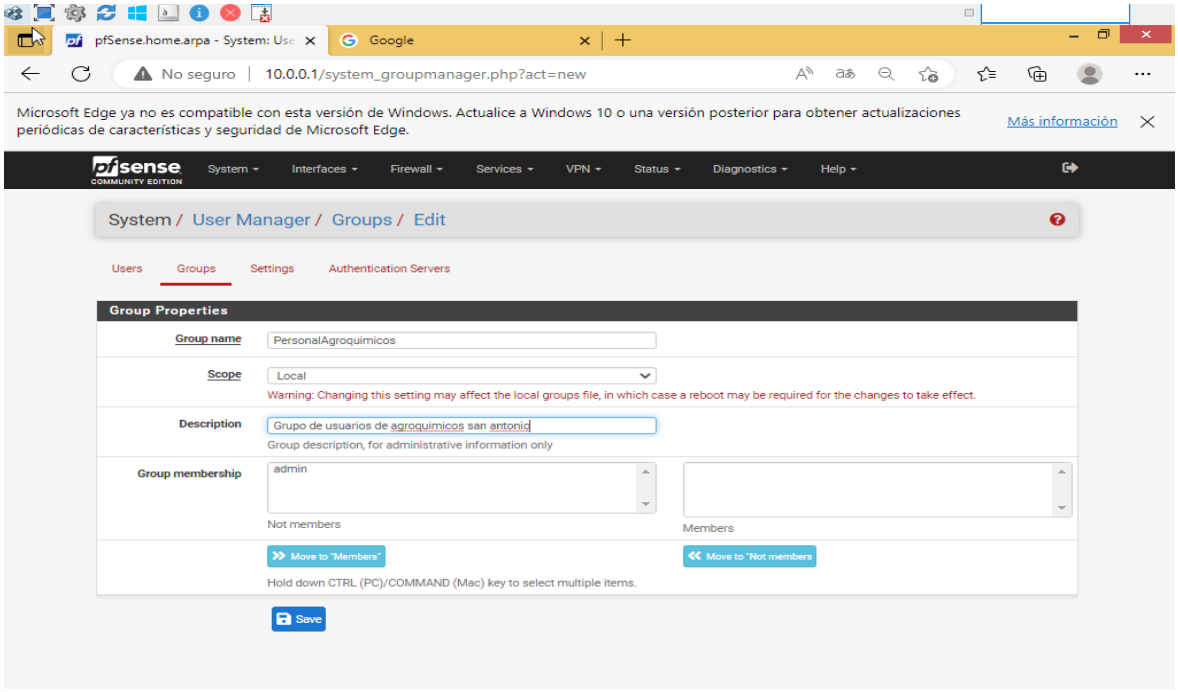
Pantalla GUI de creación de Portal Cautivo para la red LAN



Fuente. *Autor,*

Ilustración 11

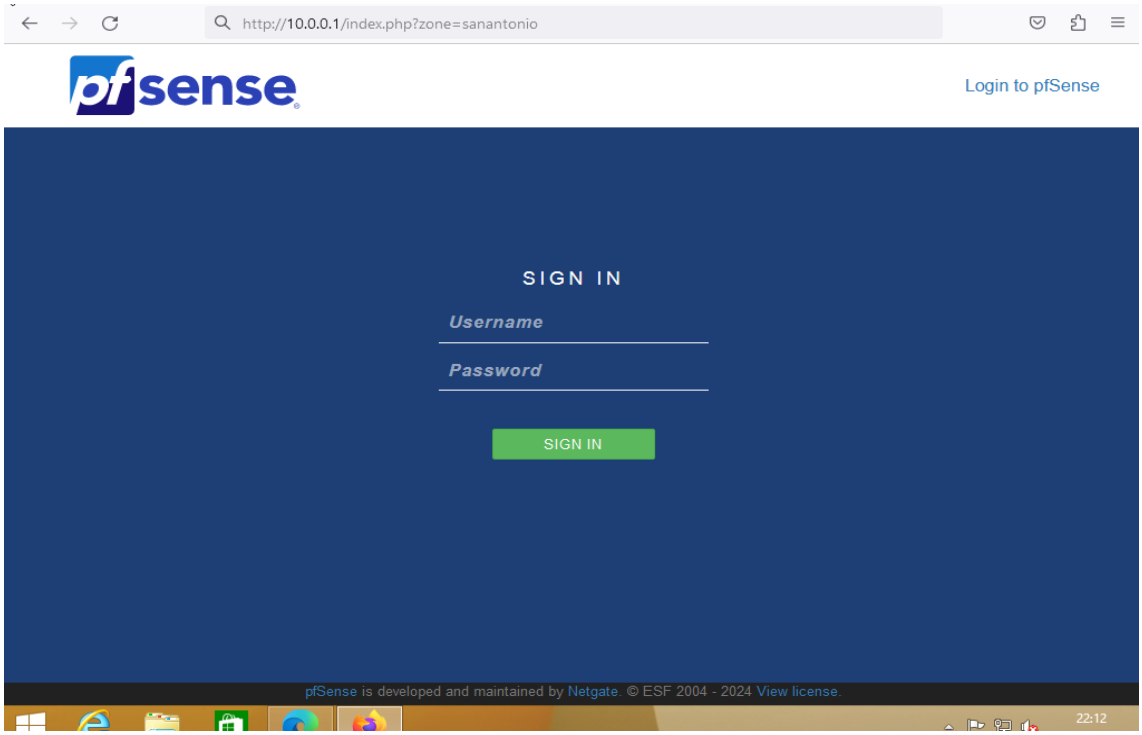
Pantalla GUI para creación de grupos, credenciales y autenticaciones autorizada.



Fuente. *Autor*.

Ilustración 12

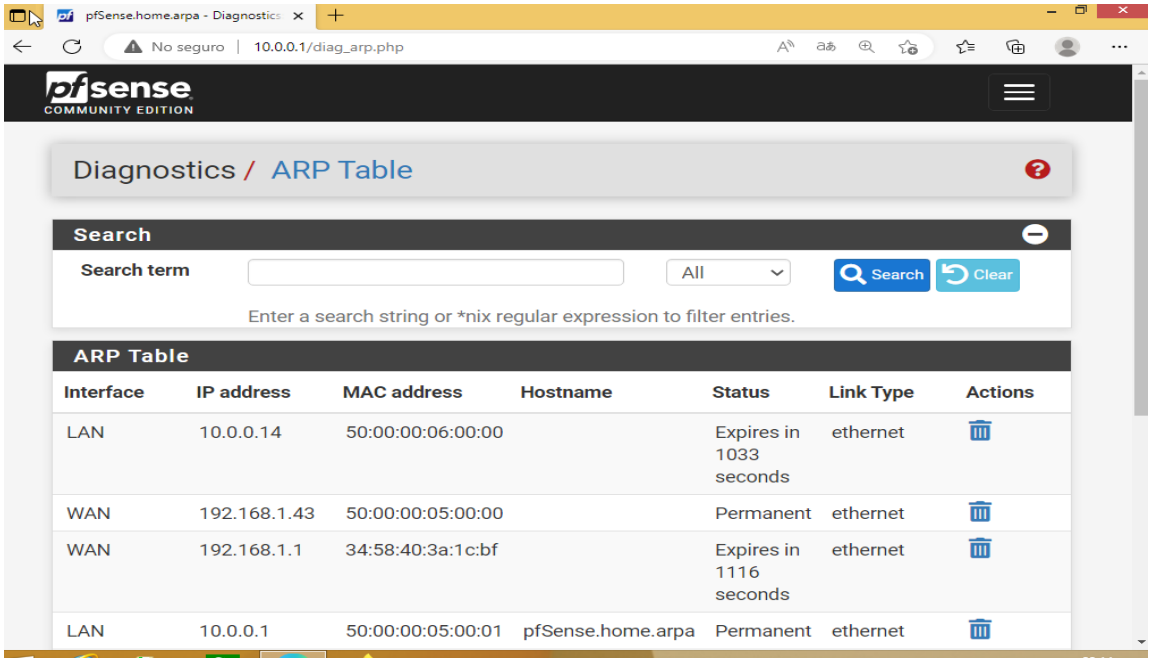
Pantalla GUI de autenticación de usuarios autorizados por Pfsense al acceder a un navegador web.



Fuente. *Autor*.

Ilustración 13

Pantalla GUI de IP en la red.

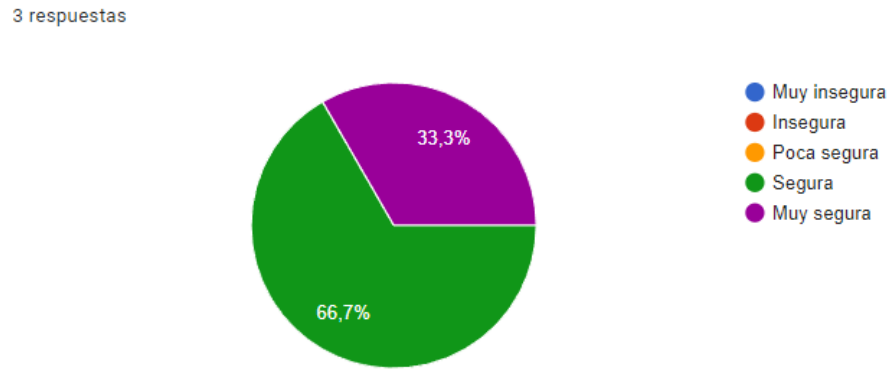


Fuente. *Autor.*

Durante las encuestas dirigidas hacia el personal seleccionado de la empresa, se obtuvieron las siguientes respuestas:

Figura 1

Pregunta 1 ¿Qué tan segura considera usted que es la nueva infraestructura de red?



.

Figura 2

Pregunta 2 ¿Qué tan satisfecho se encuentra con la seguridad proporcionada por la nueva infraestructura?

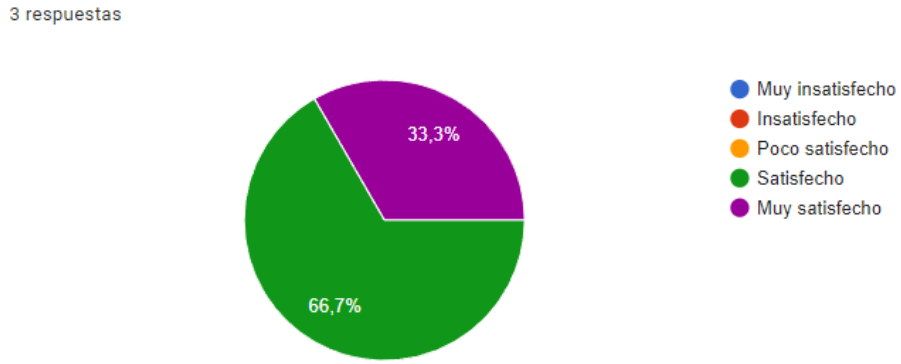


Figura 3

Pregunta 3 ¿Qué tan disponible ha encontrado el acceso a los servicios en la nueva infraestructura?

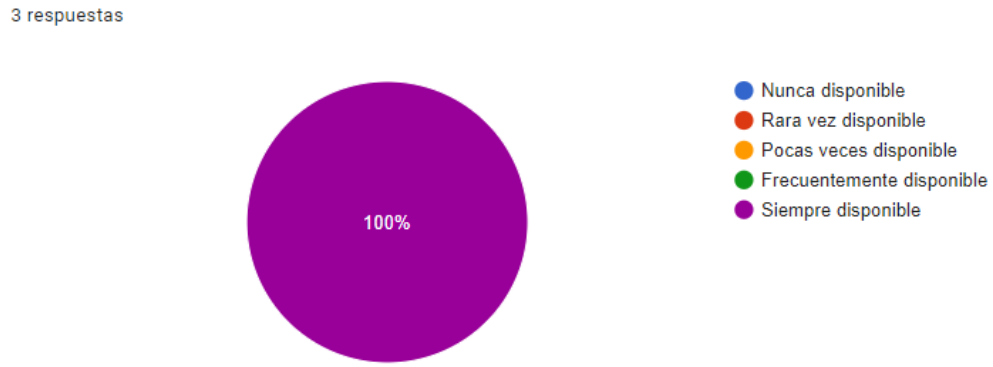
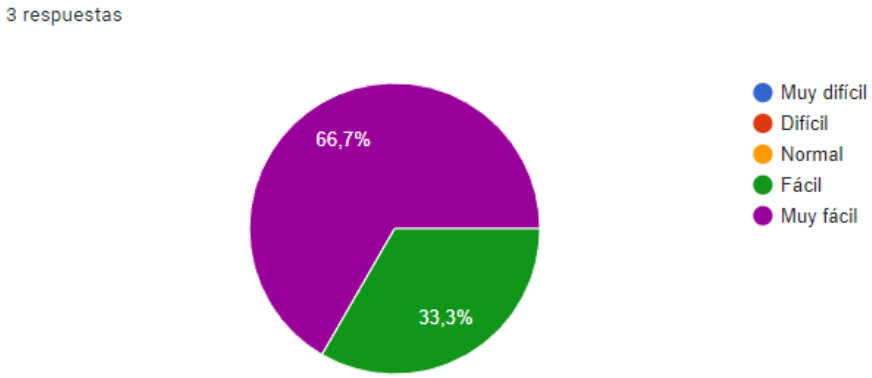


Figura 4

Pregunta 4 ¿Qué tan fácil considera usted que es usar la nueva infraestructura en funcionamiento a sus actividades?



.

4.2. Discusión

El análisis de los datos descriptivos obtenidos por parte de las herramientas empleadas durante la investigación muestra los problemas que se presentaron en la red de la empresa, a medida que genera un impacto significativo entre sus usuarios. La información proporcionada por cada uno de ellos fueron factores y puntos a considerar para complementar los procesos posteriores.

Tras identificar los activos de la empresa se lleva a cabo la gestión de los mismos de manera que se pueda organizarlos para así efectuar la valoración que tiene como activo en la empresa y de qué manera puede afectar la operatividad de los procesos que se llevan a cabo, así mismo, siendo este resultado importarte para identificar las brechas y vulnerabilidades que se encuentran entre los activos, especialmente en su parte lógica.

Estos resultados generan y respaldan un conjunto de pasos que se deben seguir como plan de seguridad y medidas de riesgo para evitar que futuros incidentes dentro de la red, de manera que efectúe la aplicación de los mismos.

El diseño de la infraestructura de red mejora significativamente el control de los accesos que no son autorizados aplicando un conjunto de reglas y procedimientos que deben seguir los usuarios para obtener acceso a la red, esto aplicado a una segmentación que gestiona la información que puede acceder una cantidad de usuarios específica, controlando así el tiempo de conectividad que puede mantener cada sesión de los usuarios que se encuentren registrados en las configuraciones establecidas por el firewall y ejecutar acciones en base al tráfico que generen.

En los resultados obtenidos por medio de la encuesta que se realizó a los usuarios de la empresa se obtiene información positiva y favorable sobre la infraestructura de red en aspectos de seguridad y calidad de servicios.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

La información que contienen las empresas siempre es importante y vital para que estas se encuentren en un correcto funcionamiento, así mismo como es importante mantener la seguridad y las operaciones tecnológicas siempre disponibles para que estas puedan ofrecer la información solicitada por los usuarios.

Realizar análisis e identificación de los activos que se encuentran disponibles en las redes empresariales es un proceso esencial que se debe efectuar, ya que este permite la identificación de brechas de seguridad y problemas que se puedan presentar entre los mismos, lo que posibilita la creación de planes de seguridad efectivos que son indispensables para mejorar a medida la infraestructura de red, asegurando así una mejor protección de la información, una mejorar seguridad en la disponibilidad de los accesos y de los servicios tecnológicos que se encuentren disponibles.

Además, la optimización de los recursos en una infraestructura de red es importante, debido a que los costos de los componentes físicos son elevados, por lo que los entornos virtuales son una excelente opción, ya que además de permite reducir los elevados costos que conlleva el desarrollo de una infraestructura de red, estos aumentan la flexibilidad y la escalabilidad de la misma, de manera que ofrece una mejor adaptación a nuevos cambios y demandas que se presenten sin adquirir nuevos dispositivos físicos que cumplan una función determinada.

5.2. Recomendaciones

Sobre la importancia de mantener segura la información, gestionar la accesibilidad de los usuarios y asegurar la continuidad de los servicios tecnológicos frente a incidentes informáticos, se recomienda aplicar una infraestructura de red capaz de gestionar el tráfico que es generado y transferido entre los usuarios de la red, ya que una gestión eficiente del tráfico permite identificar y mitigar actividades que podrían ser maliciosas o potencialmente perjudiciales para la red.

Así mismo, se recomienda establecer un control sobre la accesibilidad de los usuarios, ajustando los permisos y el acceso en función de los segmentos que son definidos en la red, de manera que los activos de administración sean accesibles únicamente por los usuarios que sean autorizados y que no haya riesgo de que usuarios no pertenecientes al segmento establecido puedan gestionar o interferir esos recursos. También aplicar el uso de portales cautivos para obtener acceso a la red, ya que permite gestionar la autenticación de usuarios de los que son autorizados sus accesos y la monitorización del tráfico que genere cada uno, lo que posibilita un control más fácil sobre las actividades que son realizadas, además de reglas y políticas de seguridad que permitan asegurar la información de los usuarios.

REFERENCIAS

Abanca. (2023, 3 abril). *Tipos de vulnerabilidades informáticas y cómo evitarlas | ABANCA Blog*. Cuentas Claras By ABANCA | Ahorro, Finanzas Personales y Actualidad. https://www.cuentasclaras.es/ciberseguridad/tipos-de-vulnerabilidades-informaticas/

Abba, M. (2023, 20 diciembre). *Qué es Wireshark, para qué sirve y casos de uso*. InnovaciónDigital360. https://www.innovaciondigital360.com/iot/que-es-wireshark-y-casos-de-uso/

Abrie, A. (2022, 6 mayo). *Nmap: Análisis de puertos y monitorización de redes*. ICM. https://www.icm.es/2022/05/06/nmap-analisis-de-puertos-y-monitorizacion-de-redes/

Aguirre, M. F. (2020, 27 octubre). *Infraestructura informática: componentes y beneficios*. appvizer.es. https://www.appvizer.es/revista/it/virtualizacion/infraestructura-informatica

Ahijon, R. (2023, 12 septiembre). *¿Qué es un escaneo de puertos? - MSMK University*. MSMK. https://msmk.university/ciberseguridad/que-es-un-escaneo-de-puertos-msmk-university

Alam, M. (2023, 19 diciembre). *¿Qué es la investigación cuantitativa? Definición, ejemplos, principales ventajas, métodos y buenas prácticas*. IdeaScale. https://ideascale.com/es/blogs/que-es-la-investigacion-cuantitativa/

Albarrán, C. (2023, 4 enero). *Qué es un firewall o cortafuegos, cómo funciona, tipos y usos*. Redes&Telecom. https://www.redestelecom.es/seguridad/que-es-un-firewall-o-cortafuegos-como-funciona-tipos-y-usos/

Arsys. (2024, 4 abril). *¿Qué es una máquina virtual y para qué sirve?* https://www.arsys.es/blog/que-es-una-maquina-virtual-y-para-que-sirve

Ashtreelane. (2024, 24 junio). *¿Qué es pfsense y para qué sirve?* LabsMac. https://www.labsmac.es/que-es-pfsense-y-para-que-sirve/

Aurora. (2022, 10 agosto). *¿Qué es una vulnerabilidad informática?* ID Digital School - Bootcamps. https://iddigitalschool.com/bootcamps/que-es-una-vulnerabilidad-informatica/

Avendaño, J. (2024, 7 febrero). *Qué son los servicios tecnológicos - Centelle*. Centelle. https://www.centelle.mx/blog/que-son-los-servicios-tecnologicos/

Bermúdez, J. (2024, 31 mayo). ¿Qué son los protocolos de red y cuáles son los más usados? *loscreativos*. https://loscreativos.co/sin-categoria/que-son-los-protocolos-de-red/

Canive, T. (2020, 7 julio). *Enfoque y características del Método Cuantitativo | Sinnaps*. Gestor de Proyectos Online. https://www.sinnaps.com/blog-gestion-proyectos/metodo-cuantitativo

César. (2021, 30 enero). *Qué es EVE-NG? el «nuevo» emulador para redes | Info++*. Info++. https://cesarcabrera.info/que-es-eve-ng-un-nuevo-emulador-para-redes/

Ekon, E. (2023, 15 junio). *Tipos de análisis de datos cualitativos y cómo aprovecharlos*. Ekon. https://www.ekon.es/blog/tipos-analisis-datos-cualitativos/

Enríquez, L. (2022, 30 noviembre). *¿Qué es una Red WAN?* ENI Networks. https://www.eninetworks.com/que-es-una-red-wan/

España, M. (2021, 7 junio). Tipos de riesgos informáticos. *Markel*. https://markel.com.es/blog/abc-del-seguro/tipos-de-riesgos-informaticos/

Eviciti, E. (2024, 25 mayo). *¿Qué es la infraestructura de red y el cableado estructurado? - Eviciti*. Eviciti - One Step Further. https://www.eviciti.com.mx/blog-post/que-es-la-infraestructura-de-redes-y-el-cableado-estructurado/

García, A. (2023, 22 junio). *3 tipos de riesgos informáticos a los que se exponen las empresas*. Worldsys. https://www.worldsys.co/3-tipos-de-riesgos-informaticos-a-los-que-se-exponen-las-empresas/

Gonzalez, F. (2023, 6 junio). *¿Qué es un virus informático? Tipos y como protegerte*. https://www.inbest.cloud/comunidad/que-es-un-virus-informatico

Hernandez, Y. (2022, 21 septiembre). *¿Qué es una Amenaza en Seguridad Informática y cómo prevenirla?* Tutoriales Dongee. https://www.dongee.com/tutoriales/que-es-una-amenaza-en-seguridad/

Hwang, D. (2021, 23 abril). *Red de área local o LAN*. ComputerWeekly.es. https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN

Inforolot, I. (2021, 23 septiembre). *Los diferentes tipos de tecnología de redes*. Inforolot. https://www.inforolot.com/los-diferentes-tipos-de-tecnologia-de-redes/

It, A. (2024, 16 mayo). *Plan de seguridad informática en la empresa: Salvaguardando activos tecnológicos*. Alanait. https://alanait.com/es/plan-de-seguridad-informatica/

Jesús. (2024, 21 enero). *Qué es un Puerto de Red: Conceptos Básicos y Aplicaciones*. Tutoriales Dongee. https://www.dongee.com/tutoriales/que-es-un-puerto-de-red/

Jiménez, J. (2024, 11 febrero). Qué tipos de redes informáticas existen. *RedesZone*. https://www.redeszone.net/tutoriales/redes-cable/tipos-redes-informaticas/

Jurado, Á. (2023, 24 mayo). *Amenazas de seguridad física para los sistemas de información*. Canal Gestión Integrada. https://www.inesem.es/revistadigital/gestion-integrada/amenazas-seguridad-fisica-sistemas-de-informacion/

Kullick, E. (2024, 5 febrero). Escaneo de vulnerabilidades de red - baud.mx. *Baud*. https://baud.mx/seguridad/escaneo-de-vulnerabilidades-de-red/

Latto, N. (2022, 17 septiembre). *¿Qué es un virus informático y cómo funciona?* ¿Qué Es un Virus Informático y Cómo Funciona? https://www.avast.com/es-es/c-computer-virus

León, F. (2020, 16 marzo). *¿Por qué son importantes los Entornos Virtuales? - Cloud Computing | Ingeniería y Servicios TIC | Partner Cisco | IEAISA*. Cloud Computing | Ingeniería y Servicios TIC | Partner Cisco | IEAISA. https://ieaisa.es/por-que-son-importantes-los-entornos-virtuales/

Manuel. (2023, 18 marzo). *Los 114 controles de la ISO 27001*. Capitalis. https://capitalis-it.com/114-controles-iso-27001/

Migallón, L. (2021, 8 noviembre). *Qué tipos de servicios existen y su definición*. Witei. https://get.witei.com/es/articulos/que-tipos-de-servicios-existen-y-su-definicion/

Muñoz, J. H. (2024, 31 mayo). ¿Qué es la virtualización y para qué sirve? | Servicios informáticos para empresas. *Servicios informáticos para empresas*. https://salesystems.es/virtualizacion/

Navarro, L. N. (2023, 28 marzo). *¿Qué es un Firewall y como funciona? en Red Fibra te enseñamos*. RedFibra. https://redfibra.mx/que-es-un-firewall-y-como-funciona-tipos-de-firewall/

Ortega, C. (2024, 29 enero). *Investigación aplicada: Definición, tipos y ejemplos*. QuestionPro. https://www.questionpro.com/blog/es/investigacion-aplicada/

Parrales, H. (2023, 1 enero). *Investigacion bibliografica*. Aprobados. https://aprobados.net/investigacion-bibliografica/

Pathak, A. (2024, 14 mayo). *Diferencia entre cortafuegos de hardware, software y en la nube*. Geekflare Spain. https://geekflare.com/es/hardware-vs-software-cloud-firewall/

Perez, C. (2023, 17 marzo). *Red MAN: qué es, ejemplos, características. . .* https://es.ccm.net/aplicaciones-e-internet/museo-de-internet/enciclopedia/10910-que-es-una-red-man/

Portal, T. (2022, 14 marzo). *Tecnología de redes*. TIC Portal. https://www.ticportal.es/glosario-tic/tecnologia-redes

Qualtrics. (2023, 26 octubre). Qualtrics. https://www.qualtrics.com/es-la/gestion-de-la-experiencia/investigacion/investigacion-cualitativa/

Rojas, A. (2024, 13 febrero). *Qué son los servicios tecnológicos y cómo puedes aprovecharlos*. Rittal Net. https://rittalnet.cl/servicios-tecnologicos/

Santander. (2022, 8 noviembre). *Cómo evitar los virus informáticos*. https://www.santander.com/es/stories/como-evitar-los-virus-informaticos

Sepulveda, M. (2023, 20 julio). Que es Nessus y como utilizarlo - El Club de la Ciberseguridad. *El Club de la Ciberseguridad*. https://ciberseguridad.club/que-es-nessus-y-como-utilizarlo/

Spasojevic, A. (2024, 10 abril). *¿Qué es la disponibilidad?* phoenixNAP IT Glossary. https://phoenixnap.mx/glosario/que-es-la-disponibilidad

Stic. (2023, 8 mayo). *Confidencialidad, integridad y disponibilidad*. Ciberseguridad. https://ciberseguridad.comillas.edu/confidentiality-integrity-and-availability/

Susan, S. (2021, 19 febrero). *Red LAN*. Buscador.com. https://www.buscador.com/red-lan/#Tipos_de_redes_LAN

Toapanta, K. (2024, 10 mayo). *¡No te Dejes Hackear! Descubre Cómo Proteger tu Empresa de las Amenazas Informáticas*. ITSQMET. https://itsqmet.edu.ec/descubre-los-riesgos-informaticos-protege-tu-empresa/

Toro, R. (2024, 15 marzo). *¿Qué es la seguridad de la información y cuantos tipos hay?* PMG SSI - ISO 27001. https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Villanueva, A. (2023, 29 mayo). *CVE y CVSS, para la clasificación de vulnerabilidades de seguridad digital*. OSTEC | Segurança Digital de Resultados. https://ostec.blog/es/aprendizaje-descubrimiento/cve-y-cvss-para-la-clasificacion-de-vulnerabilidades-de-seguridad-digital/

Zorrilla, A. (2023, 11 julio). *¿Cómo se realiza una investigación documental o bibliográfica?* Campus Digital Idyd. https://campusidyd.com/investigacion-documental-o-bibliografica/

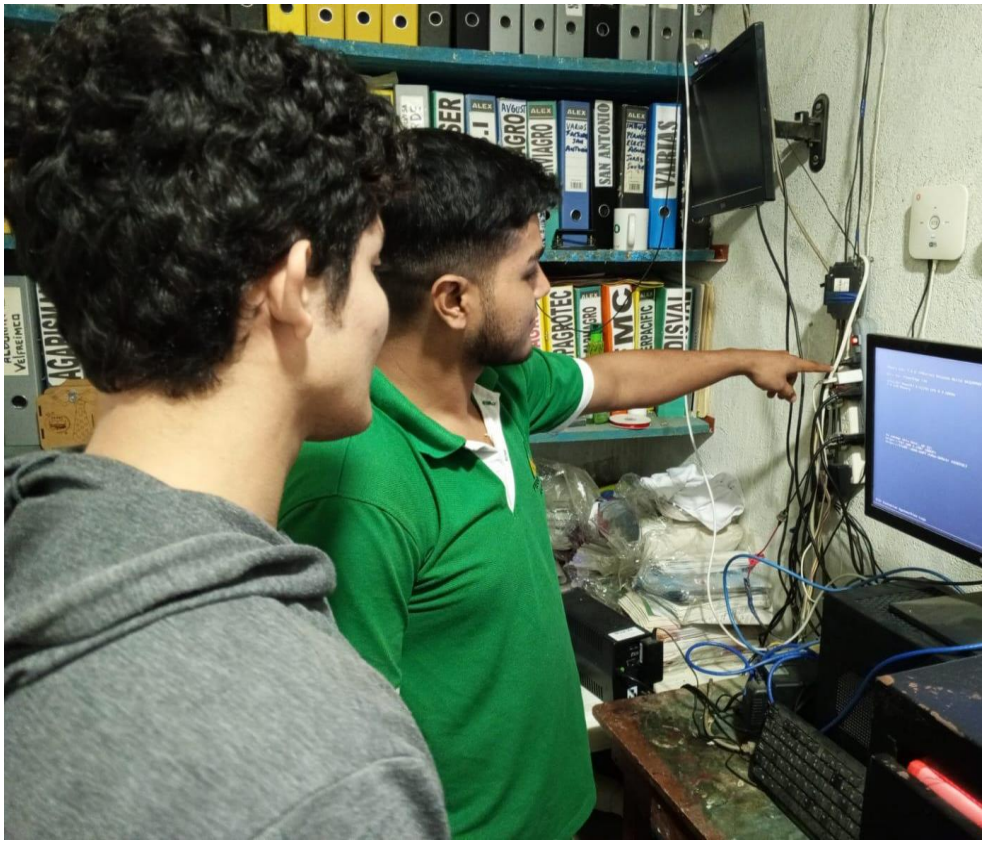
ANEXOS

BANCO DE PREGUNTAS PARA EL REPRESENTANTE DE LA EMPRESA		
Entrevista dirigía al representante legal de la Empresa "Agroquímicos San Antonio"		
Nro.	**PREGUNTAS**	**RESPUESTAS**
1	¿Cómo podría describir el impacto que tuvo el problema de seguridad presentado en la empresa?	
2	¿Qué tipo de información se vio comprometida durante el ataque informático que presentó la empresa?	
3	¿Qué medidas de seguridad considera que se deberían aplicar para proteger la información de la empresa?	
4	¿Considera usted la posibilidad de que sucedan futuros ataques informáticos como el ya experimentado?	

BANCO DE PREGUNTAS PARA PERSONAL CON CONOCIMIENTO EN EL ÁREA DE LA EMPRESA			
Entrevista dirigida a personal de trabajo de la Empresa "Agroquímicos San Antonio" con conocimientos en el área de sistemas.			
NRO.	**PREGUNTAS**	**RESPUESTAS**	**RESPONSABLE**
1	¿Cuáles son los problemas que se presentaron en su trabajo durante el incidente informático?		
2	¿Qué tipo de información de la que hace uso durante su trabajo se vio afectada por el incidente presentado en la empresa?		
3	¿Cuánto tiempo cree que se perdió debido a la interrupción de los servicios causada por el incidente informático?		
4	¿Cree que la falta de aplicar medidas de seguridad hacia la red o establecer configuraciones inadecuadas en los dispositivos contribuyeron en la posibilidad del incidente informático?		
5	¿Qué medidas de seguridad cree que serían necesarias para proteger la red de la empresa y prevenir futuros incidentes como el ya experimentado?		


FERRETERIA
AMION


FACTURAS
AGARISMAL
AGROFARMA



tenable Nessus

Agroquimicos San Antonio

Report generated by Nessus™ Sun, 26 May 2024 09:40:37 UTC