UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

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 ESTRATEGIAS PARA BRINDAR SEGURIDAD INFORMÁTICA EN LAS REDES Y SERVIDORES DEL GAD MONTALVO

ESTUDIANTE:

STEVEN ALEXANDER NARANJO ALCIVAR

TUTOR:

ING. HARRY SALTOS

CONTENIDO

PLANTEAMIENTO DEL PROBLEMA

En la era de la información, las empresas dependen en gran medida de sus sistemas de información para llevar a cabo sus actividades empresariales. Sin embargo, con el aumento del uso de tecnologías de la información y la comunicación, también aumentan las amenazas de seguridad informática que pueden afectar la integridad, confidencialidad y disponibilidad de los datos de la empresa.

La seguridad informática en redes y servidores es una preocupación importante para las empresas, y es esencial que los profesionales de seguridad estén preparados para identificar y prevenir posibles amenazas. Las amenazas pueden incluir ataques de virus, malware, ransomware, ataques de fuerza bruta, ataques de phishing y ataques DDoS.

A pesar de que se han implementado medidas de seguridad, incluyendo firewalls, antivirus, existe la posibilidad de que los ataques cibernéticos continúen siendo una amenaza constante. Por lo tanto, es necesario evaluar la efectividad de las medidas de seguridad para garantizar que la organización esté protegida contra las amenazas cibernéticas.

En el municipio del cantón Montalvo uno de los principales problemas que se encuentra es la falta de seguridad en la información que se maneja dentro de la institución lo cual es muy sencillo que podría ser víctimas de un ataque cibernético a consecuencia de eso se podría filtrar información confidencial o podrían interrumpir las conexiones de red obteniendo las direcciones ip de computadores que son sumamente importante otro de los problemas son que se encuentran instalados softwares que no están actualizados siendo así vulnerables a cualquier tipo de penetración logren acceder a toda información, en este estudio de caso se va a analizar y escanear con la herramienta Nessus para que permita identificar y prevenir las amenazas de seguridad informática en sus redes y

servidores. Esto implica una revisión de las políticas y prácticas de seguridad existentes, la identificación de las áreas de vulnerabilidad, la evaluación de las amenazas y la implementación de medidas de seguridad efectivas.

JUSTIFICACION

Otorgar seguridad informática en redes y servidores es importante porque las empresas y organizaciones de todos los tamaños y sectores están cada vez más expuestas a riesgos cibernéticos, y necesitan implementar medidas para protegerse contra ellos. Con la creciente cantidad de datos almacenados electrónicamente y la dependencia de la tecnología de la información en todas las facetas del negocio, una falla en la seguridad informática puede ser catastrófica para una organización en este caso es una entidad pública. Además, los ataques cibernéticos están en constante evolución y se vuelven más sofisticados y difíciles de detectar y prevenir.

El análisis de estrategias para brindar seguridad informática en redes y servidores permite a las organizaciones evaluar sus actuales medidas de seguridad y tomar medidas para mitigar los riesgos. Al identificar las amenazas de seguridad informática y las brechas en la protección, una organización puede determinar qué estrategias de seguridad son las más adecuadas para sus necesidades y recursos. Además, mediante la realización de pruebas de penetración y simulaciones de ataques, las organizaciones se pueden evaluar la efectividad de sus estrategias de seguridad existentes y determinar áreas de mejora.

La seguridad informática es un tema crítico en el mundo empresarial y la evaluación de estrategias de seguridad para redes y servidores es crucial para proteger a las organizaciones contra las crecientes amenazas cibernéticas.

OBJETIVOS

Objetivo General:

Analizar las estrategias que permitan brindar seguridad informática en las redes y servidores del GAD de Montalvo

Objetivos Específicos:

- ✓ Realizar pruebas de escaneo para evaluar la efectividad de las estrategias de seguridad existentes y determinar áreas de mejora.
- ✓ Analizar Referencias bibliográficas e información de expertos para lograr determinar las mejores prácticas de seguridad informática.
- ✓ Proponer las mejores prácticas a través de estrategias que permitan brindar más seguridad de la información.

LINEA DE INVESTIGACION

El caso de estudio actual se enfoca en la investigación en la línea de "sistemas de información y comunicación, emprendimiento e innovación", junto con la sublínea de "redes y tecnologías inteligentes de software y hardware".

Esta línea de investigación busca explorar cómo la tecnología de la información y la comunicación (TIC) pueden impulsar el emprendimiento y la innovación en diferentes ámbitos, como empresas, organizaciones gubernamentales y comunidades locales. Se centra en la aplicación de las TIC para mejorar los procesos empresariales, la toma de decisiones, la gestión de proyectos, la colaboración y la creación de nuevos productos y servicios. En resumen, esta línea de investigación busca explorar cómo las TIC pueden impulsar la innovación y el emprendimiento en diversos contextos.

En cuanto la sublínea de investigación sobre se centra en el estudio de cómo las tecnologías inteligentes pueden ser aplicadas en el desarrollo de software y hardware para mejorar el rendimiento de las redes de comunicación y su eficiencia energética.

Esta sublínea de investigación busca desarrollar soluciones innovadoras para mejorar la conectividad, la velocidad y la seguridad en las redes de comunicación, utilizando tecnologías inteligentes como el aprendizaje automático, la inteligencia artificial, el internet de las cosas, entre otras.

MARCO CONCEPTUAL

LA INFORMÁTICA Y GOBIERNO MUNICIPAL

El municipio de Montalvo actualmente se encuentra ubicado en la avenida Antonia de las Bastidas, brindando servicios relacionados con catastros y ordenación territorial, como la legalización de propiedades y trámites relacionados con el suministro de agua potable.

La red informática distribuida en el edificio está configurada con un servidor Windows Server 2012, motor de base de datos SQL Server 2014 y Postgre13, junto con 4 switches, incluyendo el principal, y 8 routers. El SIC, el sistema de cobro de agua potable y el sistema sistema de información registral del ecuador (SIRE), son los sistemas principales con los que trabajan, y almacenan información importante que necesita ser protegida por medio de sistemas de defensa como antivirus y firewalls, como ESET Internet Security.

La organización considera la necesidad de aplicar protocolos de seguridad para proteger la integridad y disponibilidad de los datos, dado que los ataques informáticos, como el secuestro o robo de información, son cada vez más comunes.

LA IMPORTANCIA DE LOS SISTEMAS DE INFORMACIÓN EN EL SECTOR PÚBLICO

En los últimos años, ha habido una revolución tecnológica que ha afectado a todos los aspectos de la vida. La informática se ha vuelto fundamental y esencial para la mayoría de las personas. La tecnología ha permitido coordinar equipos de trabajo que están en diferentes lugares geográficos, lo que ha facilitado la comunicación entre los empleados a través de correo electrónico. Además, trabajar con una única base de datos actualizada

permite que cualquier cambio relacionado con un cliente pueda ser visto inmediatamente por todos los miembros del equipo.

Otro motivo importante por el cual los servicios informáticos son indispensables es porque protegen nuestros datos de posibles amenazas cibernéticas. Con el avance tecnológico, también aumenta el riesgo de amenazas cibernéticas, por lo que es fundamental trabajar con tecnologías de seguridad actualizadas y herramientas capaces de hacer frente a estas amenazas y mantener nuestros datos a salvo. En resumen, los servicios informáticos son esenciales para mejorar la eficiencia y seguridad en el trabajo, y en general para facilitar nuestra vida diaria. (CTi solociones, 2023)

INFRAESTRUCTURA TECNOLÓGICA MUNICIPAL

TIPOS DE REDES

Las redes informáticas son herramientas esenciales en la actualidad para la mayoría de las empresas y negocios, ya que se utilizan para llevar a cabo una amplia variedad de tareas, desde acceder a Internet y descargar archivos hasta imprimir documentos y enviar correos electrónicos con archivos adjuntos. En este artículo, se presentarán los diferentes tipos de redes informáticas que existen y se utilizan con mayor frecuencia en el mundo empresarial. (Tokio., 2023)

Red de área personal (PAN)

Una Red de Área Personal (PAN) se refiere a una red comúnmente encontrada en pequeñas oficinas o residencias privadas, y es administrada por una sola persona o empresa desde un único dispositivo. Un ejemplo común de la red PAN es la conexión que se establece entre dos dispositivos en un área limitada a través de Bluetooth. (Tokio., 2023)

Red de área local (LAN)

Una LAN es una red de área local donde múltiples dispositivos que se encuentran en una misma ubicación pueden conectarse entre sí. Sin embargo, si la conexión se establece entre más de dos dispositivos, se requieren componentes de red adicionales para mejorar y estabilizar la conexión de la LAN. (Tokio., 2023)

Red de área local inalámbrica (WLAN)

Las redes WLAN funcionan de manera similar a las LAN, con la diferencia de que utilizan tecnología inalámbrica, como la Wi-Fi. Esencialmente, las WLAN son una variante de las redes LAN que ofrecen conectividad inalámbrica para los dispositivos que se conectan a ellas. (Tokio., 2023)

Red de área del campus (CAN)

Las redes de área del campus (CAN) son más extensas que las LAN, aunque más reducidas que otras que se detallarán más adelante. Suelen ser comunes en las universidades, por lo que es uno de los tipos de redes informáticas más usuales en el ámbito académico. (Tokio., 2023)

Red de área metropolitana (MAN)

Las redes de área metropolitana (MAN) son sistemas de comunicación de mayor escala que las LAN y CAN. Estas redes cubren una zona geográfica extensa, como una ciudad o un pueblo, y generalmente se componen de varias redes LAN interconectadas. En resumen, las MAN son redes informáticas más grandes que permiten la conexión de múltiples redes LAN dentro de una zona geográfica determinada. (Tokio., 2023)

Red de área amplia (WAN)

Las redes WAN son aquellas que permiten conectar computadoras que se encuentran a largas distancias físicas. Con el objetivo de facilitar la comunicación entre

dispositivos remotos, las redes WAN se expanden a través de una gran red, permitiendo la transmisión de datos incluso a kilómetros de distancia. (Tokio., 2023)

Red de área de almacenamiento (SAN)

Las redes de área de almacenamiento (SAN) son sistemas informáticos rápidos que conectan conjuntos compartidos de dispositivos de almacenamiento con múltiples servidores. A diferencia de las redes LAN o WAN, las SAN tienen una red de alto rendimiento dedicada exclusivamente para sus dispositivos de almacenamiento, lo que la aleja de la red principal. De esta manera, se logra una mejor gestión de recursos y un mayor rendimiento en el almacenamiento de datos. (Tokio., 2023)

Red de área local óptica pasiva (POLAN)

La POLAN es una estructura de LAN de varios puntos que utiliza divisores ópticos para distribuir la señal de una fibra óptica monomodo entre distintos dispositivos y usuarios. Se trata de una tecnología de red que permite la comunicación y conexión de múltiples dispositivos en una misma red utilizando la señal de fibra óptica. (Tokio., 2023)

Red privada empresarial (EPN)

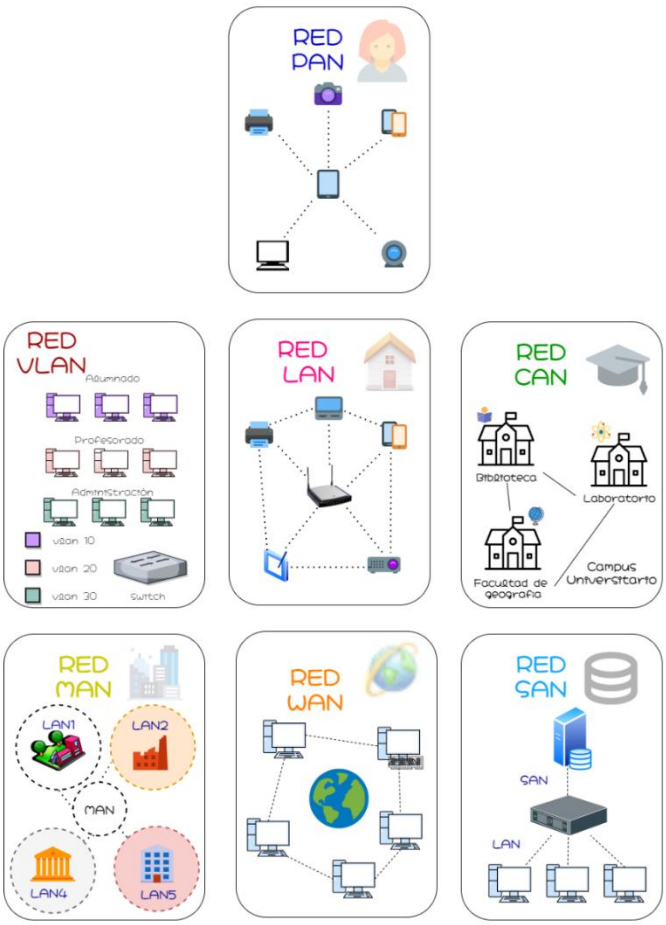
Las EPN son redes privadas que son creadas y pertenecen a empresas que buscan establecer una conexión segura entre sus diferentes ubicaciones con el fin de compartir recursos informáticos. (Tokio., 2023)

Red privada virtual (VPN)

La tecnología VPN (Red Privada Virtual) permite a los usuarios enviar y recibir datos como si estuvieran conectados a una red privada, incluso cuando no lo están físicamente. A través de una conexión segura y encriptada, los usuarios pueden acceder de forma remota a recursos de red que normalmente solo estarían disponibles de forma local, como servidores, impresoras y archivos compartidos (Tokio., 2023)

Figura 1

Tipos de redes



Nota: describe los tipos de redes mas comunes que se utiliza generalmente (Limones, 2021)

VULNERABILIDADES INFORMATICAS

Según incibe cuando se habla de vulnerabilidades desde la perspectiva informática, se refiere a debilidades o sistemas de información poco resistentes que hacen que los sistemas de una empresa sean más susceptibles a todo tipo de amenazas cibernéticas. Esta situación representa un problema significativo para proteger la

información, ya que impacta directamente en la disponibilidad e integridad de los datos almacenados, lo que dificulta mantenerlos a salvo. (2018)

TIPOS DE VULNERABILIDADES

Las debilidades o fallos en los sistemas de información representan una amenaza para la seguridad de los datos y pueden facilitar la entrada de posibles amenazas que pueden generar graves consecuencias en una organización administrativa, a continuación, se presentan unas de las vulnerabilidades más comunes:

Vulnerabilidades en el software de sistema operativo

Los sistemas operativos como Windows, Linux y MacOS han tenido varias vulnerabilidades que pueden ser explotadas por los atacantes.

Windows: Las principales son las siguientes:

- Servidores y servicios web expuestos
- Workstation service
- Microsoft SQL Server (MSSQL)
- Autenticación de usuarios de Windows
- Navegadores web (como Edge)
- Aplicaciones de intercambio de archivos peer-to-peer (P2P)
- LSAS (Servicio de Subsistema de Autoridad de Seguridad Local)
- Clientes de correo electrónico (Outlook)
- Programas de mensajería instantánea (como Skype)

Linux: En Linux, se han encontrado las siguientes vulnerabilidades más comunes en la mayoría de sus versiones:

- BIND DNS (Domain Name System)

- Servidor web
- Autenticación
- Sistemas de control de versiones
- Mail Transport Service
- SNMP (Simple Network Management Protocol)
- OpenSSL (Secure Sockets Layer)
- Configuración errónea de NIS/NFS
- Base de datos
- Kernel

MacOS: Según varios expertos, el sistema operativo MacOS es considerado uno de los más seguros en el mercado, aunque no está exento de vulnerabilidades. Los atacantes necesitan ser expertos en la materia para poder acceder y extraer información de este sistema. Algunas de las vulnerabilidades más conocidas son:

Robo de credenciales: Las fallas de identificación son una de las principales vulnerabilidades del sistema operativo MacOS, lo que permite a los hackers extraer datos de usuarios, incluyendo sus credenciales.

Fallas en los mecanismos de defensa: De acuerdo con las últimas investigaciones de Filippo Cavallarin, existen debilidades en el mecanismo de defensa de MacOS, lo que significa que este sistema podría ser burlado.

EFIS desactualizados: Los EFIS no siempre se actualizan por completo, lo que significa que un sistema o software desactualizado es una brecha potencial para un ataque. (InternetPasoAPaso, 2023)

Vulnerabilidades en aplicaciones web

Las aplicaciones web son un objetivo común para los atacantes, ya que a menudo están conectadas a bases de datos con información valiosa. Las vulnerabilidades como las inyecciones SQL, cross-site scripting (XSS) y cross-site request forgery (CSRF) son comunes en las aplicaciones web. (TARLOGIC, 2023)

Vulnerabilidades en protocolos de red

Las vulnerabilidades en los protocolos de red como TCP/IP, DNS y SSL/TLS, pueden permitir a los atacantes interceptar y manipular el tráfico de red.

- **TCP/IP:** El protocolo TCP/IP es ampliamente utilizado en redes de computadoras y puede ser vulnerable a ataques de denegación de servicio (DoS), ataques de inyección de paquetes y otros tipos de ataques
- **DNS:** El sistema DNS se utiliza para traducir nombres de dominio en direcciones IP. Las vulnerabilidades en el DNS pueden permitir a los atacantes interceptar o manipular las solicitudes de DNS, lo que podría resultar en redireccionamiento malintencionado o phishing.
- **SSL/TLS:** es un protocolo de seguridad utilizado para proteger la comunicación en línea. Las vulnerabilidades en SSL/TLS, como Heartbleed y POODLE, pueden permitir a los atacantes comprometer la confidencialidad y la integridad de la comunicación en línea. (Digicert, 2023)

SEGURIDAD INFORMÁTICA

Según UNIR La protección de información y el procesamiento seguro de datos son los principales objetivos de la seguridad informática o ciberseguridad. Su finalidad es prevenir el acceso no autorizado o la manipulación de datos y procesos por parte de terceros malintencionados. La seguridad informática también busca proteger tanto a los usuarios como a los dispositivos tecnológicos contra daños y amenazas potenciales. Es

esencial implementar medidas de seguridad adecuadas para proteger la información y los sistemas críticos contra posibles vulnerabilidades. (UNIR, 2021)

TIPOS DE SEGURIDAD INFORMATICA

Existen diferentes tipos de seguridad informática que se utilizan para proteger los sistemas, redes y datos de las organizaciones y usuarios. Algunos de los tipos más comunes son los siguientes:

Seguridad de Aplicaciones

La protección de las aplicaciones es el proceso mediante el cual se diseñan, integran y verifican características de seguridad en las aplicaciones para prevenir vulnerabilidades de seguridad frente a posibles amenazas, incluyendo la alteración y el acceso no autorizado. (VMWARE, 2023)

Seguridad de Software

Este método es utilizado para proteger los sistemas contra ataques maliciosos de hackers y otros peligros relacionados con las debilidades que puedan presentar los programas. Los intrusos pueden acceder a los sistemas a través de estas "fallas", por lo que se necesitan soluciones que incluyan modelos de autenticación y otras medidas de seguridad para prevenir estos riesgos. (UNIR, 2021)

Seguridad de hardware

Esta forma de seguridad está asociada con la protección de dispositivos que tienen como objetivo proteger sistemas y redes contra amenazas externas, como aplicaciones y programas. El enfoque principal es la implementación de medidas preventivas mediante el uso de sistemas como los de alimentación ininterrumpida (SAI), servidores proxy, firewall, módulos de seguridad de hardware (HSM) y prevención de pérdida de datos

(DLP). Además, se preocupa por la protección de los dispositivos físicos contra daños materiales. (UNIR, 2021)

Seguridad de Red

La seguridad de red se encarga de la protección de la red y su perímetro mediante el uso de múltiples capas de defensa. Cada capa de seguridad de red aplica políticas y controles para garantizar que solo los usuarios autorizados tengan acceso a los recursos de la red, bloqueando a los usuarios malintencionados para evitar ataques a las vulnerabilidades y salvaguardar la seguridad. Existen diversos tipos de seguridad de red, tales como:

- Firewalls
- Detección y prevención de intrusos (IDS/IPS)
- Seguridad de correo electrónico
- VPN
- Autenticación y control de acceso
- Seguridad de Wi-Fi. (CISCO, 2023)

ANALISIS DE VULNERABILIDADES

El análisis de vulnerabilidades es un proceso importante en la seguridad informática que tiene como objetivo identificar y evaluar los posibles puntos débiles en los sistemas y aplicaciones que puedan ser explotados por atacantes.

Este proceso implica la utilización de herramientas y técnicas para detectar vulnerabilidades y analizar su impacto en el sistema o aplicación. Algunas de las técnicas utilizadas incluyen el análisis de puertos, escaneo de vulnerabilidades, pruebas de penetración, análisis de código fuente y evaluaciones de configuración. (ZOHO CORPORATION, 2023)

Escáner de Vulnerabilidades

Un escáner de vulnerabilidades es una solución o herramienta utilizada para examinar y evaluar una computadora, red o aplicación en busca de posibles amenazas y vulnerabilidades conocidas. Para comprender cómo funciona, es importante conocer qué implica el análisis de vulnerabilidades. Este proceso consiste en identificar sistemas en la red que presenten vulnerabilidades conocidas o identificadas, tales como brechas de seguridad, puntos de entrada inseguros, errores de configuración del sistema y exploits. (ZOHO CORPORATION, 2023)

ESCANEO DE REDES

El escaneo de redes es una técnica utilizada para explorar y descubrir dispositivos y servicios conectados a una red. Consiste en enviar solicitudes de información a través de la red y recibir respuestas de los dispositivos y servicios que están disponibles. (Luz, 2022)

HERRAMIENTAS PARA EL ESCANEO DE RED

Existen muchas herramientas de escaneo de red disponibles en el mercado, algunas de las más populares son:

- Nmap
- OpenVAS
- Nessus
- Qualys
- Wireshark
- Metasploit. (Luz, 2022)

NESSUS

Nessus es una herramienta de escaneo de seguridad de red ampliamente utilizada para identificar vulnerabilidades en sistemas informáticos y redes. Fue desarrollada originalmente por Renaud Deraison en 1998 y ahora es propiedad de Tenable Network Security. Nessus utiliza una base de datos de vulnerabilidades conocidas y realiza pruebas en sistemas y redes para identificar posibles puntos de entrada para atacantes. La herramienta es compatible con múltiples plataformas y sistemas operativos y cuenta con una amplia gama de funciones y características para la gestión de vulnerabilidades.

OPENVAS

OpenVAS es un marco de trabajo de seguridad de redes que ofrece servicios de escaneo de vulnerabilidades y análisis de seguridad en sistemas informáticos. Es una herramienta de código abierto que se utiliza para identificar vulnerabilidades en sistemas y redes, y es compatible con una amplia gama de sistemas operativos y dispositivos. OpenVAS se basa en el Protocolo de Seguridad Abierto (OSP) y utiliza una serie de módulos para identificar vulnerabilidades en sistemas y redes, incluyendo escaneo de puertos, detección de servicios y detección de vulnerabilidades conocidas. Los resultados del escaneo pueden ser presentados en un informe detallado que incluye recomendaciones para abordar las vulnerabilidades identificadas. OpenVAS es ampliamente utilizado por administradores de sistemas, auditores de seguridad y profesionales de la seguridad informática para mejorar la seguridad de las redes y sistemas.

NORMATIVA ISO 27001

La normativa ISO 27001 es un estándar internacional que establece los requisitos para implementar, mantener y mejorar un sistema de gestión de seguridad de la información en una organización. Esta normativa se enfoca en la protección de la

confidencialidad, integridad y disponibilidad de la información, y se aplica a cualquier tipo de organización, independientemente de su tamaño o actividad.

Entre los principales objetivos de la normativa ISO 27001 se encuentran:

- Establecer un marco para la gestión de la seguridad de la información en una organización.
- Identificar los riesgos asociados a la información y establecer controles para mitigarlos.
- Mejorar la capacidad de la organización para responder a incidentes de seguridad.
- Asegurar el cumplimiento de los requisitos legales y reglamentarios en materia de seguridad de la información.
- Fomentar una cultura de seguridad de la información en toda la organización.

La implementación de la normativa ISO 27001 puede ayudar a una organización a proteger sus activos de información, aumentar la confianza de sus clientes y partes interesadas, y mejorar su capacidad para competir en el mercado.

MARCO METODOLOGICO

En el presente estudio de caso se han adoptado diferentes tipos de investigación, como la investigación de campo y la investigación bibliográfica. En cuanto a la investigación de campo, se seleccionó este enfoque para obtener información precisa y veraz de primera mano del lugar donde se desarrollan los hechos. Este método de investigación ayudará a garantizar que el análisis realizado esté en consonancia con los objetivos de la investigación. Para lograr el objetivo de la investigación, se llevarán a cabo observaciones en el lugar donde se desarrollan los procesos, así como juntas con los profesionales que laboran en el área de TICS.

Se llevará a cabo la implementación de la normativa ISO 27001 para el estudio de seguridad que se realizará, centrada en la seguridad informática y en los criterios de buenas prácticas y gestión de la información. Esta implementación permitirá analizar de forma sistemática las actividades que se llevan a cabo en los procesos que se manejan en el objeto de estudio a través del cumplimiento de los estándares y requisitos establecidos por la normativa. De esta forma, se podrán identificar de manera más efectiva las debilidades y los problemas que puedan surgir en relación a la seguridad informática y se podrán establecer medidas para mitigar los riesgos

Con respecto a las herramientas de investigación, se ha aplicado una entrevista al jefe de sistemas del GAD Municipal del cantón Montalvo. Para ello, se utilizó un cuestionario de preguntas abiertas. Esta estrategia de investigación permitirá analizar los niveles de seguridad informática que se aplican en el GAD Municipal del cantón Montalvo. Además, se evaluarán las prácticas actuales de la empresa en relación con los estándares de seguridad. De esta manera, se obtendrá una comprensión más profunda de

los niveles de seguridad informática y se podrán proponer medidas de mejora para garantizar la protección de la información de dicha organización.

RESULTADOS

La metodología aplicada en este estudio de caso ha permitido obtener resultados significativos mediante la combinación de dos técnicas de investigación: la investigación de campo y la investigación bibliográfica.

En primer lugar, se llevó a cabo una investigación de campo para obtener información precisa y veraz de primera mano sobre el lugar donde se desarrollan los procesos en cuestión. Para complementar la información obtenida mediante la investigación de campo, se realizó un escaneo del host principal utilizando la herramienta Nessus y OpenVas, las cuales permitieron identificar un conjunto de vulnerabilidades asociadas al sistema bajo estudio.

Los resultados obtenidos de los escaneos indican que el sistema presenta un 13% de vulnerabilidades críticas, un 31% de vulnerabilidades de alta prioridad, un 21% de vulnerabilidades de prioridad media, y un 1% de vulnerabilidades de baja prioridad. Además, se detectó que el 34% de las vulnerabilidades identificadas corresponden a información sin clasificación.

Para complementar la información obtenida de los escaneos, se realizó una encuesta con preguntas abiertas dirigidas al personal de sistemas del área de estudio, quienes proporcionaron información adicional relevante. Las respuestas proporcionadas por los participantes permitieron obtener una visión más detallada y precisa de los procesos y la infraestructura de sistemas del área de estudio.

La metodología aplicada en este estudio de caso ha permitido obtener resultados detallados y precisos acerca de las vulnerabilidades presentes en el sistema bajo estudio, gracias a la combinación de la investigación de campo, la herramienta Nessus, OpenVas y las entrevistas realizadas.

La información obtenida se usó para diseñar estrategias de mitigación de vulnerabilidades con la implementación de la normativa ISO 27001 en línea con las mejores prácticas y estándares de seguridad. La implementación de estas medidas busca garantizar la integridad y confidencialidad de la información y reducir la exposición a amenazas y ataques.

A continuación, se mostrará las estrategias producto de las entrevistas realizadas, las cuales se encuentran en el anexo 1

ESTRATEGIA 1

Actualización y parcheo de software y sistemas operativos: Es importante contar con software y sistemas operativos actualizados y parcheados para evitar vulnerabilidades y exposición a riesgos de seguridad.

Instalación de software de seguridad: Es recomendable instalar software de seguridad, como antivirus y firewalls, en todos los dispositivos que conforman la red y servidores del GAD Montalvo para protegerlos contra virus, malware y posibles intrusiones.

Uso de contraseñas seguras: Se deben establecer políticas de contraseñas seguras y obligatorias para todos los usuarios, y se debe promover la creación de contraseñas robustas y el cambio periódico de las mismas.

ESTRATEGIA 2

La gestión de accesos y la autenticación de usuarios son elementos cruciales en la seguridad de la red. Se requiere de un modelo que permita a los administradores limitar y supervisar el acceso a la información y aplicaciones por parte de los usuarios.

Auditoría y monitoreo de actividad: Es recomendable contar con herramientas de auditoría y monitoreo de la actividad de la red y servidores del GAD Montalvo para detectar y prevenir posibles amenazas o intrusiones.

Segmentación de la red: La segmentación de la red permite limitar la exposición a riesgos de seguridad, ya que cada segmento de la red puede ser tratado como una red independiente con sus propias políticas y controles de seguridad.

ESTRATEGIA 3

Protección física: Se deben implementar medidas de protección física para asegurar la integridad de los equipos y servidores del GAD Montalvo, como el uso de cerraduras, sistemas de alarma y vigilancia.

Plan de contingencia: Es importante contar con un plan de contingencia que defina las medidas a tomar en caso de incidentes de seguridad informática, como una guía para la recuperación de datos y sistemas afectados por posibles ataques.

Capacitación del personal: Es fundamental capacitar al personal del GAD Montalvo en temas de seguridad informática para que puedan identificar y prevenir posibles riesgos y amenazas de seguridad, y así poder mejorar la seguridad de la red y servidores del GAD Montalvo.

ANÁLISIS DE ESTRATEGIAS:

Según las estrategias mencionadas llegó a tener mejores resultados implementando actualizaciones y parcheo de software y sistemas operativos ya que dado los resultados del análisis cuentan con sistemas desactualizados y también hay computadoras que no cuentan con una licencia original ya que gracias a eso pueden llegar a ser muy vulnerables en cuanto la seguridad informática, también es recomendable

instalar software de seguridad, como antivirus y firewalls, en todos los dispositivos que conforman la red y servidores del municipio de Montalvo para protegerlos contra virus, malware y posibles intrusiones.

Se debe establecer el uso de contraseñas seguras y obligatorias para todos los usuarios, y se debe promover la creación de contraseñas robustas y el cambio periódico de las mismas dentro del departamento de TICS para que única y exclusivamente el personal de sistemas tenga las opciones de entregar y modificar todas las contraseñas que se necesiten para todo el personal administrativo.

Referente a el control de acceso y autenticación de usuarios es importante contar con un modelo de control de acceso que permita al personal de sistemas limitar la red y controlar el acceso de los usuarios a la información y aplicaciones implementando reglas de accesibilidad en las horas laborables siendo así que el personal administrativo tenga hora de inicio y hora de cerrar sesión cuando ya sea la hora de salida, dando a entender que los computadores que son pertenecientes al municipio de Montalvo no corran con el riesgo de ser manipulados fuera del horario laborable establecido.

DISCUSIÓN DE RESULTADOS

La metodología aplicada en este estudio de caso ha resultado en la obtención de resultados significativos y detallados acerca de las vulnerabilidades presentes en el sistema bajo estudio. Se han combinado diversas técnicas de investigación, tales como la investigación de campo, el uso de la herramienta Nessus y la realización de una encuesta con preguntas abiertas al personal de sistemas del área de estudio.

El escaneo realizado mediante Nessus permitió identificar un conjunto de vulnerabilidades críticas, de alta prioridad, de prioridad media y de baja prioridad, así como también información sin clasificación. Por su parte, las respuestas proporcionadas por el personal de sistemas permitieron obtener una visión más detallada y precisa de los procesos y la infraestructura de sistemas del área de estudio.

La investigación bibliográfica permitió identificar vulnerabilidades en el sistema y verificar si ya habían sido solucionadas, lo que resultó en la elaboración de una lista de estrategias para mitigar las vulnerabilidades encontradas y reducir los riesgos de posibles ataques o violaciones de seguridad. La combinación de las técnicas de investigación aplicadas ha permitido obtener información clave y relevante para el diseño de estrategias específicas de mitigación de vulnerabilidades, en línea con las mejores prácticas y estándares de seguridad en la industria.

La implementación de estas medidas busca garantizar la integridad y confidencialidad de la información del sistema, y reducir la exposición a posibles amenazas y ataques. La combinación de las dos técnicas de investigación utilizadas permitió obtener una visión completa del sistema y de los procesos involucrados, así como de las vulnerabilidades presentes en el mismo.

La información obtenida de la investigación de campo y del escaneo realizado mediante la herramienta Nessus permitió identificar una serie de vulnerabilidades de diferentes niveles de prioridad, lo que hace evidente la necesidad de tomar medidas para mitigar los riesgos asociados a estas vulnerabilidades. La encuesta realizada al personal de sistemas del área de estudio permitió obtener información valiosa sobre los procesos y la infraestructura de sistemas, lo que resulta de gran utilidad para el diseño de estrategias específicas para brindar la seguridad informática en las redes y servidores del municipio de Montalvo.

En consecuencia, la metodología aplicada ha permitido obtener resultados significativos y relevantes para el diseño de estrategias para brindar la seguridad informática, en línea con las mejores prácticas y estándares de seguridad en la industria. La implementación de estas medidas busca garantizar la integridad y confidencialidad de la información del sistema, y reducir la exposición a posibles amenazas y ataques.

CONCLUSIONES

Después de examinar la red informática del municipio de Montalvo mediante el uso de la herramienta Nessus, se han identificado varias debilidades y vulnerabilidades en la red que pueden ser aprovechadas por hackers. Estas debilidades ponen en riesgo la seguridad de los equipos de almacenamiento del municipio y su información, lo que podría permitir la manipulación, divulgación o sustracción de datos por parte de terceros no autorizados. Es evidente que la red informática carece de suficientes normas de seguridad tanto en sus sistemas como en sus equipos, especialmente teniendo en cuenta el tipo de actividades que lleva a cabo la organización y la cantidad y calidad de información que maneja.

En lo que se refiere a la implementación de software de seguridad, la entidad únicamente utiliza el que viene incluido de manera predeterminada en algunos sistemas, como firewalls y antivirus. Además, se han identificado equipos que no cuentan con licencias originales de sistemas operativos y de antivirus.

En cuanto a la estructura de la red, se ha constatado que el cuarto de equipos no cuenta con las medidas de seguridad necesarias, ya que no posee filtro de seguridad no actualizado, lo que lo hace vulnerable a posibles intrusiones por parte de personas ajenas a la organización. Además, el cableado no se encuentra debidamente organizado ni segmentado por departamentos, lo que supone un riesgo adicional para la seguridad de la red.

RECOMENDACIONES

Basado en los resultados del escaneo del host principal utilizando la herramienta Nessus, se recomienda tomar medidas inmediatas para abordar las vulnerabilidades identificadas.

Se recomienda al director de tecnologías: Realizar una evaluación de riesgos para determinar el impacto potencial de las vulnerabilidades en el sistema, que está reflejada en la estrategia 1 que dice lo siguiente:

El municipio de Montalvo debe implementar medidas de seguridad informática como actualizaciones y parcheos de software ya que no todas las computadoras cuentan con licencias y como consecuencias lo hace vulnerable, instalar software de seguridad tales como firewalls y antivirus en todos los dispositivos y servidores de la red.

También se recomienda establecer el uso de contraseñas seguras y obligatorias otorgados por el área de sistemas, y un control de acceso y autenticación de usuarios con reglas de accesibilidad en horas laborables para evitar manipulaciones fuera de horario y con respecto a la navegación en la red implementar reglas que limiten el acceso a paginas indebidas y que no puedan descargar archivos maliciosos que pueda perjudicar la seguridad. Estas medidas ayudarán a proteger la información y sistemas del municipio de posibles intrusiones y virus.

BIBLIOGRAFÍA

Adrian, y. (19 de 03 de 2023). *ConceptoDefinicion*. https://conceptodefinicion.de/informatica/

Apen30. (2022). *Apen30 soluciones informaticas*. https://apen.es/glosario-de-informatica/hardware/

CISCO. (2023). *CISCO*. https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html#~how-network-security-works

Content, R. R. (2021). *RockConent*. https://rockcontent.com/es/blog/hardware-y-software/

CTi solociones. (2023). *CTi solociones*. https://www.ctisoluciones.com/blog/la-importancia-los-servicios-informaticos-la-empresa

Digicert. (2023). *web security digicert*. https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https

incibe_. (20 de 3 de 2018). *incibe_*. https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

InternetPasoAPaso. (2023). *InternetPasoAPaso*. https://internetpasoapaso.com/vulnerabilidades-sistemas-operativos/

Limones, E. (15 de 3 de 2021). *openWebinars*. https://openwebinars.net/blog/que-son-las-redes-informaticas-y-que-tipos-existen/

Luz, S. d. (22 de 12 de 2022). *RZ Redes Zone*. https://www.redeszone.net/tutoriales/seguridad/mejores-escaner-vulnerabilidades-gratis-hacker/

Panda security. (28 de 11 de 2022). *Panda mediacenter*. https://www.pandasecurity.com/es/mediacenter/seguridad/evaluacion-vulnerabilidad/

TARLOGIC. (2023). *TARLOGIC*. https://www.tarlogic.com/es/blog/owasp-top-10-vulnerabilidades-web/

Tokio. (2023). *TokioSchool*. https://www.tokioschool.com/noticias/tipos-redes-informaticas/

UNIR. (15 de 6 de 2021). *Unir la universidad en internet*. https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/

VMWARE. (2002). *VmWare*.

VMWARE. (2023). *VmWare*. https://www.vmware.com/latam/topics/glossary/content/application-security.html

ZOHO CORPORATION. (2023). *Manage Engine*. https://www.manageengine.com/latam/vulnerability-management/analisis-de-vulnerabilidades.html#:~:text=El%20an%C3%A1lisis%20de%20vulnerabilidades%20es,errores%20de%20configuraci%C3%B3n%20del%20sistema

ANEXOS

Anexo 1

Entrevista al personal del área de sistemas del GAD Montalvo.

Nombre: Ing. Richard Guerrero

Lugar de trabajo: GAD Montalvo

¿Qué medidas de seguridad considera más efectivas en la protección de los sistemas de información?

Mantener los sistemas actualizados con las últimas actualizaciones de seguridad y parches.

Implementar políticas de contraseñas sólidas y cambiarlas regularmente.

Configurar firewalls y sistemas de detección de intrusiones para evitar ataques externos.

Realizar regularmente copias de seguridad de los datos y almacenarlas en un lugar seguro fuera de las instalaciones de la empresa.

¿Cómo se asegura de que los datos y la información de la empresa estén respaldados y protegidos ante posibles fallas o ataques cibernéticos?

Realizo copias de seguridad regularmente en un dispositivo externo y las almaceno en un lugar seguro fuera de las instalaciones de la empresa.

Implemento políticas de seguridad de datos, como la limitación de acceso a la información confidencial solo a empleados autorizados.

¿Cuál ha sido la estrategia de seguridad informática más efectiva que ha implementado en su carrera profesional y por qué?

Realicé talleres y charlas sobre seguridad informática para que el personal comprendieran los riesgos de la seguridad informática y cómo prevenir posibles ataques. Como resultado, los personales de trabajo se volvieron más conscientes de la seguridad y tomaron medidas para proteger mejor la información que poseen.

Nombre: Ing. Oswaldo Cabrera

Lugar de trabajo: GAD Montalvo

¿Qué medidas de seguridad considera más efectivas en la protección de los sistemas de información?

Las medidas de seguridad más efectivas es el uso de contraseñas seguras y la autenticación multifactorial, la encriptación de datos, la implementación de firewalls y sistemas de detección de intrusiones, la actualización regular del software y la capacitación del personal.

¿Cómo se asegura de que los datos y la información de la empresa estén respaldados y protegidos ante posibles fallas o ataques cibernéticos?

se recomienda implementar sistemas de copias de seguridad y almacenamiento de datos en la nube, realizar pruebas regulares de recuperación de datos y contar con un plan de contingencia en caso de emergencias.

¿Cuál ha sido la estrategia de seguridad informática más efectiva que ha implementado en su carrera profesional y por qué?

La estrategia de seguridad informática más efectiva que he implementado en mi carrera profesional ha sido la implementación de un sistema de monitoreo de seguridad en tiempo real, que me permite detectar y responder rápidamente a posibles amenazas y ataques cibernéticos antes de que causen daño. Esto ha sido efectivo porque me permite

actuar de manera proactiva en lugar de reactiva en la protección de los sistemas de información.

Nombre: Ing. Winey Tapia

Lugar de trabajo: GAD Montalvo

¿Qué medidas de seguridad considera más efectivas en la protección de los sistemas de información?

La autenticación multifactorial, encriptación de datos, firewalls, sistemas de detección de intrusiones, actualizaciones regulares de software y capacitación de personal.

¿Cómo se asegura de que los datos y la información de la empresa estén respaldados y protegidos ante posibles fallas o ataques cibernéticos?

Se asegura mediante la implementación de sistemas de copias de seguridad y almacenamiento de datos en la nube, pruebas regulares de recuperación de datos y un plan de contingencia.

¿Cuál ha sido la estrategia de seguridad informática más efectiva que ha implementado en su carrera profesional y por qué?

La implementación de autenticación de múltiples factores ha sido la estrategia de seguridad informática más efectiva que he implementado debido a que reduce significativamente el riesgo de ataques de phishing y suplantación de identidad.

Anexo 2

Figura 2

Encuesta al personal de sistemas

Figura 3

Encuesta al personal de sistemas

Anexo 3

Instalación y ejecución de la herramienta Nessus y OpenVas

Figura 4

Descarga de Nessus

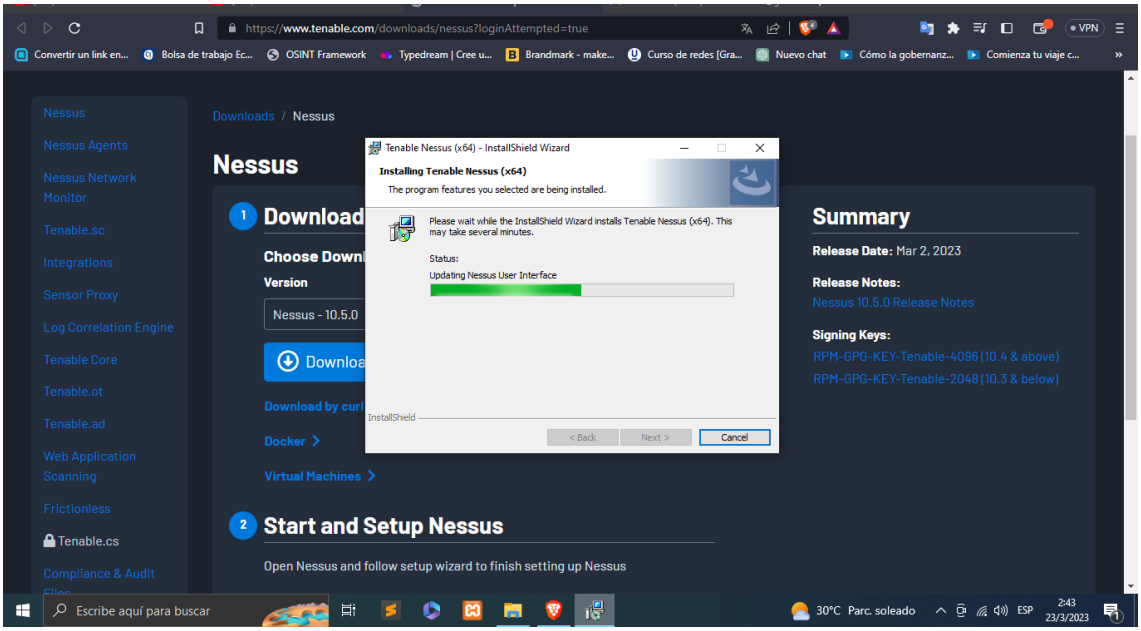


Figura 5

Iniciando Nessus

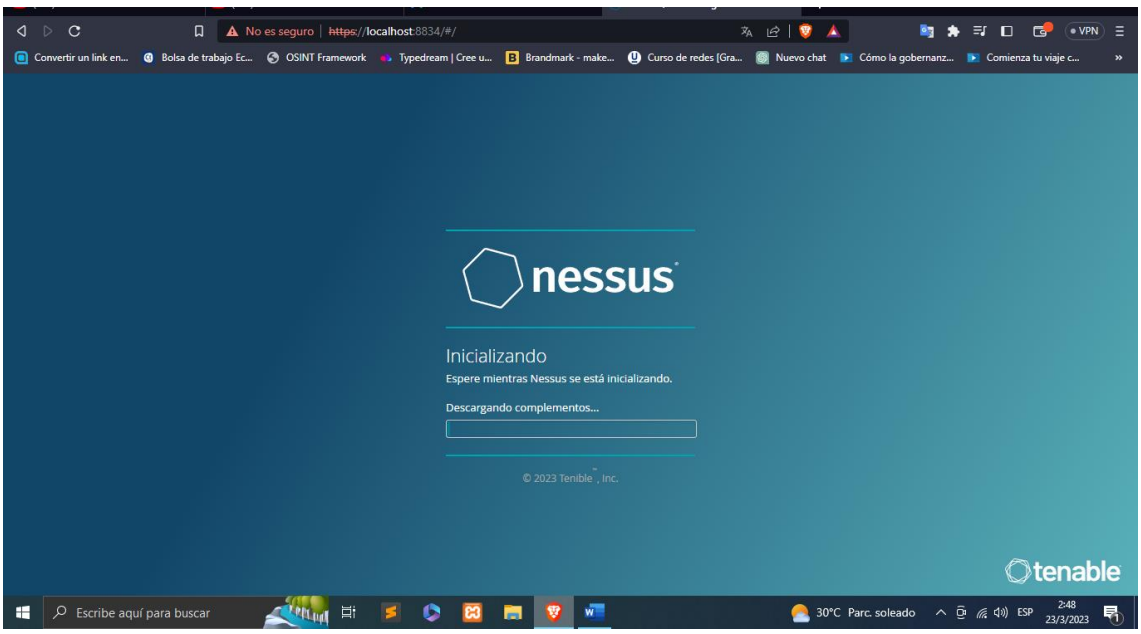


Figura 6

Iniciando OpenVas

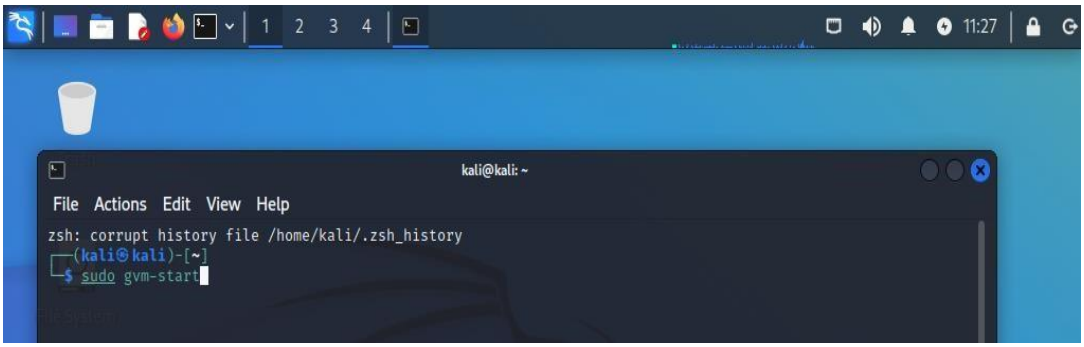


Figura 7

Interfaz desde el Navegador

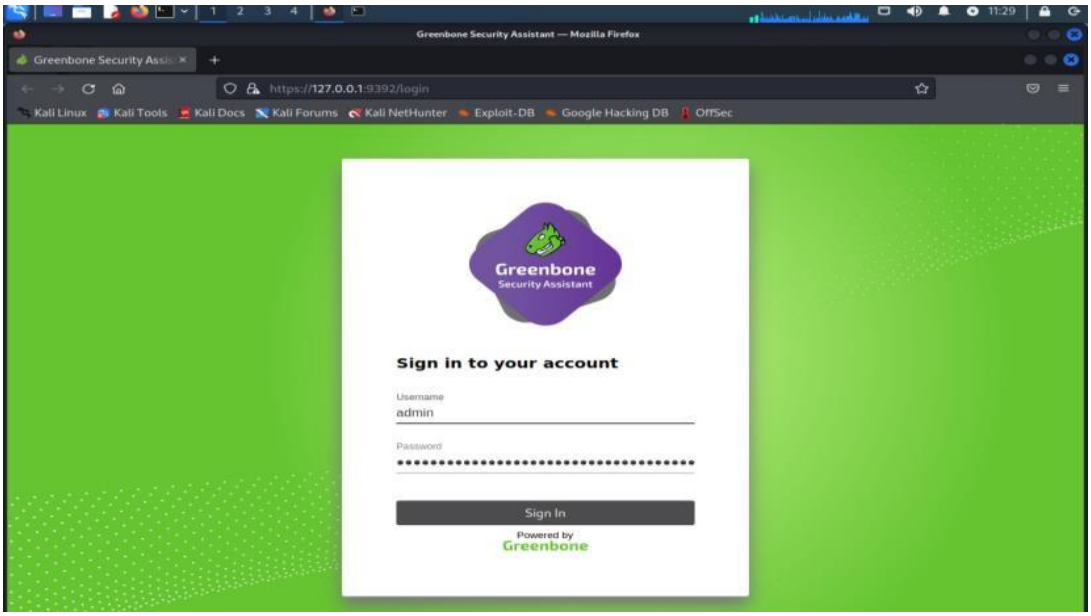


Figura 8

Gráficos de los Resultados

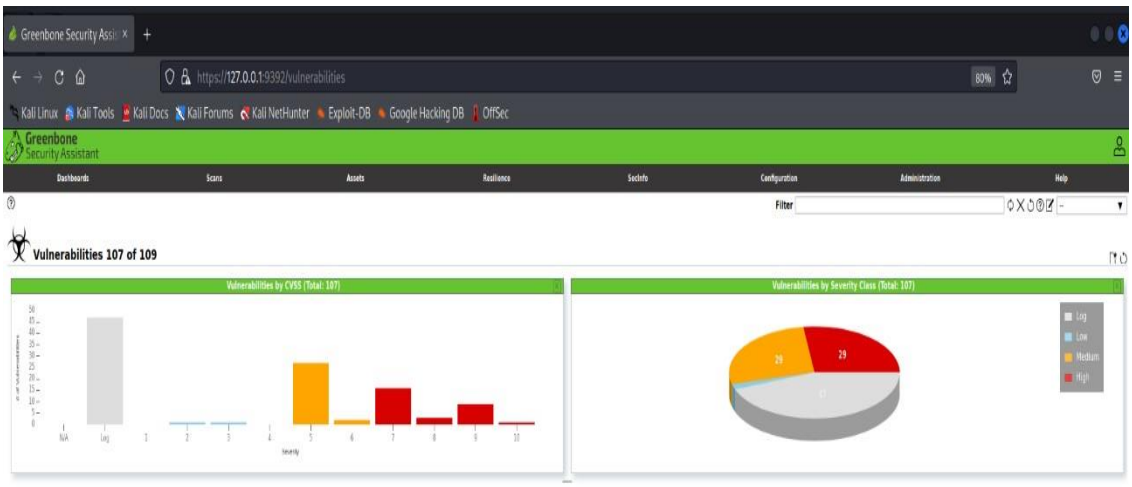


Figura 9

Nuevo escaneo en nessus

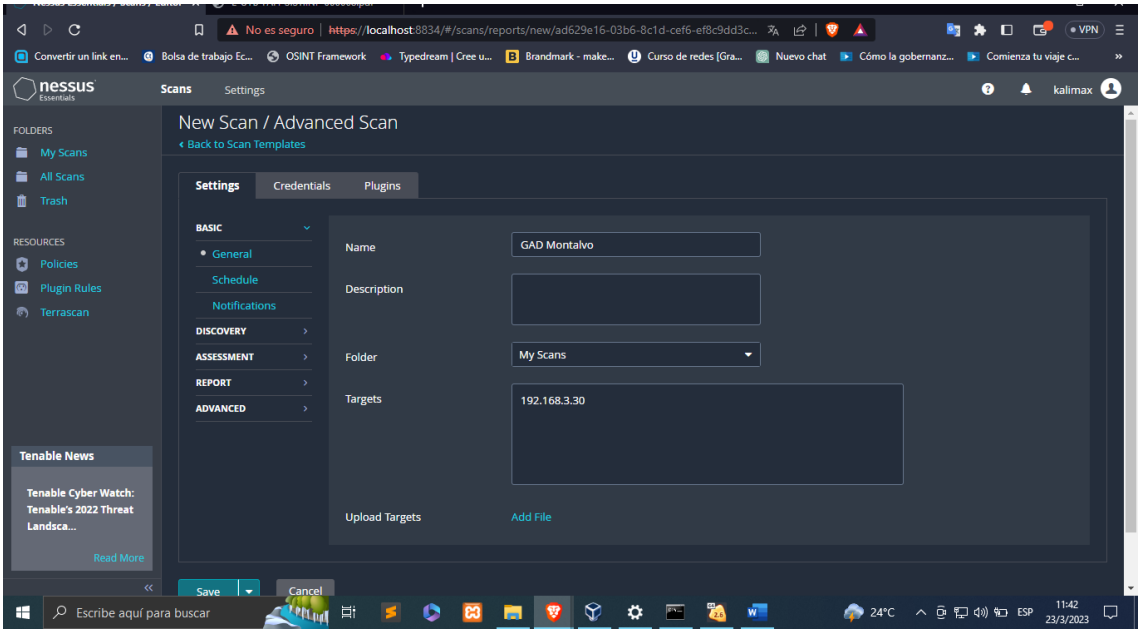


Figura 10

Resultados

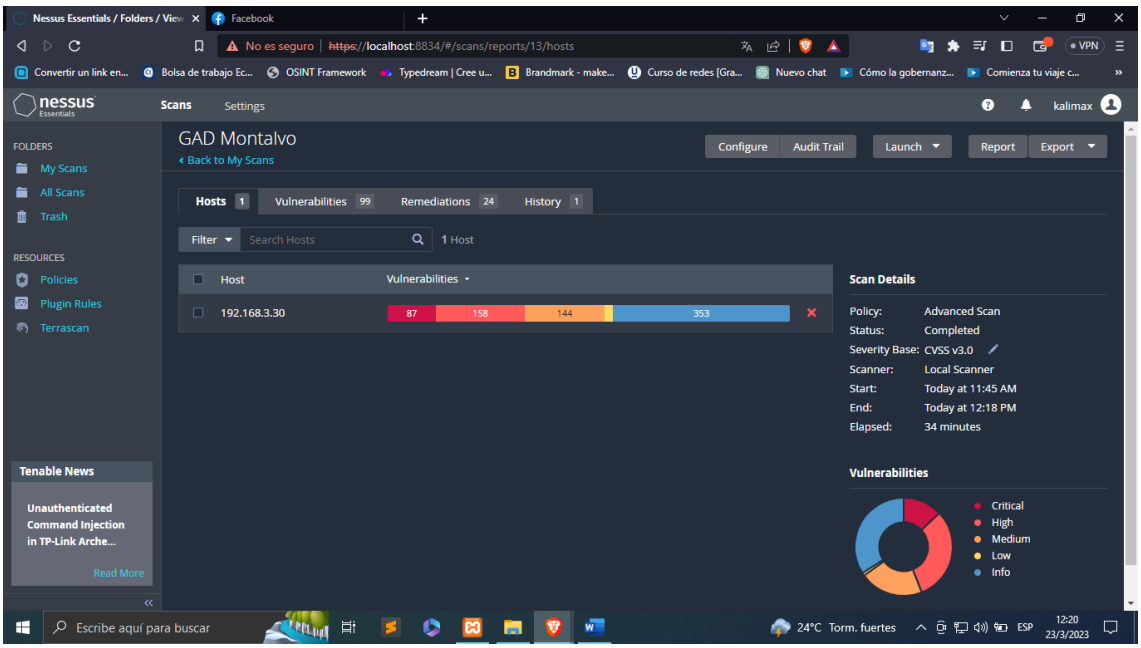


Figura 11

Lista vulnerabilidades

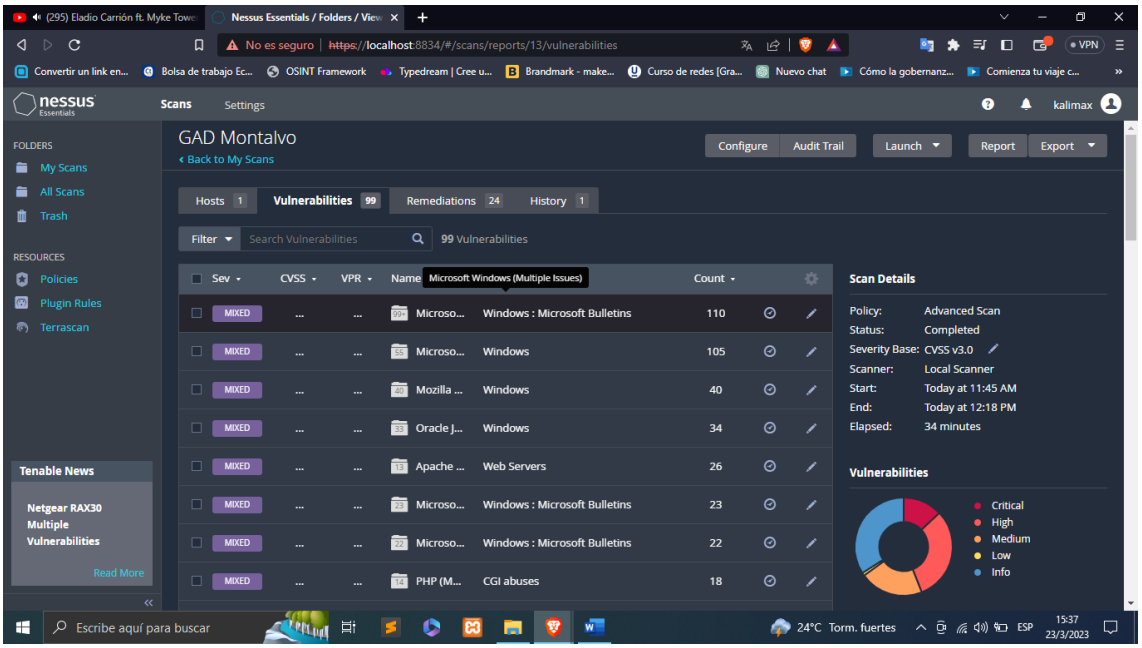


Figura 12

Lista vulnerabilidades

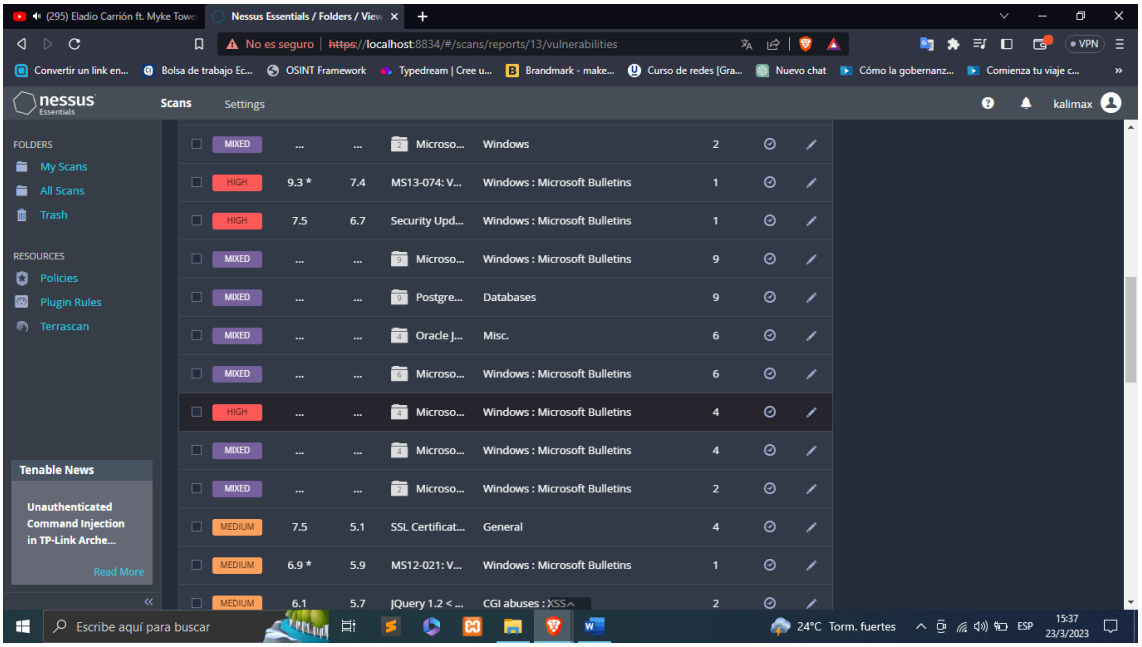


Figura 13

Lista vulnerabilidades

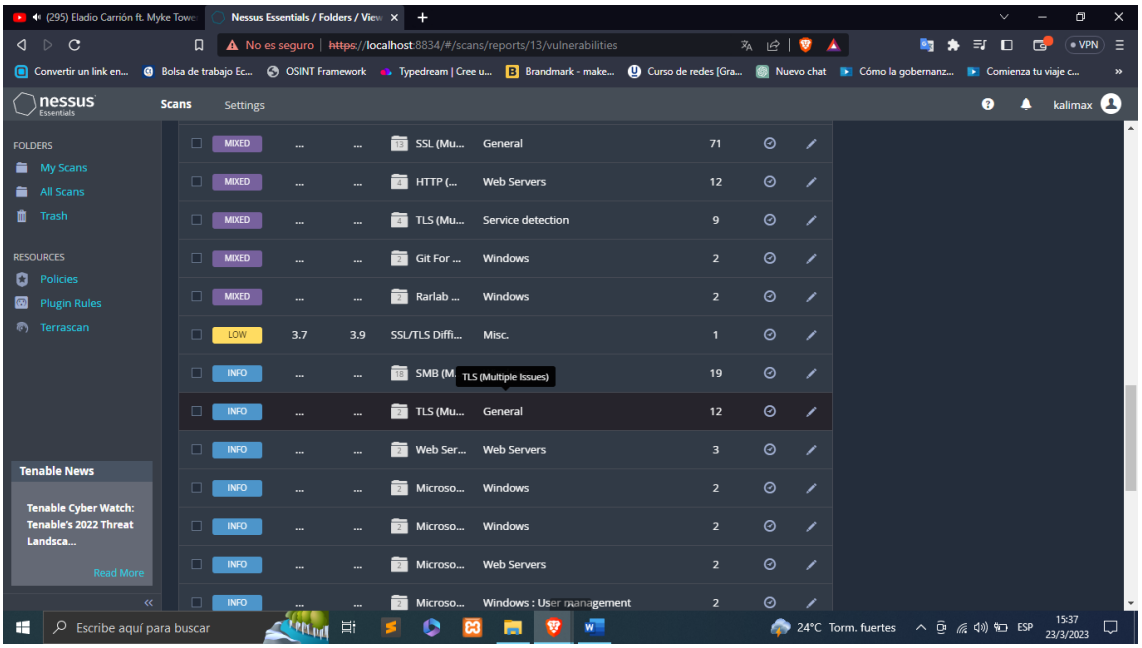
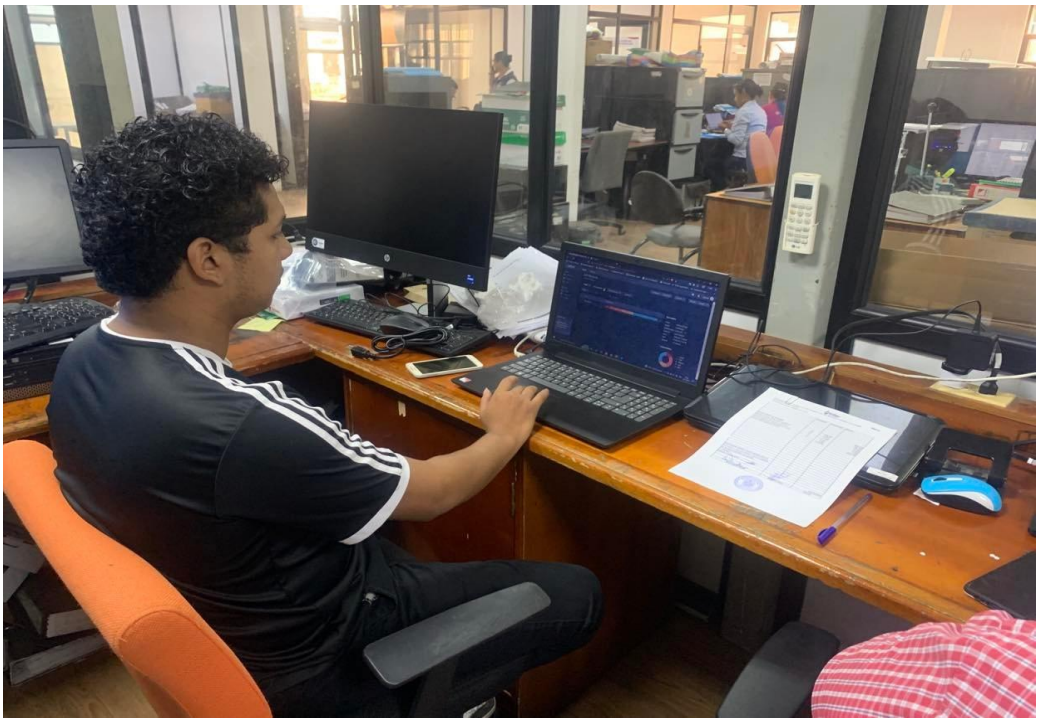


Figura 14

Ejecución de escaneo



Anexo 4

Vulnerabilidades encontradas

Tabla 1

Vulnerabilidad critica

vulnerabilidad	
Nombre:	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF
Impacto:	Critical
Descripción:	La versión de Apache httpd instalada en el host remoto es igual o superior a la 2.4.7 y anterior a la 2.4.52. Por lo tanto, está afectado por una falla relacionada con la actuación como proxy de reenvío.

Tabla 2

Vulnerabilidad critica

vulnerabilidad	
Nombre:	PostgreSQL 9.4.x < 9.4.24 / 9.5.x < 9.5.19 / 9.6.x < 9.6.15 / 10.x < 10.10
Impacto:	Critical
Descripción:	La versión de PostgreSQL instalada en el host remoto es 9.4.x anterior a 9.4.24, 9.5.x anterior a 9.5.19, 9.6.x anterior a 9.6.15, 10.x anterior a 10.10 o 11.x anterior

	a 11.5. Está, por tanto, afectado por múltiples vulnerabilidades: - Una vulnerabilidad no especificada que permite a un atacante ejecutar SQL arbitrario como propietario de la función. (CVE-2019-10208) - Existe una vulnerabilidad de manejo de contraseñas inseguras en el instalador de Windows de EnterpriseDB debido al uso de un archivo temporal. Un ataque puede explotar esto para leer la contraseña de superusuario de PostgreSQL del archivo. (CVE-2019-10210) - Existe una vulnerabilidad de ejecución de código arbitrario en libeay32.dll debido al uso de un directorio de configuración codificado. Un atacante puede explotar esto para cargar y ejecutar código arbitrario como usuario que ejecuta un servidor o cliente PostgreSQL. (CVE-2019-10211)

Tabla 3

Vulnerabilidad mediana

vulnerabilidad	
Nombre:	MS12-021: Vulnerability in Visual Studio Could Allow Elevation of Privilege
Impacto:	Medium

Descripción:	La versión instalada de Microsoft Visual Studio no valida correctamente los complementos en la ruta antes de cargarlos en la aplicación. Un atacante puede elevar sus privilegios colocando un complemento especialmente diseñado en la ruta que utiliza Visual Studio y convenciendo a un usuario con mayores privilegios para que inicie Visual Studio.

Tabla 4

Vulnerabilidad baja

vulnerabilidad	
Nombre:	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
Impacto:	Low
Descripción:	El anfitrión remoto permite conexiones SSL/TLS con módulos Diffie-Hellman que son menores o iguales a 1024 bits. Debido a esta debilidad, un tercero puede descubrir fácilmente el secreto compartido a través de criptoanálisis. La velocidad del proceso dependerá del tamaño del módulo y los recursos del atacante. Como resultado, es posible que un atacante pueda obtener acceso al texto sin cifrar o incluso comprometer la integridad de las conexiones.

Anexo 5

Montalvo
Gobierno Municipal

Oficio No. GADMCM-UTH-2023-051-SKMH
Montalvo, 14 de marzo del 2023

LCDO. MAE.
Eduardo Gáleas Guijarro.
DECANO DE LA UNIVERSIDAD TECNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
En su despacho.-

De mi consideración.

Expresándole un cordial y afectuoso saludo, en atención al oficio N° D-FAFI-UTB-0028-2023 con fecha 23 de enero del 2023, y recibido en esta unidad el 09 de marzo del 2023.

Con lo expuesto en el oficio antes descrito, se autoriza el ingreso al señor NARANJO ALCÍVAR STEVEN ALEXANDER estudiante de la carrera de Sistemas de Información de la Universidad Técnica de Babahoyo, para que realice el Caso de Estudio en el tema ANALISIS DE ESTRATEGIAS PARA BRINDAR SEGURIDAD INFORMATICA EN LAS REDES Y SERVIDORES DEL GAD MUNICIPAL DEL CANTON MONTALVO, en el área de tecnologías de la Información y Comunicaciones del GAD Municipal del Cantón Montalvo.

Particular que pongo a su conocimiento para los fines consiguientes.

Atentamente,

Ing. Sonnia Moncayo Hernández
Jefe de Administración de Talento Humano

Elaborado por: Tlga. María Aldaz Silva-SECRETARIA DE UNIDAD	

Dirección: Av. Antonia de la Bastida y 10 de Agost
Email: municipiomontalvo@montalvo.gob.ec
www.montalvo.gob.ec