UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

MAYO 2023 - SEPTIEMBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE LA RED DE LA EMPRESA INTERGTEL EN LA CIUDAD DE BABAHOYO PARROQUIA FEBRES CORDERO

ESTUDIANTE:

MIGUEL ELADIO GARCIA GARCIA

TUTOR:

Msc. Enrique Ismael Delgado Cuadro

AÑO 2023

ÍNDICE

Índice de tablas

Índice de imágenes

Resumen

El análisis de vulnerabilidades en la red de Intergtel mediante la metodología MAGERIT reveló debilidades preocupantes. Utilizando Nessus, se descubren vulnerabilidades como puertos inseguros (53/tcp, 999/tcp y 2000/tcp) y respuestas a paquetes de eco ICMP, señalando posibles accesos no autorizados. Estas vulnerabilidades podrían exponer la red a ataques externos, comprometiendo la confidencialidad y disponibilidad de datos. Por ejemplo, el puerto 53/tcp abierto podría permitir accesos no autorizados. Es crucial abordar estas debilidades con medidas como la aplicación de parches de seguridad y configuración adecuada de firewalls para evitar la pérdida de datos y la interrupción de operaciones

Palabras clave:

Análisis de vulnerabilidades, Metodología MAGERIT, Amenazas, Vulnerabilidades, Seguridad de la información, Red de Intergtel, Herramienta Nessus, Puertos inseguros, Paquetes de eco ICMP, Riesgos potenciales, Gestión de seguridad, confidencialidad, integridad, Disponibilidad, Operaciones comerciales, Activos tecnológicos, Medidas de mitigación, Cortafuegos, Políticas de seguridad, Gestión continua de seguridad.

Abstract

The analysis of vulnerabilities in the Intergtel network using the MAGERIT methodology revealed worrying weaknesses. Using Nessus, vulnerabilities such as insecure ports (53/tcp, 999/tcp and 2000/tcp) and responses to ICMP echo packets are discovered, signaling possible unauthorized access. These vulnerabilities could expose the network to external attacks, compromising the confidentiality and availability of data. For example, open port 53/tcp could allow unauthorized access. It is crucial to address these weaknesses with measures such as applying security patches and properly configuring firewalls to avoid data loss and interruption of operations.

Keywords:

Vulnerability Analysis, MAGERIT Methodology, Threats, Vulnerabilities, Information Security, Intergtel Network, Nessus Tool, Insecure Ports, ICMP Echo Packets, Potential Risks, Security Management, Confidentiality, Integrity, Availability, Business Operations, Technological Assets, Mitigation measures, Firewalls, Security policies, Continuous security management.

Planteamiento del problema

La empresa Intergtel, dedicada a la distribución de servicios de internet en la ciudad de Babahoyo, parroquia Febres Cordero, enfrenta una serie de desafíos y problemáticas en su red de comunicaciones. Estas problemáticas pueden tener un impacto significativo en la calidad del servicio ofrecido a sus clientes, así como en la eficiencia y rentabilidad de la empresa. A continuación, se presenta una problemática identificada en relación a la red de Intergtel en esta área específica.

Una de las principales problemáticas que enfrenta Intergtel en la parroquia Febres Cordero es la falta de una infraestructura de red óptima para ofrecer una conectividad confiable y de alta velocidad a sus usuarios. La empresa ha experimentado dificultades para satisfacer la creciente demanda de internet en la zona, lo que ha llevado a una disminución en la calidad del servicio y a una insatisfacción por parte de los clientes. Esto se traduce en una baja retención de clientes y una pérdida de oportunidades de crecimiento para la empresa.

Otro desafío importante es la limitada cobertura geográfica de la red de Intergtel en la parroquia Febres Cordero. Algunas áreas rurales y zonas remotas aún no cuentan con acceso a internet o tienen una conexión deficiente, lo que genera una brecha digital y limita las oportunidades de desarrollo para los habitantes de estas áreas. Esto representa un obstáculo tanto para los residentes como para la empresa, ya que no se está aprovechando todo el potencial del mercado y se está dejando de atender a un segmento de clientes importante.

Además, la empresa se enfrenta a la competencia de otros proveedores de servicios de internet en la zona, lo que genera una presión adicional para mejorar su infraestructura y ofrecer servicios de calidad que se destaquen en el mercado. La falta de una red sólida y confiable puede hacer que los clientes opten por otras alternativas, lo que afecta directamente la rentabilidad y el crecimiento de Intergtel.

Por este motivo la empresa se encuentra en una posición única para abordar esta problemática y mejorar la vida de los residentes en la parroquia Febres Cordero. Al analizar y mejorar su infraestructura de red, la empresa puede contribuir significativamente al cierre de la brecha digital en la región y mejorar la calidad de vida de sus habitantes.

La falta de una infraestructura de red óptima, la limitada cobertura geográfica y la presión competitiva representan desafíos críticos para Intergtel en la parroquia Febres Cordero. Estos desafíos pueden tener un impacto significativo en la calidad del servicio ofrecido a los clientes y en la capacidad de la empresa para competir en el mercado de servicios de internet. Para abordar estos problemas, es esencial llevar a cabo un análisis exhaustivo de la red de comunicaciones de Intergtel y buscar soluciones efectivas que mejoren la conectividad y la calidad del servicio en la región.

Justificación

La justificación de este estudio basa en la importancia de analizar la red de comunicaciones de la empresa Intergtel en la parroquia Febres Cordero. En la actualidad, el acceso a internet se ha convertido en una necesidad fundamental para las personas y las empresas, ya que proporciona un amplio abanico de oportunidades en términos de comunicación, educación, comercio y desarrollo socioeconómico.

En el contexto específico de la parroquia Febres Cordero, se ha observado que existe una demanda creciente de servicios de internet, tanto por parte de los residentes locales como de las empresas que operan en la zona. Sin embargo, la infraestructura de red actual de Intergtel presenta limitaciones que afectan la calidad y la disponibilidad del servicio, lo que genera insatisfacción entre los usuarios y dificulta el desarrollo de actividades comerciales y educativas que requieren una conexión estable y rápida.

La mejora de la red de comunicaciones de Intergtel en la parroquia Febres Cordero es fundamental para impulsar el desarrollo socioeconómico de la región. Al contar con una infraestructura de red robusta y eficiente, se podrán ofrecer servicios de internet confiables y de alta calidad, lo que contribuirá a mejorar la conectividad de la comunidad y a fomentar la inclusión digital.

Por otro lado, la optimización de la red de Intergtel permitirá ampliar la cobertura geográfica, llegando a zonas rurales y remotas que actualmente tienen dificultades para acceder a servicios de internet. Esto abrirá nuevas oportunidades para el desarrollo de emprendimientos, el acceso a información y conocimientos, así como la mejora de la comunicación y la participación ciudadana. En un mercado cada vez más exigente y competitivo, es fundamental contar con una infraestructura de red moderna y eficiente que pueda satisfacer las demandas de los clientes.

Objetivos

Objetivo general:

Analizar la red de comunicaciones de la empresa Intergtel en la parroquia Febres Cordero, con el fin de ofrecer un servicio de internet confiable y de alta calidad a sus clientes.

Objetivos específicos:

- Reconocer la cobertura y el funcionamiento actual de la red de Intergtel en la parroquia Febres Cordero, identificando áreas de alcance y posibles deficiencias en la conectividad.
- Evaluar el rendimiento de la infraestructura de red actual de Intergtel en la parroquia Febres Cordero, identificando posibles puntos débiles y áreas de mejora.
- Definir estrategias para ampliar la cobertura geográfica de la red de Intergtel, garantizando un acceso equitativo a internet en las zonas rurales y remotas de la parroquia.

Líneas de investigación

El caso de estudio actual toma lugar en la investigación que se lleva a cabo en la línea de investigación titulada "sistemas de información y comunicación, emprendimiento e innovación", en colaboración con la sublínea de investigación centrada en "redes y tecnologías inteligentes de software y hardware". Esta sublínea de investigación gana una importancia creciente en el ámbito de las redes, ya que las redes inalámbricas de alta velocidad se vuelven cada vez más cruciales en la sociedad actual, especialmente en las zonas geográficas con menor cobertura. Además, esta área de enfoque nos brinda la oportunidad de desarrollar estrategias de mejora para el desempeño de las redes de comunicaciones inalámbricas de alta velocidad. Estas estrategias incluyen la identificación de los problemas principales que impactan el rendimiento de estas redes, como la interferencia de señales, la limitación del ancho de banda y la congestión de la red, así como el análisis de diversas metodologías de optimización de redes.

Esto abarca técnicas relacionadas con el control de acceso al medio, el enrutamiento y la asignación de recursos. El estudio toma forma debido a que se encuentra bastamente relacionado con las áreas de investigación que se centran en los sistemas de información, ya que estos implican administración y control de datos a través del analisis de la red de la empresa. En particular, es esencial que estos servicios presenten una excelente calidad y eficiencia, garantizando la fidelidad de los clientes. Para alcanzar este propósito, es necesario aplicar los objetivos del estudio con el fin de protección y salvaguardias adicionales, especialmente en lo que respecta a la poca disponibilidad del internet debido a su zona geográfica.

Marco conceptual

1. Redes de Comunicación

1.1.1. Definición de redes de comunicación.

Las redes de comunicación son sistemas interconectados que permiten la transferencia de datos, voz y otros tipos de información entre dispositivos y usuarios, independientemente de su ubicación física. Estas redes son la columna vertebral de la infraestructura de comunicaciones moderna y desempeñan un papel fundamental en la conectividad global (Barcelo, 2021).

En su esencia, las redes de comunicación se componen de nodos (como computadoras, servidores, enrutadores, etc.) y enlaces (cables, conexiones inalámbricas, fibras ópticas) que facilitan la transmisión de información. Estos sistemas pueden abarcar desde redes locales (LAN) utilizadas en entornos empresariales o domésticos hasta vastas redes de área amplia (WAN) que conectan ciudades y países.

1.1.2. Tipos de redes: cableadas e inalámbricas.

Las redes de comunicación se dividen principalmente en dos categorías: redes cableadas e inalámbricas. Estos dos tipos de redes tienen características distintivas y se utilizan en diferentes contextos según las necesidades y las limitaciones de la infraestructura (Echeberría, 2020). A continuación, se exploran estos dos tipos de redes:

Redes Cableadas: Las redes cableadas se basan en la transmisión de datos a través de cables físicos. Utilizan medios de transmisión como cables de cobre, fibras ópticas o cables coaxiales para transportar señales eléctricas o de luz que representan datos (Zais, 2019).

Redes Inalámbricas: Las redes inalámbricas, como su nombre indica, no dependen de cables físicos para la transmisión de datos. En su lugar, utilizan tecnologías de radiofrecuencia para enviar y recibir datos a través del aire (Chambergo, 2021).

Herramienta Nessus para la Evaluación de Vulnerabilidades:

Nessus es una herramienta líder en la evaluación de vulnerabilidades ampliamente utilizada por profesionales de ciberseguridad y administradores de sistemas. Su función principal es identificar debilidades y posibles riesgos de seguridad en sistemas, dispositivos y redes (Becci, Morandi, & Marrone, 2019). A continuación, se exploran las capacidades clave de Nessus en la evaluación de vulnerabilidades:

- **Escaneo Exhaustivo:** Nessus realiza escaneos exhaustivos en busca de vulnerabilidades conocidas en sistemas y servicios. Utiliza una base de datos actualizada de vulnerabilidades y técnicas de análisis avanzadas para identificar posibles amenazas.
- **Detección de Vulnerabilidades Remotas y Locales:** Nessus es capaz de detectar vulnerabilidades tanto a nivel remoto como local. Esto significa que puede evaluar tanto servicios expuestos a través de la red como configuraciones y aplicaciones locales en dispositivos.
- **Identificación de Riesgos Críticos:** La herramienta asigna calificaciones de gravedad a las vulnerabilidades encontradas, lo que ayuda a los equipos de seguridad a priorizar las correcciones. Las vulnerabilidades críticas se destacan para una atención inmediata.
- **Informes Detallados:** Nessus genera informes detallados que incluyen información sobre las vulnerabilidades identificadas, recomendaciones de mitigación y detalles técnicos. Estos informes son esenciales para la toma de decisiones informadas en cuanto a la seguridad.
- **Escaneos Programados:** Nessus permite programar escaneos automáticos periódicos, lo que facilita la supervisión continua de la seguridad y la identificación de nuevas vulnerabilidades a medida que surgen.

- **Compatibilidad con Estándares de Seguridad:** Nessus es compatible con diversos estándares y marcos de seguridad, como el Common Vulnerability Scoring System (CVSS) y el Payment Card Industry Data Security Standard (PCI DSS), lo que facilita la alineación con los requisitos de seguridad específicos de la industria.
- **Integración con Herramientas de Seguridad:** Nessus se integra con otras herramientas de seguridad y sistemas de gestión de eventos e información (SIEM), lo que permite una respuesta más efectiva a las amenazas identificadas.
- **Actualizaciones Continuas:** Nessus se actualiza de manera constante para mantenerse al día con las últimas amenazas y vulnerabilidades. Los profesionales de seguridad confían en su precisión y capacidad para detectar riesgos emergentes.

Nessus es una herramienta esencial en la caja de herramientas de ciberseguridad de una organización. Su capacidad para identificar y evaluar vulnerabilidades en sistemas y redes permite a los equipos de seguridad tomar medidas proactivas para mitigar los riesgos de seguridad y mantener un entorno de TI más seguro y resistente frente a las amenazas cibernéticas.

Importancia de las redes en la sociedad actual.

La importancia de las redes en la sociedad actual es innegable y está respaldada por la opinión de expertos y estudios realizados en el campo de las tecnologías de la información y las comunicaciones (TIC). Aquí, se presentan algunas perspectivas de autores relevantes que resaltan la significativa relevancia de las redes en la sociedad contemporánea:

Roberto Hernández (2021), destaca cómo la conectividad y las redes son esenciales para la creación de lo que él llama "sociedades en red". Argumenta que las redes de comunicación son la base de la organización social y económica en la actualidad.

El autor Javier Ruipérez (2021) investiga sobre "¿Qué está haciendo Internet con nuestras mentes?", ofrece una visión crítica pero reflexiva de cómo Internet y las redes están remodelando la forma en que pensamos y trabajamos. Examina cómo estas tecnologías han alterado la estructura cognitiva y la cultura de la sociedad.

1.2.1. Evolución de las redes de comunicación.

La evolución de las redes de comunicación ha sido un proceso fascinante y revolucionario que ha transformado la forma en que interactuamos, trabajamos y vivimos en la sociedad moderna. Como experto en el campo de las tecnologías de la información y las comunicaciones (TIC), puedo ofrecer una visión concisa y precisa de este tema crucial (Zais, 2019).

- ✓ **Los Inicios de las Redes de Comunicación:** Las redes de comunicación tienen sus raíces en las redes telegráficas y telefónicas del siglo XIX. Estas primeras redes permitieron una comunicación más rápida a larga distancia y desempeñaron un papel fundamental en la expansión económica y la coordinación (Castellanos & García, 2020).
- ✓ **La Era de Internet y las Redes de Datos:** El hito más significativo en la evolución de las redes de comunicación fue el surgimiento de Internet en la década de 1960. Inicialmente desarrollado para la comunicación militar, Internet se abrió al público en la década de 1990, transformando la forma en que compartimos información y nos comunicamos. La transición de las redes analógicas a las redes de datos digitales permitió la transmisión de voz, datos y

medios en una sola infraestructura, allanando el camino para la convergencia de servicios (Chambergo, 2021).

- ✓ **La Revolución Inalámbrica:** Otro hito importante fue el avance de las redes inalámbricas. La tecnología Wi-Fi, introducida en la década de 1990, liberó a las computadoras y dispositivos móviles de las restricciones de los cables. Esto permitió la conectividad en cualquier lugar y en cualquier momento, lo que cambió drásticamente nuestra forma de trabajar y comunicarnos (Solórzano, Rodríguez, Anzules, & Mar, 2022).
- ✓ **Redes Sociales y Comunicación Social:** La evolución de las redes de comunicación también incluye la proliferación de las redes sociales. Plataformas como Facebook, Twitter e Instagram han transformado la forma en que nos conectamos y compartimos información. Estas redes han dado voz a las personas, facilitando la difusión de ideas y la participación en discusiones globales (Sacoto, 2020).
- ✓ **El Futuro de las Redes de Comunicación:** El futuro de las redes de comunicación se enfoca en la expansión de la conectividad a través de tecnologías emergentes como el 5G y la Internet de las cosas (IoT). Estas tecnologías prometen una conectividad más rápida y confiable, así como la interconexión de dispositivos y sensores en una red global (Oviedo, Zhuma, Guzmán, & Cáceres, 2020).

La evolución de las redes de comunicación ha sido un viaje impresionante desde las redes telegráficas hasta la era de la conectividad global e inalámbrica. Estos avances han transformado fundamentalmente la forma en que vivimos y trabajamos, y el futuro promete aún más innovación y conectividad. Como experto en TIC, es emocionante ser parte de esta revolución continua.

2. Internet y su Impacto

El surgimiento y la expansión de Internet han tenido un impacto profundo en empresas y usuarios en todo el mundo. Como experto en tecnologías de la información, puedo proporcionar una visión informada sobre este tema crítico (Hernández, 2020).

2.1.1. Impacto de Internet en Empresas

El autor Padilla (2020) menciona que La llegada de Internet ha transformado la forma en que las empresas operan en múltiples aspectos, por ejemplo:

- ✓ Globalización de los Mercados: Internet ha eliminado las barreras geográficas, permitiendo a las empresas expandirse a nivel global. Las empresas pueden llegar a clientes en todo el mundo a través de sitios web y plataformas de comercio electrónico.
- ✓ Comunicación y Colaboración: Internet ha revolucionado la comunicación empresarial. Correos electrónicos, videoconferencias y herramientas de colaboración en línea han mejorado la eficiencia y la conectividad de las empresas.
- ✓ Automatización y Eficiencia: La automatización de procesos empresariales a través de Internet ha aumentado la eficiencia operativa. Desde la gestión de inventario hasta la contabilidad, las empresas han adoptado sistemas en línea para simplificar tareas.
- ✓ Nuevos Modelos de Negocio: Internet ha habilitado nuevos modelos de negocio, como el software como servicio (SaaS) y la publicidad en línea. Estos modelos han impulsado la innovación y la competitividad.

3. Infraestructura de Redes

La infraestructura de redes es esencial para la conectividad en la sociedad actual. Aquí, como experto en el tema, proporcionará información detallada sobre los elementos clave de la infraestructura de redes:

Elementos Fundamentales

- ✓ Nodos de Red: Los nodos son dispositivos como computadoras, servidores, enrutadores y conmutadores que actúan como puntos de conexión en una red. Son esenciales para el enrutamiento de datos y la transmisión de información.
- ✓ Medios de Transmisión: Estos son los medios físicos o inalámbricos a través de los cuales se transmiten los datos. Incluyen cables de fibra óptica, cables de cobre, microondas y señales de radio. La elección del medio depende de la distancia y la velocidad requeridas.
- ✓ Protocolos de Comunicación: Los protocolos son reglas y estándares que gobiernan la comunicación entre dispositivos en una red. Ejemplos comunes son TCP/IP para Internet y HTTP para la World Wide Web.

Infraestructura de Red Avanzada

- ✓ Enrutadores: Estos dispositivos dirigen el tráfico entre redes. Utilizan tablas de enrutamiento para determinar la mejor ruta para enviar datos.
- ✓ Conmutadores: Los conmutadores operan en la capa de enlace de datos y permiten la comunicación eficiente entre dispositivos dentro de una red local (LAN).
- ✓ Firewalls: Los firewalls son componentes cruciales para la seguridad de la red. Filtran el tráfico entrante y saliente para proteger contra amenazas y ataques.

- ✓ Servidores: Los servidores almacenan, gestionan y distribuyen recursos y servicios en una red. Pueden ser servidores de archivos, de correo electrónico, web, entre otros.
- ✓ Dispositivos de Seguridad: Incluyen dispositivos de detección y prevención de intrusiones, antivirus y sistemas de gestión de amenazas. Protegen la red contra amenazas cibernéticas.

Hardware y software utilizados en redes.

Como experto en el tema de redes, es crucial destacar los aspectos clave relacionados con el hardware y software utilizados en redes (Barcelo, 2021). Aquí proporcionará una visión general concisa y precisa:

Hardware en Redes:

- ✓ Routers: Los routers son dispositivos esenciales que conectan redes y dirigen el tráfico entre ellas. Son responsables de determinar la mejor ruta para enviar datos de un lugar a otro.
- ✓ Switches: Los switches operan a nivel de capa de enlace de datos y permiten la comunicación eficiente entre dispositivos en una red local (LAN). Son cruciales para la segmentación de redes y la prevención de colisiones.
- ✓ Servidores: Los servidores son computadoras especializadas que almacenan y gestionan recursos y servicios en una red. Esto puede incluir servidores de archivos, de correo electrónico, web, entre otros.
- ✓ Firewalls: Los firewalls son dispositivos o software diseñados para proteger una red al filtrar el tráfico no deseado o malicioso. Son esenciales para la seguridad de la red.
- ✓ Dispositivos de Conexión: Incluyen cables, enlaces de fibra óptica, tarjetas de red y dispositivos de acceso inalámbrico como puntos de acceso (AP).

Software en Redes:

- ✓ Sistemas Operativos de Red: Los sistemas operativos de red, como Windows Server, Linux, y Cisco IOS, son fundamentales para administrar y controlar dispositivos en la red.
- ✓ Protocolos de Comunicación: Los protocolos, como TCP/IP, HTTP y SMTP, permiten la comunicación efectiva entre dispositivos en una red. Son las reglas que rigen la transferencia de datos.
- ✓ Aplicaciones de Red: Estas son aplicaciones específicas diseñadas para su uso en una red. Pueden incluir servicios de correo electrónico, aplicaciones web, sistemas de gestión de bases de datos, entre otros.
- ✓ Software de Seguridad: Incluye programas antivirus, soluciones de detección de intrusiones, cortafuegos y herramientas de cifrado utilizadas para proteger la red contra amenazas cibernéticas.
- ✓ Software de Gestión de Red: Estas aplicaciones permiten a los administradores de red monitorear, configurar y gestionar dispositivos de red de manera eficiente.

MAGERIT

La elección de una metodología adecuada es esencial para llevar a cabo un análisis de vulnerabilidades eficaz y completo en la red de la empresa Intergtel. En este caso, se optó por la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), una metodología ampliamente reconocida y utilizada en el campo de la seguridad de la información.

MAGERIT es una metodología desarrollada por el Centro Criptológico Nacional de España y está diseñada específicamente para realizar un análisis integral de riesgos en sistemas de información (Hernandez, 2021). Su enfoque se basa en identificar, analizar y

gestionar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información en una organización.

- ✓ **Fase 1: Identificación de Activos**

En esta fase inicial, se lleva a cabo la identificación de todos los activos de información de Intergtel que podrían estar en riesgo. Esto incluye sistemas de red. Los activos se catalogan y se asigna un valor en función de su importancia para la organización.

- ✓ **Fase 2: Identificación de Amenazas**

En la segunda fase, se identifican las amenazas que podrían poner en riesgo los activos de información de la empresa. Estas amenazas incluyen posibles brechas de seguridad, ataques cibernéticos, intrusiones maliciosas y otras amenazas relacionadas con la red y la infraestructura tecnológica.

- ✓ **Fase 3: Identificación de Salvaguardias**

En esta etapa, se evaluan las salvaguardias existentes en la red de la empresa. Esto incluye medidas de seguridad como firewalls, sistemas de detección de intrusiones, políticas de seguridad, actualizaciones de software y más. Se identifican las medidas de mitigación necesarias para reducir los riesgos identificados.

- ✓ **Fase 4: Análisis de Impacto Residual**

Después de aplicar las medidas de mitigación, se procede a analizar el impacto potencial que aún podría tener un riesgo en caso de que se materialice. Esto permite determinar si las medidas son efectivas para reducir el riesgo a un nivel aceptable o si se requerían acciones adicionales.

- ✓ **Fase 5: Análisis de Riesgo Residual**

En la quinta y última fase, se evalúa el riesgo residual, es decir, el riesgo que permanece después de aplicar todas las medidas de mitigación disponibles. Esto proporciona

una imagen clara de los riesgos que las empresas aún enfrentan y ayudan a la organización a tomar decisiones informadas sobre cómo abordar estos riesgos restantes.

Es decir, la metodología MAGERIT permite un análisis de vulnerabilidades completo y efectivo en la red, lo que ayuda a la empresa a tomar medidas proactivas para proteger sus activos tecnológicos y garantizar la seguridad de la información.

Escalabilidad y Actualización

Es importante que tanto el hardware como el software sean escalables y puedan actualizarse. A medida que las necesidades de la red cambian con el tiempo, es crucial que los componentes de la red puedan adaptarse y evolucionar (Chambergo, 2021).

Para garantizar la interoperabilidad, es vital que tanto el hardware como el software cumplan con los estándares y protocolos establecidos, como TCP/IP en el caso de protocolos de comunicación.

Diseño de una infraestructura de red eficiente

El diseño de una infraestructura de red eficiente es un proceso crítico para garantizar el funcionamiento óptimo de una red de comunicaciones. Aquí se presenta un enfoque paso a paso para diseñar una infraestructura de red eficiente, junto con la perspectiva de un autor destacado en el campo (Radicelli & Torres, 2021).

- ✓ ***Paso 1: Requisitos y Objetivos de la Red***

El primer paso en el diseño de una infraestructura de red eficiente es comprender los requisitos y objetivos de la red. Esto implica definir el propósito de la red, el número de usuarios, los tipos de aplicaciones que se ejecutarán y las expectativas de rendimiento. Como menciona Tanenbaum en su libro "Computer Networks", este paso sienta las bases para todo el proceso de diseño (Becci, Morandi, & Marrone, 2020).

- ✓ ***Paso 2: Topología de Red:***

Decidir la topología de la red es esencial. ¿Será una red de estrella, bus, anillo o malla? La elección depende de la escalabilidad, la redundancia y las necesidades de rendimiento de la red. Autores como Forouzan, en su libro "Data Communications and Networking", proporcionan información valiosa sobre las diferentes topologías (Ormachea, Almidón, Vicente, & Pacheco, 2022).

- ✓ ***Paso 3: Selección de Hardware y Software:***

Basándose en los requisitos y la topología, se deben seleccionar los componentes de hardware y software adecuados. Esto incluye la elección de enrutadores, switches, servidores, sistemas operativos, protocolos y software de seguridad. Autores como Comer en su libro "Internetworking with TCP/IP" detallan las opciones de hardware y software disponibles (Buñay, Pastor, Paguay, & Moreno, 2019).

- ✓ ***Paso 4: Diseño de la Capacidad de Ancho de Banda:***

El diseño de una infraestructura de red eficiente debe incluir la planificación de la capacidad de ancho de banda para satisfacer las demandas de tráfico. Esto se hace considerando la velocidad de conexión de los dispositivos, el tráfico esperado y las aplicaciones críticas. Autores como Stallings, en su libro "Data and Computer Communications", ofrecen información sobre el cálculo de la capacidad de ancho de banda (Oviedo, Zhuma, Bowen, & Patiño, 2021).

- ✓ ***Paso 5: Seguridad de la Red:***

La seguridad es fundamental en el diseño de redes. Esto implica la implementación de firewalls, sistemas de detección de intrusiones, cifrado y autenticación. Autores como Cisco Press en su libro "CCNA Security" abordan en detalle las prácticas de seguridad en redes (Chambergo, 2021).

- ✓ ***Paso 6: Escalabilidad y Tolerancia a Fallos:***

El diseño debe considerar la escalabilidad para permitir futuras expansiones de la red sin problemas. Además, se debe garantizar la tolerancia a fallos para minimizar el tiempo de inactividad. Autores como Tanenbaum y Wetherall en su libro "Computer Networks" ofrecen información sobre la escalabilidad y la tolerancia a fallos en las redes (Barcelo, 2021).

Marco Metodológico

En el marco de la metodología de investigación adaptada para este estudio de caso, se empleó el método de observación de manera generalizada. Este método implicó la observación directa de la infraestructura de red y el entorno operativo de Intergtel en la parroquia Febres Cordero. Aquí se explica cómo se aplicó este método:

Observación de la Infraestructura de Red: Los investigadores llevaron a cabo observaciones detalladas de la infraestructura de red de Intergtel. Esto incluyó la identificación y documentación de los activos de red, como equipos de red, cables, conexiones y configuraciones técnicas. Se registraron los aspectos físicos de la infraestructura y cualquier anomalía evidente.

Observación de la Operación Diaria: Se realizaron observaciones continuas de la operación diaria de la red de comunicaciones de Intergtel. Esto implicó registrar el flujo de datos, la velocidad de conexión, la disponibilidad del servicio y cualquier interrupción o problemas que surgieran durante el período de estudio.

Registro de Eventos y Vulnerabilidades: Durante el proceso de observación, se registraron eventos relevantes y posibles vulnerabilidades en la red. Esto incluyó la detección de aperturas de puertos inseguros, respuestas a paquetes de eco ICMP y cualquier otra actividad que pudiera indicar una vulnerabilidad de seguridad.

Análisis de Rendimiento: Se observó el rendimiento general de la red, incluyendo la velocidad de conexión, la estabilidad y la capacidad de respuesta. Se prestaron especial atención a posibles cuellos de botella, congestiones o limitaciones en la infraestructura.

El método de observación proporcionó una visión detallada y objetiva de la infraestructura de red y su funcionamiento en la parroquia Febres Cordero. Esta información complementó otros métodos de investigación y contribuyó a una comprensión más completa de los desafíos y las áreas de mejora en la red de Intergtel.

Resultados

En el transcurso de esta investigación, se llevaron a cabo diversas fases para analizar la red de la empresa Intergtel en la parroquia Febres Cordero. En la primera fase, se reconoció la cobertura y el funcionamiento actual de la red de intergtel, esto con el fin de Indagar y describir los activos tecnológicos utilizados por Intergtel, incluyendo elementos como el OLT Marca Vsol, el enrutador MikroTik CCR2004-12G 2S+, el conmutador Cisco Catalyst 4948E-F, entre otros. Estos activos se catalogaron junto con sus características clave.

En la segunda fase, se evaluó el rendimiento de la infraestructura de red actual de intergtel con el fin de explorar las amenazas y vulnerabilidades que podrían poner en riesgo los activos tecnológicos. Para llevar a cabo esta tarea, se utilizó la herramienta Nessus, que permitió la identificación de posibles brechas de seguridad en la red. Se escanearon puertos y se identificaron vulnerabilidades, como la apertura de puertos inseguros, como el puerto 53/tcp, 999/tcp y 2000/tcp. Además, se registraron eventos relevantes y se realizó un análisis de trazabilidad. También se centró en la evaluación de las salvaguardas existentes en la red de Intergtel. Se identificaron medidas de seguridad implementadas, como firewalls, sistemas de detección de intrusiones (IDS) y la aplicación regular de actualizaciones de software y parches de seguridad. Estas salvaguardas tienen como objetivo proteger la red y sus activos contra amenazas externas y posibles intrusiones.

Como último punto se definieron ciertas estrategias estos riesgos, se establece que Intergtel tome medidas concretas, como la aplicación de parches de seguridad y la configuración adecuada de firewalls. El riesgo residual debe ser monitoreado continuamente y se debe responder de manera proactiva a nuevas vulnerabilidades que puedan surgir. En resumen, este análisis de vulnerabilidades proporciona una visión detallada de los desafíos de seguridad que enfrenta Intergtel y destaca la importancia de mantener una infraestructura tecnológica segura y actualizada.

Discusión de resultados

El análisis de vulnerabilidades realizado en la red de la empresa Intergtel utilizando la metodología MAGERIT ha arrojado resultados significativos que requieren una evaluación crítica y acciones concretas. A través de este análisis, se han identificado amenazas, vulnerabilidades y áreas de mejora en la seguridad de la información de la organización. A continuación, se discutirán los resultados en detalle, respaldados por datos y números proporcionados en el informe.

Uno de los hallazgos clave de este análisis fue la identificación de amenazas y vulnerabilidades en la red de Intergtel. La herramienta Nessus se utilizó de manera efectiva para explorar posibles debilidades en la infraestructura tecnológica. Se encontraron vulnerabilidades específicas, como la apertura de puertos inseguros (puertos 53/tcp, 999/tcp y 2000/tcp) y respuestas a paquetes de eco ICMP. Estas vulnerabilidades representan riesgos potenciales para la seguridad de la red y los activos tecnológicos de la organización.

Los datos proporcionados revelan la magnitud de estas vulnerabilidades. Por ejemplo, se detectó que el puerto 53/tcp estaba abierto, lo que podría permitir un acceso no autorizado a través de ese puerto. Este hallazgo resalta la necesidad de abordar estas vulnerabilidades de inmediato para mitigar el riesgo.

Es esencial comprender el impacto potencial de las vulnerabilidades identificadas. En este contexto, el análisis de riesgo residual juega un papel crucial. Algunas de las vulnerabilidades pueden exponer la red de Intergtel a ataques externos y comprometer la confidencialidad, integridad y disponibilidad de datos y servicios. Esto podría llevar a la pérdida de datos, la degradación del rendimiento de la red y la interrupción de las operaciones comerciales.

El análisis de riesgo residual también destaca la importancia de las medidas de mitigación. Si bien se han identificado vulnerabilidades, la implementación de salvaguardias adecuadas puede reducir significativamente el riesgo. Estas medidas pueden incluir la aplicación de parches de seguridad, la configuración adecuada de firewalls y la implementación de políticas de seguridad sólidas.

Se comenzó con la identificación de activos tecnológicos utilizados por Intergtel en su red de distribución de Internet. Esta fase es fundamental, ya que establece la base para comprender qué activos son esenciales para la organización. Los activos tecnológicos identificados incluyeron OLTs, enrutadores, conmutadores y otros componentes críticos de la infraestructura de red.

La importancia de esta fase se refleja en la necesidad de proteger adecuadamente los activos clave de la organización. Los datos proporcionados indican que estos activos son fundamentales para la operación de Intergtel y, por lo tanto, deben estar protegidos de manera efectiva contra amenazas y vulnerabilidades.

La identificación de salvaguardas en la fase 3 es un paso esencial en la gestión de la seguridad de la información. Las salvaguardas son medidas de seguridad, procedimientos o mecanismos que se implementan con el propósito de reducir o eliminar riesgos de seguridad. En este análisis, se identificaron salvaguardas clave, como firewalls, sistemas de detección de intrusiones y políticas de seguridad.

Los resultados indican que Intergtel ha implementado medidas de seguridad sólidas. Sin embargo, también resaltan áreas de mejora, como la necesidad de actualizaciones de software y parches de seguridad. Esto sugiere que aunque existen salvaguardas, es fundamental mantenerlas actualizadas y adaptarlas a las amenazas en constante evolución.

Conclusiones

En base al análisis realizado en la primera fase de este estudio se centró en el reconocimiento de la cobertura y el funcionamiento actual de la red de Intergtel en la parroquia Febres Cordero. Durante esta fase, se llevaron a cabo observaciones detalladas y se identificaron los activos tecnológicos utilizados por Intergtel en su infraestructura de red. Estos activos fueron catalogados y se asignó un valor en función de su importancia para la organización. Se obtuvo una comprensión sólida de la infraestructura de red de Intergtel, incluyendo la capacidad de los equipos, la topología de la red y otros aspectos clave. Esta información es esencial para planificar futuras mejoras y expansiones de la red.

La segunda fase de este estudio se centró en la identificación de amenazas y vulnerabilidades que podrían afectar la seguridad de la red de Intergtel. Utilizando la herramienta Nessus, se exploraron posibles debilidades en la infraestructura tecnológica y se identificaron vulnerabilidades específicas, como la apertura de puertos inseguros y respuestas a paquetes de eco ICMP. Estos hallazgos resaltan la importancia de la seguridad cibernética en la operación de Intergtel y la necesidad de implementar medidas de mitigación efectivas para proteger la red contra posibles amenazas. La identificación de amenazas y

vulnerabilidades proporciona una base sólida para el fortalecimiento de la seguridad de la red y la protección de los activos tecnológicos.

La fase final de este estudio se centró en la definición de estrategias para abordar los riesgos identificados en la red de Intergtel. Se enfatizó la importancia de tomar medidas concretas, como la aplicación de parches de seguridad y la configuración adecuada de firewalls, para reducir el riesgo residual. Además, se destacó la necesidad de mantener una vigilancia continua y una respuesta proactiva a nuevas vulnerabilidades que puedan surgir. Esta conclusión subraya la importancia de la acción continua en la gestión de la seguridad de la información y la necesidad de adaptarse a un entorno de amenazas en constante evolución.

Recomendaciones

Resulta importante diseñar un proceso de parcheo y actualización regular para abordar las vulnerabilidades identificadas, como la apertura de puertos inseguros y las respuestas a paquetes de eco ICMP. Este proceso debe ser proactivo y estar respaldado por una política de seguridad sólida. Realizar auditorías de seguridad periódicas y análisis de vulnerabilidades utilizando herramientas como Nessus para identificar y remediar cualquier nueva debilidad que pueda surgir en la red, baso en las conclusiones se redactaron las siguientes recomendaciones:

- Para mejorar la infraestructura de red de Intergtel y garantizar un servicio de calidad, se recomienda llevar a cabo un proceso de documentación exhaustivo de la infraestructura. Esto incluye la creación de un inventario actualizado de todos los activos tecnológicos, su ubicación, configuraciones y estado. Mantener esta información al día facilitará futuras expansiones y mejoras de la red.
- Con el fin de fortalecer la seguridad de la red de Intergtel, se sugiere implementar un plan de gestión de vulnerabilidades que incluya la corrección de las vulnerabilidades identificadas. Además, se deben establecer políticas de seguridad

sólidas que regulen el acceso y la monitorización de la red. Capacitar al personal en prácticas seguras de ciberseguridad y mantener sistemas y aplicaciones actualizados son pasos críticos para reducir el riesgo de ataques cibernéticos.

- Se recomienda implementar un programa de gestión continua de la seguridad de la información que incluya evaluaciones regulares de riesgos y actualizaciones de seguridad. Además, se debe establecer un equipo de respuesta a incidentes de seguridad cibernética para abordar de manera rápida y eficiente cualquier amenaza emergente. La colaboración con proveedores de servicios de seguridad cibernética externos puede proporcionar conocimientos y herramientas adicionales para mantener la red de Intergtel segura y protegida.

Referencias

Barcelo, R. (2021). Disección y análisis del tráfico de red de Amazon Alexa. *Grado de ingeniería informática*. Recuperado el 8 de Septiembre de 2023, de https://upcommons.upc.edu/bitstream/handle/2117/348745/155639.pdf?sequence=1&isAllowed=y

Becci, G., Morandi, M., & Marrone, L. (Octubre de 2020). Diseño de sistemas de detección de intrusión en redes definidas por software: revisión basada en machine learning. *Sociedad Argentina de Informática e Investigación Operativa*, 14-31. Recuperado el 26 de Agosto de 2023, de http://sedici.unlp.edu.ar/handle/10915/121984

Becci, G., Morandi, M., & Marrone, L. A. (2019). Seguridad en la virtualización de redes definidas por software: revisión por dimensión a virtualizar. *Sociedad Argentina de Informática (SADIO)*, 1-14. Recuperado el 27 de Agosto de 2023, de http://sedici.unlp.edu.ar/handle/10915/88673

Buñay, P., Pastor, D., Paguay, P., & Moreno, S. (2019). Análisis de la Arquitectura DIFFSERV sobre redes MPLS para la provisión de QoS en aplicaciones en tiempo

real (VoIP). *Sinergia, Vol. 2*(Num. 1), 33-40. Recuperado el 2 de Septiembre de 2023, de http://scielo.senescyt.gob.ec/pdf/rns/v2n1/2631-2654-rns-2-01-00033.pdf

Castellanos, O., & García, M. (2020). Análisis y caracterización de conjuntos de datos para detección de intrusiones. *Serie Científica de la Universidad de las Ciencias Informáticas, Vol. 13*(Num. 4), 39-52. Recuperado el 7 de Agosto de 2023, de https://dialnet.unirioja.es/servlet/articulo?codigo=8590270

Chambergo, F. (2021). *Repositorio Uncp.* Recuperado el 12 de Agosto de 2023, de https://repositorio.uncp.edu.pe/bitstream/handle/20.500.12894/6751/T010_70107345_T.pdf?sequence=1&isAllowed=y

Echeberría, R. (18 de Noviembre de 2020). *Repositorio Cepal.* (CEPAL, Ed.) Recuperado el 2023, de https://repositorio.cepal.org/items/3eac272f-f3dc-47e8-b583-5f52ef9ce001

Hernandez, R. (2021). Metodologia de la investigacion. *MCGRAW-HILL*, 497. Recuperado el 1 de Febrero de 2023, de https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf

Hernández, S. (Enero de 2020). *Openaccess.* Recuperado el 12 de Agosto de 2023, de https://openaccess.uoc.edu/bitstream/10609/106369/7/shernandezc6TFM0120memoria.pdf

Ormachea, M., Almidón, C., Vicente, W., & Pacheco, L. (2022). Gestión del tráfico de red en la calidad de servicio “QoS” WAN en Tambopata-Perú 2021. *Revista de Ciencias Sociales, Vol. 28*(Num. 2), 300-318. Recuperado el 4 de Agosto de 2023, de https://dialnet.unirioja.es/servlet/articulo?codigo=8378018

Oviedo, B., Zhuma, E., Bowen, G., & Patiño, B. (2021). Voz IP seguras implementadas en redes definidas por software. *Revista de ciencias sociales, Vol. 27*(Num. 3), 111-127.

Recuperado el 2 de Septiembre de 2023, de https://dialnet.unirioja.es/servlet/articulo?codigo=8081760

Oviedo, B., Zhuma, E., Guzmán, D., & Cáceres, C. (2020). Análisis del desempeño de redes definidas por software frente a redes con arquitectura TCP/IP. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 137-150. Recuperado el 2 de Septiembre de 2023, de https://www.researchgate.net/profile/Marcelo-Oliveira-46/publication/343303948_Monitoreo_remoto_automatizado_de_calidad_del_agua_en_sistemas_acuaponicos_en_Sao_Paulo_Brasil/links/5f222b86458515b729f3293e/Monitoreo-remoto-automatizado-de-calidad-del-agua-e

Padila, J. (2020). Análisis del Comportamiento del tráfico en Internet durante la Pandemia del Covid-19: el caso de Colombia. *Entre Ciencia e Ingeniería, Vol. 4*(Num. 18), 26-33. Recuperado el 12 de Agosto de 2023, de http://www.scielo.org.co/pdf/ecei/v14n28/1909-8367-ecei-14-28-26.pdf

Radicelli, C., & Torres, I. (27 de Octubre de 2021). *Dspace.* Recuperado el 1 de Septiembre de 2023, de http://dspace.unach.edu.ec/bitstream/51000/8185/1/%e2%80%9cAN%c3%81LISIS%20Y%20SIMULACI%c3%93N%20DEL%20EST%c3%81NDAR%20802.11AX%20PARA%20EVALUAR%20EL%20RENDIMIENTO%20DE%20DESPLIEGUES%20WLAN%20EN%20ESCENARIOS%20CON%20TR%c3%81FICO%20DE%20RED%20ELEVADO%e2%80

Ruipérez, J. (2021). Seguridad en Redes definidas por software (SDN). *Universidad Politécnica De Valencia*. Recuperado el 2 de Septiembre de 2023, de https://riunet.upv.es/handle/10251/165154

Sacoto, E. (2020). Análisis basado en teoría de juegos de modelos de negocio de operadores móviles virtuales en redes 4g y 5g. *Luis Guijarro Coloma*. Recuperado el 12 de Agosto de 2023, de https://dialnet.unirioja.es/servlet/dctes?codigo=293122

Solórzano, W., Rodríguez, A., Anzules, X., & Mar, O. (2022). Redes inalámbricas, su incidencia en la privacidad de la información. *Journal TechInnovation, Vol. 1*(Num. 2), 104-109. Recuperado el 2 de Septiembre de 2023, de https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/25/42

Zais, J. (Junio de 2019). *Openaccess.* Recuperado el 1 de Septiembre de 2023, de https://openaccess.uoc.edu/bitstream/10609/94946/6/jsaizmiTFM0619memoria.pdf

Anexos

Activos tecnologicos de la empresa intergtel

EL NODO ESTA DISTRIBUIDO POR LOS SIGUIENTES EQUIPOS

Olt marca Vsol con capacidad maxima de 1024 clientes

MIRKOTIK CCR2004 -12G 2S+

Cisco catalyst 4948e-f

topologia tipo arbol por cada pon saliente de la olt

cuenta con 1 switch poe de 8 puertos para alimentar 4 sectoriales

mikrotik 15s manbox

cuenta con 1 switch poe de 24 puertos para alimentar 5 sectoriales

mikrotik 19s manbox

Proveedor del Isp Telconet con una capacidad de 3 gbs/s

Proceso con la metodología MAGERIT

Fase 1: activos

En esta primera etapa una tabla presenta una descripción concisa de los activos tecnológicos utilizados por la empresa Intergtel para la distribución de Internet a sus clientes. Cada activo se identifica junto con sus características clave.

Tabla 1: Activos Tecnológicos

Activo Tecnológico	Descripción
OLT Marca Vsol	Capacidad máxima de 1024 clientes
MikroTik CCR2004-12G 2S+	Enrutador de alto rendimiento
Cisco Catalyst 4948E-F	Conmutador de alta densidad
Topología de Árbol por PON	Configuración de red para distribución de señal
Switch PoE de 8 Puertos	Alimenta 4 sectoriales MikroTik 15S ManBox

Switch PoE de 24 Puertos	Alimenta 5 sectoriales MikroTik 19S ManBox
Proveedor del ISP Telconet	Capacidad de 3 Gbps/s

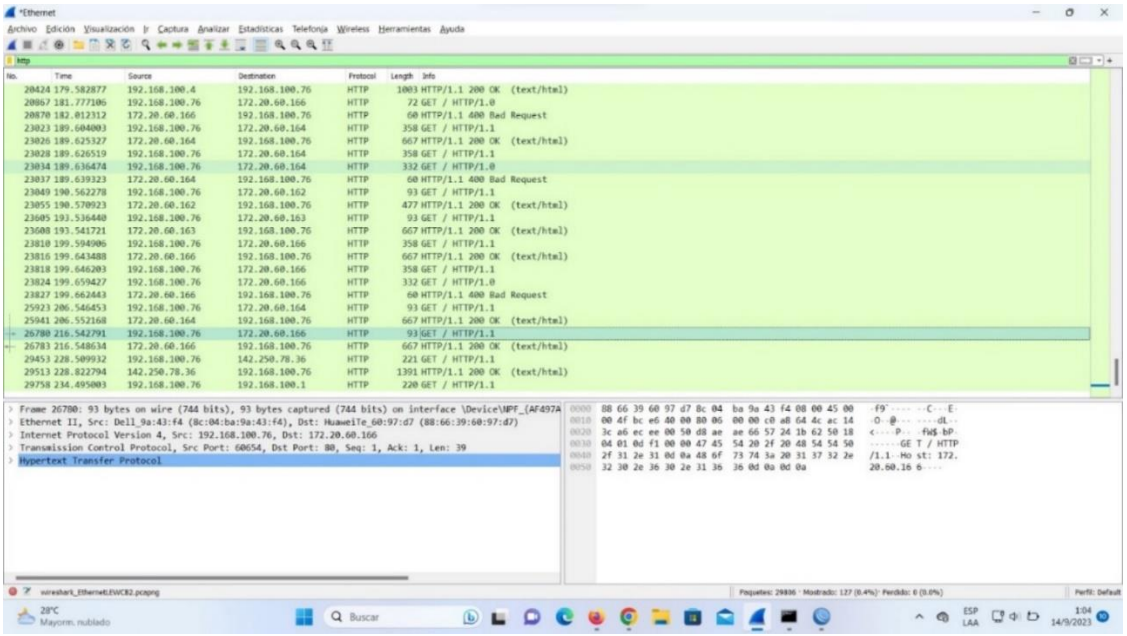
Fuente: Miguel Garcia, 2023

Fase 2: Amenazas

En esta fase se lleva a cabo la exploración de debilidades con el soporte de la herramienta Nessus, la cual es ampliamente utilizada a nivel global en el campo de análisis de red para detectar y comprobar vulnerabilidades.

A continuación, se explora la fase en la que se realiza la fase de análisis de amenazas y vulnerabilidades:

Imagen 1: Inicio de análisis de vulnerabilidades



En este período se está llevando a cabo la identificación de las amenazas y vulnerabilidades que podrían poner en riesgo los activos tecnológicos de la red de la empresa intergtel. Para realizar esta tarea, se ha utilizado la herramienta Nessus, la cual cuenta con una interfaz sencilla que permite buscar posibles brechas de seguridad en los sistemas informáticos.

Imagen 2: Determinación de amenazas y vulnerabilidades

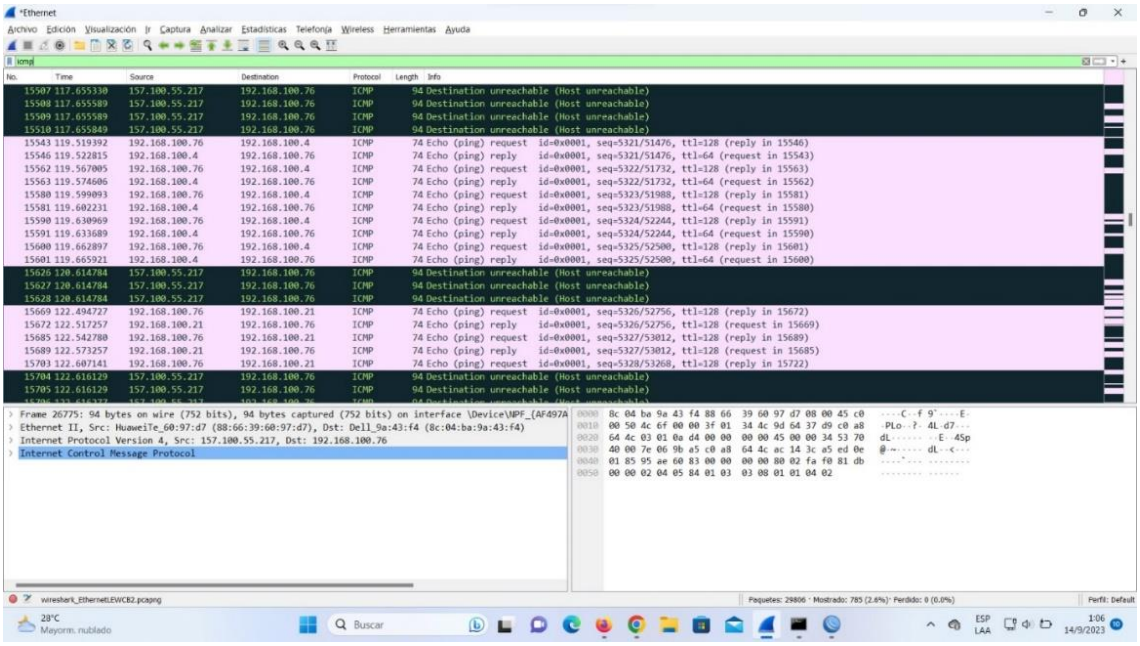


Imagen 3: Determinación de amenazas y vulnerabilidades

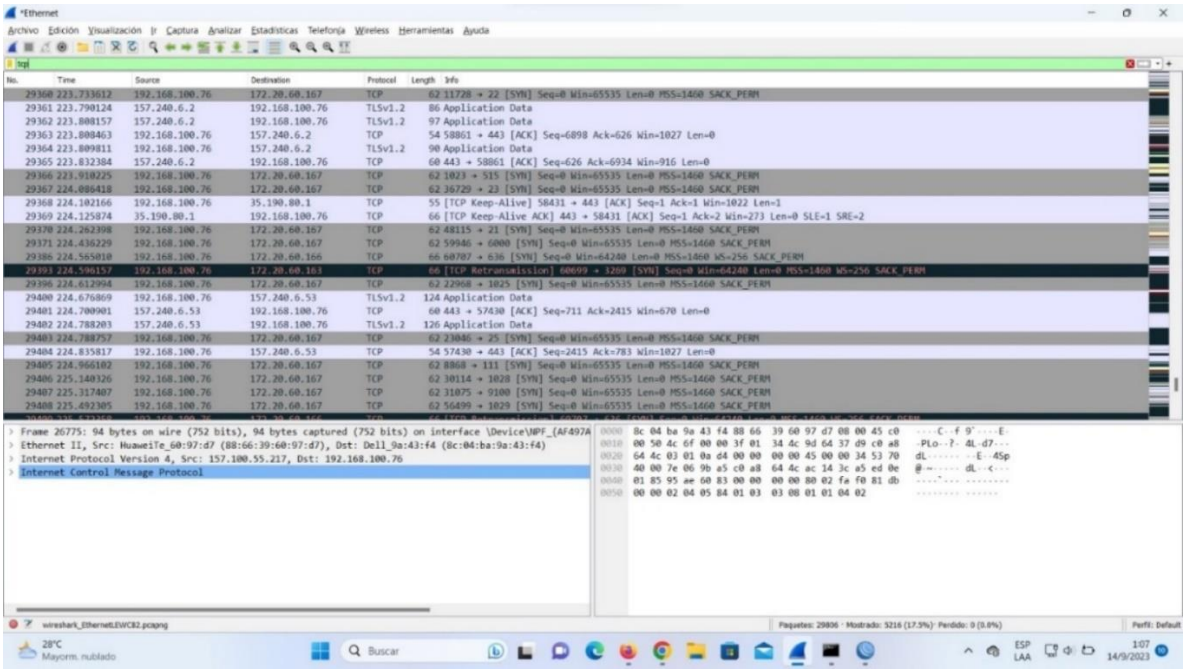
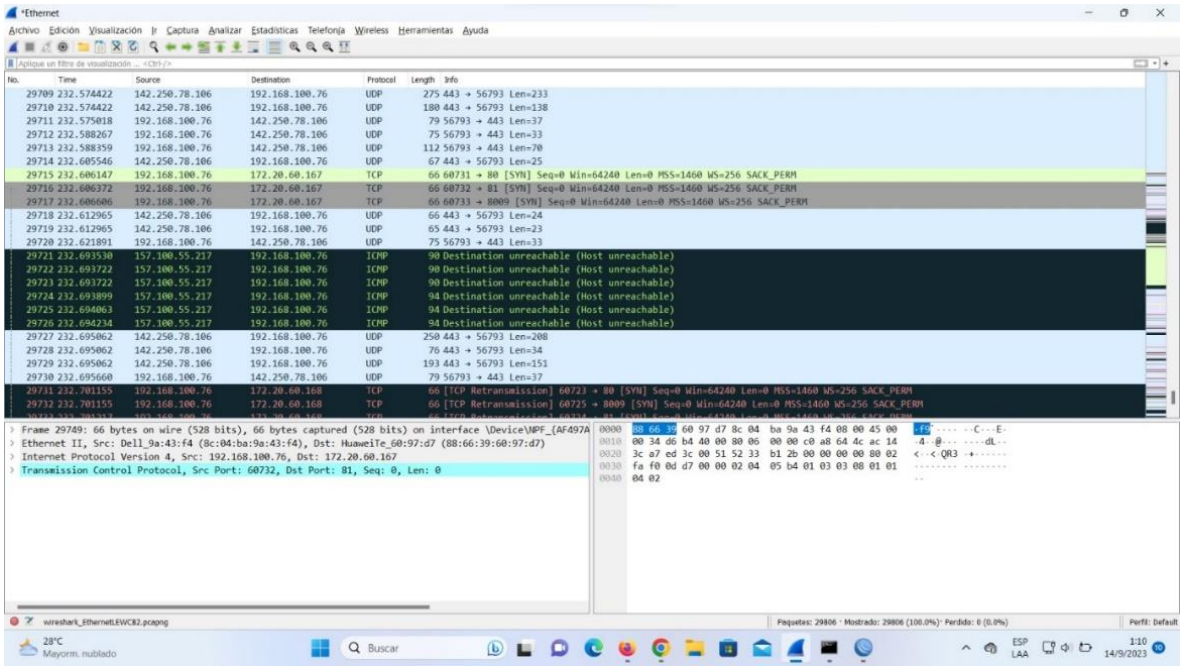


Imagen 4: Determinación de amenazas y vulnerabilidades



En esta fase, se está iniciando el escaneo de la red informática para detectar vulnerabilidades, utilizando la herramienta Nessus, la cual nos permite escanear toda la red y mostrar las posibles vulnerabilidades para prevenir posibles ataques informáticos. Después de haber completado la configuración necesaria, procedimos con la siguiente etapa que consistió en llevar a cabo la labor de escanear la red, tal y como se indica en el procedimiento.

A continuación, se presenta unas tablas que resumen el análisis de escaneo realizado mediante Nessus, lo cual nos permite identificar la cantidad de vulnerabilidades presentes en la red.

Tabla 2: Análisis de escaneo realizado mediante la herramienta Nessus

Se encontró que el puerto 53/tcp estaba abierto	
Puerto	**Hospedadores**
53/tcp/dns	172.30.70.1

Fuente: Miguel Garcia, 2023

Tabla 3: Análisis de escaneo realizado mediante la herramienta Nessus

Se encontró que el puerto 999/tcp estaba abierto	
Puerto	**Hospedadores**

999/tcp	172.30.70.1

Fuente: Miguel Garcia, 2023

Tabla 4: Análisis de escaneo realizado mediante la herramienta Nessus

Se encontró que el puerto 2000/tcp estaba abierto	
Puerto	**Hospedadores**
2000/tcp	172.30.70.1

Fuente: Miguel Garcia, 2023

Tabla 5: Análisis de escaneo realizado mediante la herramienta Nessus

No se registró ninguna salida.	
Puerto	**Hospedadores**
53/tcp/dns	172.30.70.1
53/udp/dns	172.30.70.1

Fuente: Miguel Garcia, 2023

Tabla 6: Traceroute

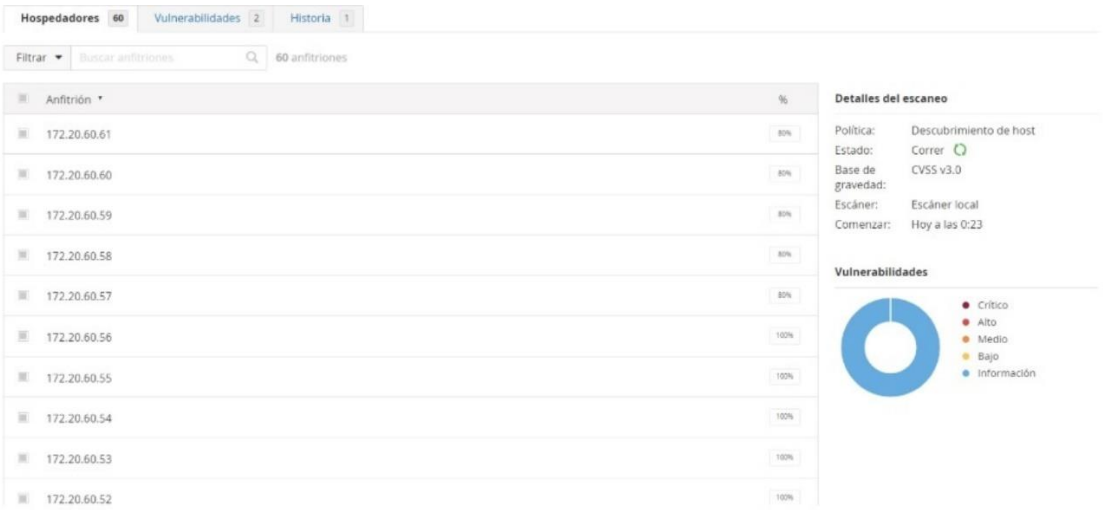
Para su información, aquí está la ruta de seguimiento de 192.168.100.76 a 172.30.70.1: 192.168.100.76 192.168.100.1 172.30.70.1 Conteo de saltos: 2	
Puerto	**Hospedadores**
0/udp	172.30.70.1

Fuente: Miguel Garcia, 2023

En la siguiente imagen se observa la hora en la que se ejecutó el análisis de vulnerabilidades el cual fue el 14 de septiembre a las 00:23 a.m. Una vez finalizada la fase de exploración, se pudieron detectar y evidenciar las debilidades y amenazas. Nessus presenta

gráficos en forma de barras y de pastel, como se muestra en la siguiente figura, para proporcionar una vista general de estas vulnerabilidades y amenazas.

Imagen 5: Scaneo Total Con Nessus



En la siguiente imagen se visualiza que Nessus pudo determinar si el host remoto está activo utilizando uno o más de los siguientes tipos de Ping.

- Un ping ARP, siempre que el host este en la subred local y Nessus se esté ejecutando a través de Etehernet
- Un ping ICMP.
- Un ping TCP, en el que el complemento envia al host remoto un paquete con el indicador SYN y el host respondera con RST o un SYN/ACK.
- Un ping UDP (por ejemplo, DNS, RPC y NTP).

Imagen 6: Producción

Fase 3: salvaguardas

En esta fase, se llevó a cabo una evaluación exhaustiva de las salvaguardas existentes en la red de la empresa Intergtel. Las salvaguardas son medidas de seguridad, procedimientos o mecanismos que se implementan con el propósito de reducir o eliminar riesgos de seguridad. La identificación de estas salvaguardas es esencial para garantizar la protección de los activos tecnológicos y la información sensible de la organización.

- ✓ **Descripción de Salvaguardas Identificadas:**

Firewalls: La empresa Intergtel utiliza firewalls para controlar y monitorear el tráfico de red. Estos firewalls se configuran para bloquear tráfico no autorizado y proteger la red contra intrusiones externas. Además, se aplican reglas de filtrado para permitir el acceso solo a servicios y aplicaciones específicos.

Sistemas de Detección de Intrusiones (IDS): Se han implementado sistemas de detección de intrusiones para identificar patrones de tráfico sospechoso y posibles intentos de intrusión. Estos sistemas generan alertas en tiempo real cuando se detectan actividades no autorizadas y ayudan en la respuesta proactiva a amenazas.

Actualizaciones de Software y Parches: La organización realiza actualizaciones regulares de software y aplica parches de seguridad en sus sistemas y dispositivos. Esto garantiza que las vulnerabilidades conocidas se aborden de manera oportuna y se reduzca el riesgo de explotación.

Fase final

La fase de impacto y riesgo residual es crucial para comprender las implicaciones reales de las vulnerabilidades detectadas y cómo estas podrían afectar a la empresa Intergtel. A través de la herramienta Nessus, se han identificado varias vulnerabilidades en la red, y ahora es fundamental evaluar su impacto potencial y determinar el riesgo residual después de aplicar las medidas de mitigación adecuadas.

Fase 4. Impacto

Algunas de las vulnerabilidades identificadas, como la apertura de puertos inseguros (como el puerto 53/tcp, 999/tcp y 2000/tcp) y la respuesta a paquetes de eco ICMP, pueden exponer la red a ataques externos y comprometer la confidencialidad, integridad y disponibilidad de los datos y servicios.

La falta de medidas de seguridad adecuadas podría permitir que los atacantes aprovechen estas vulnerabilidades para realizar acciones maliciosas, como la interrupción de servicios críticos o el acceso no autorizado a sistemas y datos confidenciales. El impacto potencial incluye la pérdida de datos, la degradación del rendimiento de la red y la interrupción de las operaciones comerciales.

Fase 5: Riesgo residual

En este punto, es fundamental que Intergtel tome medidas concretas para reducir o eliminar las vulnerabilidades detectadas. Estas medidas pueden incluir la aplicación de parches de seguridad, la configuración adecuada de firewalls y la implementación de políticas de seguridad sólidas.

Una vez que se han aplicado estas medidas, es importante reevaluar el riesgo asociado con las vulnerabilidades. El riesgo residual debe ser lo más bajo posible, lo que significa que se han tomado medidas efectivas para proteger la red y sus activos contra posibles amenazas. Esto implica un monitoreo continuo y una respuesta rápida a nuevas vulnerabilidades que puedan surgir.