UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2022 – MAYO 2023

EXAMEN COMPLEXIVO DE FIN DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERA EN SISTEMAS DE INFORMACION

TEMA:

SISTEMA DE CIBER SEGURIDAD PARA LA RED DE COMUNICACIÓN DE LA UNIVERSIDAD TECNICA DE BABAHOYO BASADO EN SISTEMAS DE CODIGO ABIERTO

ESTUDIANTE:

CARMEN ADRIANA MUÑOZ VERA

TUTOR:

ING. SOTO VALLE CARLOS JULIO

AÑO 2023

RESUMEN

El presente caso de estudio Ambiciona modernizar la Infraestructura de Red informática a través de la implementación de hiperconvergencia que permita seccionar por módulos, donde se prioriza poner en marcha un módulo de firewall que se dedique al control del tráfico de red así mismo proponer políticas de seguridad con base en configuraciones de firewall descubiertas durante el proceso de investigación, se propone el desarrollo del presente caso de estudio con el fin de flexibilizar la escalabilidad de la red, reforzar el respaldo de seguridad para los usuarios de la misma, con esto se pretende presentar políticas de seguridad que incrementen los protocolos de seguridad vigentes en la actualidad.

Objetivos detallados y concretos a cumplir: Analizar e Identificar los puntos débiles de la red informática, Presentar las respectivas correcciones que requieran un mínimo esfuerzo para mantener el bajo costo de ejecución, Proponer los respectivos ajustes y protocolos de seguridad que mantienen considerables beneficios y bajos costos de implementación para la red informática.

Adicionalmente se resalta que gracias a este caso de estudio se dio a conocer la cuales son los requerimientos en software que necesita la Universidad Técnica de Babahoyo para implementar un conjunto de reglas y configuraciones que aumenta la protección frente a ataques informáticos, generando mayor prevención lo que significa mayor confianza para los usuarios de la red.

PALABRAS CLAVES: Firewall, Hiperconvergencia, PFsense, Vulneración, Portal Cautivo, Escalabilidad.

ASTRACT

This case study aims to modernize the IT Network Infrastructure through the implementation of hyperconvergence that allows sessions by modules, where the launch of a firewall module dedicated to controlling network traffic is prioritized, as well as proposing security politics. Based on the firewall configurations discovered during the research process, the development of this case study is proposed in order to make network scalability more flexible, reinforce security support for its users, with this it is intended to present security policies that increase the security protocols in force.

Detailed and specific objectives to be met: Analyze and identify the weak points of the computer network, Present the respective corrections that require a minimum effort to maintain the low cost of execution, Propose the respective adaptations and security protocols that maintain considerable benefits and low costs implementation for the computer network.

Additionally, it is highlighted that thanks to this case study, the software requirements that the Technical University of Babahoyo needs to implement a set of rules and configurations that increase protection against computer attacks, generating greater prevention, were made known. which means greater confidence for network users.

KEY WORDS: Firewall, Hyperconvergence, PFsense, Vulnerability, Captive Portal, Scalability.

INDICE

PLANTEAMIENTO DEL PROBLEMA

La universidad Técnica de Babahoyo es la institución de educación Superior más Importante del Cantón Babahoyo, la cual se encuentra ubicada en la Av. Universitaria, se caracteriza por Formar profesionales y académicos, líderes y emprendedores con valores éticos y morales con conocimientos científicos y tecnológicos que promuevan la investigación, transferencia de tecnología e innovación y extensión de calidad, para contribuir en la transformación social y económica del país.

El problema principal es la falta de medidas de seguridad en las redes es un contratiempo que está creciendo considerablemente, debido a que existen un mayor número de atacantes y también al descuido por parte de sus administradores, por lo cual se pone en peligro la integridad y confidencialidad de la información de la institución, la misma puede quedar expuesta a usuarios no autorizados o a la modificación por parte de un especialista. La cuestión presentada el contar con una red informática sin ningún tipo de filtro de seguridad es la vulnerabilidad que demuestra ante el asedio de ciberdelincuentes o persona mal intencionada. Ya que resulta relativamente sencillo para un hacker obtener información, modificarla o secuestrarla.

Las amenazas presentes pueden ser muy invasivas o poco perceptible, en caso de presentarse un ataque muy agresivo los usuarios de la red lo detectarán, aunque ya sea tarde para tomar acciones preventivas, lo que no sucede cuando el ataque se presenta de forma sigilosa donde el usuario puede ser espiado o vulnerado sí que él, se dé cuenta que dicha invasión ajena a la red.

Los ataques suelen provenir en la mayor parte de la red interna que externa, donde pretenden acceder legítimamente a la información de los routers ya sean para modificar, eliminar

o sustraer la información y afectar el funcionamiento de los servicios, es por ello que los administradores deben conocer el comportamiento normal de tráfico de la red, hacer uso de herramientas que los ayuden a la detección de intrusos y posibles ataques para poder tomar las medidas pertinentes.

Los administradores de dominios se han convertido en uno de los principales objetivos para la escala de privilegios, facilitar el movimiento lateral al aprovechar fallas y configuraciones incorrectas. Y si de reducir costos se trata empezar por aprovechar los recursos Open Source que existen a día de hoy, que ofrecen las mismas bondades que un servicio de paga, dentro de Linux, PFSense es una Herramienta que permite tener un servicio de firewall avanzado, el cual tolera la sectorización, donde cada zona cuenta con políticas configurables para gestionar correctamente el flujo del tráfico de red, eliminar rutas de ataque, permite que los atacantes tengan problemas para encontrar una ruta de incursión y evitar su avanza en caso de encontrarlo.

Un sistema de ciberseguridad para la red de comunicación de la Universidad Técnica de Babahoyo basado en sistemas de información geográfica (SIG) puede ser una herramienta útil para ayudar a la universidad a identificar y prevenir amenazas cibernéticas. Esto se logra a través del uso de la tecnología SIG para monitorear y detectar actividades sospechosas en la red. Esto también ayudaría a la universidad a tomar medidas para prevenir futuras amenazas.

Los principales componentes de un sistema de ciberseguridad basado en SIG incluyen la recopilación de datos, el análisis de datos, el monitoreo en tiempo real y la implementación de medidas de seguridad. En primer lugar, el sistema recopilará datos sobre la red y los usuarios de la universidad. Estos datos incluirían información como la ubicación de la red y los dispositivos conectados, el tráfico de la red, el comportamiento de los usuarios y la actividad en línea. Estos datos se recopilarán a través de herramientas de monitorización de la red y de análisis de tráfico.

Una vez que se haya recopilado la información, el sistema pasará a analizar los datos de la red para identificar actividades sospechosas. Esto se logra a través del uso de algoritmos de aprendizaje automático para detectar patrones anómalos en el tráfico de la red. Estos patrones se compararán con los patrones de actividad establecidos en la base de datos para determinar si hay alguna amenaza cibernética.

Una vez que el sistema haya identificado algunas amenazas potenciales, se implementarán medidas de seguridad para prevenir futuras amenazas. Estas medidas incluirían la configuración de firewall, el uso de herramientas de cifrado, la instalación de software antivirus y la creación de una red segura. Estas medidas ayudarán a la universidad a proteger la red de futuras amenazas cibernéticas.

En resumen, un sistema de ciberseguridad para la red de la Universidad Técnica de Babahoyo basado en SIG es una herramienta útil para ayudar a la universidad a identificar y prevenir amenazas cibernéticas. El sistema recopilará datos sobre la red y los usuarios, los analizará para identificar actividades sospechosas y luego implementará medidas de seguridad para prevenir futuras amenazas. Esto permitirá a la universidad mantener un ambiente seguro para sus usuarios y una red segura para sus datos.

JUSTIFICACIÓN

La Universidad Técnica de Babahoyo necesita un sistema de ciberseguridad para proteger su red de comunicaciones. El sistema debe ser capaz de proteger la red contra amenazas externas, como el malware, el phishing y el hacking, así como detectar y prevenir intrusiones internas. El sistema de ciberseguridad también debe ser capaz de gestionar el acceso de los usuarios a los recursos de la red, incluso controlar el ancho de banda y la velocidad de conexión.

Para garantizar una red segura, el sistema de ciberseguridad ha de incluir una serie de medidas de seguridad, como el aislamiento de la red, el cifrado de los datos, la autenticación de los usuarios, la gestión de la seguridad de los dispositivos móviles, el control de acceso basado en reglas, y el control de la vulnerabilidad de la red.

Además, el sistema de ciberseguridad debe incluir herramientas de detección de amenazas, como el análisis de tráfico en tiempo real, el análisis de contenido, el análisis de registros, la detección de intrusos y el análisis de comportamiento. Estas herramientas permiten detectar y prevenir los intentos de intrusión y otros ataques.

Por último, el sistema de ciberseguridad debe proporcionar una solución de seguridad de extremo a extremo, desde el punto de acceso hasta la nube. Esto incluye la implementación de una red segura, el control de acceso a la red, el filtrado de contenido, el análisis de amenazas y la gestión de la seguridad de los dispositivos. Estas medidas ayudan a proteger la red de cualquier intento de intrusión y aseguran la integridad de los datos.

Tener una red Informática sin ningún tipo configuración de seguridad representa un objetivo sencillo de vulnerar, se conoce que la mayoría de empresas pequeñas no cuentan con el capital necesario para invertir en un Perito informático. Que se encargue de garantizar la

integridad de la red informática. Por lo que es importante establecer configuraciones sencillas que no representen gran costo para obtener la solidez en la red informática generando más confianza en las labores de los miembros activos de la Universidad Técnica de Babahoyo.

La importancia de establecer una serie de configuraciones que representen un bajo costo para la implementación de una red informática segura. Para sentar las bases de una buena cultura de prevención ante los ataques malintencionados que puedan presentarse en la red. Con intenciones de afectar la integridad de los usuarios, obtener datos personales, secuestrar información relevante, o simplemente afectar el bienestar de los miembros de la red.

Las bondades que representa tener un nivel de seguridad básica. Pueden ser muchísimos al compararlos con una red totalmente vulnerable. Ya que puede evitar la infiltración de un intruso en la red o por lo menos hacerse presente como una dificultad donde el atacante puede desistir de su asedio a la red. Además de generar la confianza necesaria para desempeñar sus actividades diarias haciendo uso de la red sin miedos, y permitiendo el desarrollo de la empresa en la que este implementaba esta metodología de seguridad.

Ofrecer un conjunto de configuraciones de seguridad, que brinde las garantías necesarias para que los usuarios de la red se sientan protegidos, tomando en cuenta: Puertos, Ips, segmentación de red, Dns. Como aspectos importantes dentro de una red para gestionar el tráfico de la red junto con las actividades de los usuarios además de controlar y limitar las actividades que realizan los usuarios, dejando en funcionamiento las funciones indispensables para el correcto desempeño de los usuarios dentro de la red informática.

Los beneficios obtenidos son evidentes ya se contará con un respaldo de investigación para evitar incursiones dentro de la red institucional de la Universidad técnica de Babahoyo,

presentando los protocolos que salvaguardan la integridad de la información en bases de datos, datos administrativos y los datos personales de los estudiantes, sobremanera la presente investigación permitirá la capacitación del personal administrativo sobre el tema de seguridad informática.

OBJETIVOS DEL ESTUDIO

OBJETIVO GENERAL

Identificar los parámetros de la red informática que pueden enriquecer la seguridad para la red de comunicación de la universidad técnica de Babahoyo, tomando como principal argumento los bajos costos

OBJETIVOS ESPECÍFICOS

- Analizar e Identificar los puntos débiles de la red informática
- Presentar las respectivas correcciones que requieran un mínimo esfuerzo para mantener el bajo costo de ejecución
- Proponer los reglas y configuraciones de seguridad que mantienen considerables beneficios y bajos costos de implementación para la red informática.

LÍNEA DE INVESTIGACIÓN

Sistemas de información y comunicación, emprendimiento e innovación.

SUBLÍNEA DE INVESTIGACIÓN

Redes y tecnologías inteligentes de software y hardware.

MARCO CONCEPTUAL

La identificación de los eslabones más débiles de la red es el primer paso a realizar para lo cual la investigación es la herramienta fundamental para enunciar cuáles son las falacias más comunes presentes en la red. Fomentar la prevención mediante la seguridad activa adelantándose a la posible vulneración de la red, generar una barrera de seguridad física y lógica para reducir los riesgos.

Los servidores Linux son más usados de forma profesional, ya que permite configurar muchos aspectos y se comporta con la robustez y el nivel necesario en todos los escenarios que se le imponga, siempre responde con la estabilidad y seguridad, además que por su eficiencia es menos susceptible a requerir mantenimientos en periodos cortos.

Afirmando (Ortega Candel, 2021)que la ciberseguridad es la encargada de salvaguardar los activos digitales, incluyendo redes, hardware y programas, y la información que es procesada, almacenada en sistemas o transportada a través de espacios de información interconectados, y nos referimos al grupo de ingeniería, gerencia sistemas y otras medidas destinadas a defender la información digital y los medios que trabajan en ella de incidentes intencionales y accidentales. (pág. 2)

Esto confirma (Alegre Ramos, 2021) que actualmente no se entienden las computadoras que funcionan separadas de otras PC, en las que la noción de una red de computadoras a partir de un sistema operativo en red juega un papel bastante fundamental en la informática. Un sistema operativo de red es cualquier cosa que nos permite trabajar en una red y explotar y compartir los recursos de red de la PC. (pág. 2)

Señaló (Smyth, 2019) que el plan CentOS, originalmente un esfuerzo basado en una asociación que usaba el código fuente de Red Hat Enterprise Linux, eliminó los requisitos de marca y suscripción de Red Hat, excluyendo la entrada al soporte técnico de Red Hat Linux. para recibir actualizaciones repetidas u ofrecer soporte contra exploits maliciosos.

Asegura (Gonzalez, 2022) que una red de computadoras se puede definir como un sistema de dispositivos interconectados que son capaces de comunicarse usando ciertos estándares comunes llamados protocolos. Dichos dispositivos se comunican para compartir recursos como archivos, impresoras y servicios. (pág. 3)

Esto sugiere (Romero Castro, y otros, 2018) que la seguridad está constantemente orientada a gestionar los peligros, lo que significa que siempre hay una manera de evitarlos o prevenirlos y que se pueden tomar ciertas acciones para evitar estas situaciones de la mejor manera posible. Se ha determinado que la estabilidad se puede catalogar como la ausencia de peligro, la definición de este término implica 4 actividades que constantemente quedan inmersas en algún tipo de problema de estabilidad, tales como: evitar el peligro, transferir el peligro, mitigar el peligro, aceptar el peligro. (pág. 13)

Revela (Francois Campertier, 2016) que la política de Seguridad tiene como objetivo conceptualizar el mantenimiento de los sistemas de información organizacional. Incluye un grupo básico para conceptualizar varias tácticas, pautas, métodos, códigos de conducta. Y normas organizativas y técnicas. Esto implica el uso de una defensa adecuada para el uso, económica y conforme a la ley. Estas políticas deben formalizarse dentro de la organización porque los archivos pueden presentar un resumen de las prácticas que rigen cómo administrar, retener y transmitir información importante o confidencial que forma parte de la organización. (pág. 54)

Menciona (Hewlett-Packard Company, 2021) que un firewall es un sistema diseñado para proteger redes privadas de intrusiones no autorizadas y no confirmadas en una conexión de red de Internet. Estos tienen la posibilidad de ser del tipo hardware o programa o una combinación de ambos. Entonces, ¿qué están haciendo realmente? Los cortafuegos protegen su PC o un conjunto de PC en una red de sitios web infectados con malware o puertos de red abiertos vulnerables. Ayudan a detener a los posibles atacantes antes de que puedan hacer daño. Los cortafuegos de red se encuentran en organizaciones, hogares, escuelas e intranets, que son redes privadas dentro de una organización. Además, se pueden configurar para evitar que los usuarios de la red accedan a sitios web externos.

Expresa (Aggarwal, 2018) que garantiza que PFSense sea un programa rico en funciones, robusto y altamente flexible. Además de la funcionalidad principal del firewall, hay muchas características adicionales para el enrutamiento de la red, la conectividad remota, el diagnóstico y la generación de informes, así como capacidades de aprovisionamiento rápido. No es necesario configurar sus propios accesorios. Todas las características de nivel empresarial y la estabilidad que ofrece pfSense lo convierten en un impresionante producto gratuito y de código abierto. Ejecutar configuraciones grandes y complejas generará mayores beneficios. Tiene la opción de comprar soporte de una licencia de experto. Pero es completamente opcional. (pág. 8)

Afirma (De Luz, 2023) que las VLAN o “redes de área local virtuales” nos permiten crear redes lógicamente independientes dentro de la misma red física usando switches administrados que soportan VLAN para segmentar adecuadamente la red. También es muy importante que los routers que utilicemos soporten VLANs, de lo contrario no podremos gestionarlos todos y permitir o bloquear la comunicación entre ellos. Hoy en día, la mayoría de

los enrutadores profesionales e incluso los sistemas operativos orientados a firewall/enrutador como pfSense u OPNsense admiten VLAN.

Según (Davis, 2019) las VLAN anidadas son un método para dividir una red en segmentos más pequeños para mejorar la administración y la seguridad de la red. Una VLAN (red de área local virtual) es una red lógica que agrupa dispositivos en una red física por ubicación, función o departamento. Las VLAN anidadas le permiten crear subredes dentro de las VLAN existentes, lo que aumenta la flexibilidad y la eficiencia de la red.

Las VLAN tradicionales agrupan los dispositivos en función de criterios como la ubicación geográfica o la función dentro de una sola red lógica. Sin embargo, esta estructura puede volverse inmanejable si hay muchos dispositivos o departamentos diferentes en la misma VLAN. Las VLAN anidadas le permiten lograr una granularidad más fina al dividir una VLAN en varias sub-VLAN.

Las declaraciones de (Liska & Stowe, 2016) sobre la seguridad del DNS son esenciales porque existen muchos agujeros de seguridad en el marco del DNS. Además de las fallas de seguridad habituales, como fallas de hardware, acceso no autorizado al servidor y ataques DDoS, también existen problemas de administración de datos, marketing de baja calidad y otros tipos de violaciones de seguridad solo de DNS. La naturaleza distribuida de DNS requiere automáticamente diferentes consideraciones de seguridad y aumenta la complejidad de los planes de seguridad. (pág. 8)

Según (Gerend, Downie, Ross, Prittie, & Mclllece, 2023), cada dispositivo en una red basada en TCP/IP requiere una dirección IP de unidifusión única para acceder a la red y sus recursos. Sin DHCP, las direcciones IP de las computadoras nuevas o las computadoras movidas

de una subred a otra deben configurarse manualmente, y las direcciones IP de las computadoras eliminadas de la red deben obtenerse manualmente. Con DHCP, todo este proceso está automatizado y administrado de forma centralizada. Un servidor DHCP mantiene un conjunto de direcciones IP y asigna direcciones a cada cliente habilitado para DHCP a medida que se inicia en la red. Debido a que las direcciones IP son dinámicas (otorgada) en lugar de estáticas (asignadas de forma permanente), las direcciones que ya no están en uso se devuelven automáticamente al grupo para su reasignación.

Él (Waschke, 2017) afirma que Secure Shell (SSH) requiere que una entidad de registro se identifique con credenciales y contraseñas seguras. Los datos que pasan a través de Secure Shell están encriptados. Cualquiera que quiera acceder a los datos primero debe descifrarlos. Esto hace que Secure Shell sea más privado. Los usuarios de Secure Shell son mucho más seguros. Sin embargo, los piratas informáticos han ideado formas de eludir Secure Shell y utilizarlo en los sistemas de seguridad. (pág. 15)

Explica (Zientara, 2018), sobre los cambios de DNS se propagan relativamente rápido, pero la naturaleza distribuida del DNS y el hecho de que no está completamente automatizado significa que los cambios de DNS pueden tardar horas en propagarse. Puede ser un problema si la dirección IP cambia con frecuencia. DDNS en realidad se refiere a dos servicios separados. El primer servicio utiliza un cliente para ejecutar DNS remoto y enviar cambios. El segundo es actualizar registros heredados sin edición manual. (pág. 116).

Menciona (Preston, 2022) que las extensiones de seguridad del sistema de nombres de dominio (DNSSEC) son firmas criptográficas que se agregan a los registros DNS para proteger los datos enviados a través de redes de protocolo de Internet (IP).

DNSSEC funciona agregando firmas criptográficas a los registros DNS existentes para configurar un DNS seguro. Las firmas se almacenan en servidores de nombres DNS con tipos de registros comunes, como AAAA y MX. A continuación, puede verificar que el registro provino directamente del servidor de nombres autoritativo comprobando la firma correspondiente al registro DNS solicitado. Esto significa que los registros nunca se han alterado ni manipulado durante la transmisión digital, lo que evita la introducción de registros falsos. DNSSEC existe porque los arquitectos fundadores del DNS no incluyeron medidas de seguridad de protocolo. Esto permitió a los atacantes encontrar oportunidades para falsificar registros y dirigir a los usuarios a sitios web maliciosos. Por lo tanto, se introdujo el protocolo DNSSEC para agregar una capa de confianza e integridad a las respuestas DNS.

Indica (Zientara, 2018) que cuando un portal cautivo está habilitado en su red, garantiza que los usuarios que intenten acceder a su red desde una computadora de escritorio/portátil o dispositivo móvil sean dirigidos primero a una página web. Los portales cautivos se pueden activar en redes cableadas, pero generalmente se usan como guardianes para redes inalámbricas. Cuando un usuario se conecta a una red protegida por un portal cautivo, se muestra la página del portal cautivo. A continuación, el usuario intenta acceder a la URL. Si la solicitud de URL es de un cliente desconocido. Los sistemas operativos de red reconocen que los usuarios deben pasar por un portal cautivo para obtener acceso completo a la red. (pág. 77)

Él (Deb Chowdhury, 2021) afirma que el propósito básico de NTP es proporcionar sincronización de tiempo entre dispositivos de red específicos al hacer referencia a una fuente de reloj con autoridad absoluta o relativa. El reloj absoluto representa la hora GNSS/GPS que se puede rastrear hasta UTC, la hora relativa representa la hora en el dispositivo con la que se deben sincronizar todos los demás dispositivos de red, pero la hora está en UTC con la que se

sincroniza. No se deriva ni se vincula a cualquier fuente. El tiempo relativo es el tiempo establecido por el administrador de la red para aproximarse a la hora de un reloj eléctrico en la pared dentro del edificio donde se implementa la red. (pág. 2)

Indica (Bottini, 2022) SSL mantiene seguras las conexiones a Internet, protege la información confidencial que se envía entre dos sistemas y evita que los delincuentes lean o modifiquen los datos en tránsito, incluida la información que podría considerarse privada. SSL utiliza algoritmos de cifrado para codificar los datos transmitidos, haciéndolos ilegibles para los piratas informáticos cuando se envían a través de una conexión. Esta información puede ser información confidencial o de identificación personal, como números de tarjetas de crédito y otra información bancaria, nombres y direcciones.

Menciona (Fernandez, 2022) sobre protocolo simple de gestión de redes. El protocolo SNMP está disponible en casi cualquier dispositivo que pueda conectarse a una red. También puede monitorear y ajustar de forma remota la configuración de su equipo monitoreado. Este registro orientado a gráficos. Cada dispositivo administrado tiene un agente que se comunica con el dispositivo central que lo administra.

Indica (Simpson & Novak, 2018) VMware Workstation Player ejecuta máquinas virtuales existentes (a veces llamadas dispositivos o vApps) y apunta a versiones gratuitas y con licencia para sistemas Windows y Linux. Un dispositivo virtual o vApp es una máquina virtual configurada para ejecutar una aplicación o servicio específico. VMware Workstation facilita la ejecución de máquinas virtuales creadas con VWware. Workstation Player es un excelente hipervisor tanto para usuarios domésticos como para estudiantes. (pág. 511)

Explica (Botto-Tobar, Díaz Cadena, León-Acurio, & Montiel Díaz, 2019) que la implementación de la hiperconvergencia en los centros de datos puede abordar problemas como el escalamiento, la disponibilidad y el respaldo, por lo que los servicios alojados siempre están accesibles, y este no es el caso. caso de los servicios tradicionales. arquitectura. La hiperconvergencia consolida el almacenamiento, las redes y los servidores, permite una conectividad asequible con otras tecnologías, como la computación en la nube de alta disponibilidad, y permite a los administradores mejorar el rendimiento de la infraestructura. Esto le permite reducir el tiempo de inactividad del servicio, tolerar períodos cortos de inactividad y maximizar la disponibilidad y la eficiencia del servicio. (pág. 65)

Según (Chakraborty, Ghosh, & Kumar Mandal, 2022), Nutanix Hybrib Cloud se basa en el concepto de HCI. Cualquier plataforma en la nube generalmente consta de tres partes principales: cómputo, almacenamiento y red. HCI fusiona dos de ellos. El objetivo aquí es reducir los gastos generales asociados con estas partes. Por ejemplo, es posible que necesite almacenar datos de funciones Informáticas. Sin embargo, no tener medios informáticos y de almacenamiento juntos puede generar costos. En este caso, los datos deben enviarse a través de la red al dispositivo de almacenamiento. El ancho de banda se considera el recurso más caro de la red. La combinación de procesamiento y almacenamiento evita este costo de movimiento. Esta es la idea detrás de la infraestructura hiperconvergente de Nutanix.(pág. 362)

MARCO METODOLOGICO

En el desarrollo del presente caso de estudio se aplicó el método cuantitativo y cualitativo con el Objetivo de Obtener la Información necesaria de las herramientas y el modelo de estructura utilizados actualmente en la Red Informática de la Universidad Técnica de Babahoyo para el cual se considera la entrevista como la mejor alternativa de recolección de información. Cuya entrevista está dirigida al ingeniero Luis Alcivar Torres. Jefe de Operaciones del área de Sistemas, de refuerzo para la investigación se hace una encuesta dirigida a estudiantes y profesores como miembros activos y usuarios regulares de la red informática de la institución.

La presentación del análisis de los beneficios de tener un software dedicado a la protección firewall además de las bondades de contar con un entorno de hiperconvergencia se realiza mediante tablas comparativas que hacen evidente el propósito de la presente investigación, lo que hace posible desarrollar reglas para la configuración del firewall demostrando que es relevante realizar dichos ajustes en el sistema para acrecentar el respaldo de seguridad en la Institución educativa.

A continuación, se presentan la lista de preguntas utilizadas en la encuesta:

1. ¿La seguridad informática es un factor relevante en su vida diaria?
2. ¿Usted tiene conocimiento sobre la función de un firewall?
3. ¿Considera usted que la red de la Universidad Técnica de Babahoyo le ofrece la suficiente seguridad?
4. ¿Tiene conocimiento usted sobre los softwares que imitan el funcionamiento de un ordenador físico, es decir crean entornos virtualizados?
5. ¿Opina usted que la red universitaria es lo suficientemente disponible para atender todas las peticiones de sus usuarios?
6. ¿Cree usted necesario actualizar el esquema de red de la Institución para mejorar la seguridad y disponibilidad?

7. ¿Confiaría en la implementación de herramientas de bajo costa para enriquecer la seguridad informática de la institución?
8. ¿Cree usted que en la Institución se requiere combinar recursos de cómputo, almacenamiento, red y virtualización en un solo sistema integrado, para aumentar la conectividad?

En esta Investigación: Se realizará una investigación para identificar las principales vulnerabilidades de seguridad existentes en la red de comunicación de la Universidad Técnica de Babahoyo. Esta investigación incluirá la recopilación de datos sobre los sistemas de seguridad existentes, así como la identificación de amenazas potenciales a la red. 2) Diseño: Luego de la investigación, se diseñará un sistema de ciberseguridad para la red de comunicación de la Universidad Técnica de Babahoyo. El diseño incluirá técnicas de seguridad como la criptografía, autenticación y control de acceso. Se implementarán controles de seguridad basados en la última tecnología de ciberseguridad y se tomarán en cuenta prácticas recomendadas por el gobierno y la industria. 3) Implementación: Una vez diseñado el sistema, se procederá a implementarlo. Esto incluirá la instalación de los dispositivos de seguridad, la configuración de los servidores, la instalación de software de seguridad, la realización de pruebas para garantizar el correcto funcionamiento y la implementación de un plan de gestión de la seguridad. 4) Evaluación: Después de la implementación, se evaluará el sistema de ciberseguridad para garantizar que esté funcionando de manera óptima. Esta evaluación incluirá pruebas de seguridad para medir el nivel de protección ofrecido por el sistema, así como la realización de auditorías para verificar su estado. 5) Mantenimiento: El mantenimiento del sistema de seguridad de la Universidad Técnica de Babahoyo debe realizarse de forma periódica para garantizar la seguridad de la red. Esto incluye la actualización de los dispositivos de seguridad, la supervisión del sistema y la realización de pruebas periódicas.

RESULTADOS

A continuación, las preguntas para la encuesta estructurada:

Tabla 1: Entrevista Estructurada Elaborado por: Carmen Muñoz

N	PREGUNTAS	SI	NO	TALVEZ	DETALLES
1	¿Considera usted que la red Informática de la universidad técnica de Babahoyo requiere una solución de respaldo de seguridad de costos?	X			
2	¿La seguridad aplicada actualmente sobre la red informática es suficientes para garantizar la seguridad de la institución y de su usuario?		X		
3	¿Actualmente la universidad hace uso de un sistema operativo de software libre y gratuito, detalle su respuesta?	X			Sistema Operativo Linux CentOS en su versión 7
4	¿La Institución cuenta con un Firewall dedicado que gestiones todos los sectores de subdivisión de la red Informática?		X		
5	¿Verdaderamente la Universidad Técnica de Babahoyo cuenta con Políticas de Seguridad Informática?	X			
6	¿Considera Usted que las Políticas de seguridad Actuales se pueden mejorar?	X			
7	¿Cree usted que enriquecer la estructura de seguridad de la Institución aumenta la Capacidad de disponibilidad y reacción de la red Informática?	X			
8	¿Toma en cuenta la actualización la estructura de la red informática actual de la institución para acrecentar la seguridad informática de la UTB?	X			

Elaborado por: Carmen Muñoz

INTERPRETACION DE ENTREVISTA

Para el desarrollo del presente caso de estudio se empleó la herramienta de investigación entrevista para recabar información relevante que ayude a plantear las resoluciones necesarias, se identificó que la Universidad técnica de Babahoyo requiere una solución de respaldo de seguridad de costos, asimismo se hace conocer que La seguridad aplicada actualmente sobre la red informática es suficientes para garantizar la integridad de la institución ,administrativos, profesores, estudiantes e invitados, se hizo saber de la Universidad ya usa una herramienta de software libre y gratuito que es el sistema operativo de red CentOS en su versión 7, sobremanera se identificó que no se cuenta con firewall dedicado a gestionar todos los sectores de subdivisión de la red Informática. Se dio a saber que la universidad técnica de Babahoyo si cuenta con políticas de seguridad, pero no son suficientes y se requiere mejorar en el aspecto de configuraciones necesarias para generar confianza en la red. Afianzar de que la disponibilidad y capacidad de reacción de la red es lo suficientemente robusta para resistir un ataque cibernético. Se hizo evidente que la estructura de la red puede ser actualizado buscando perfeccionar las estrategias de seguridad.

Políticas de seguridad

A continuación, se propone los protocolos de ajustes a considerar en firewall (PFsense):

1. Limitar el acceso VLAN: configuración de autentificación y autorización para cada VLAN, asignar permisos de acceso, sectorizando y permitir acceso solo a los usuarios que sean necesarios en cada VLAN.

2. Separar el Trafico VLAN: el uso de VLANs divididas para diferente tráfico de red voz, datos, video, separar los diferentes tipos de tráfico de red disminuye el riesgo de que tráfico malicioso afecte a todo el tráfico de red

3. Configurar VLAN nativa: es recomendable que no se utilicen VLANs nativas en el tráfico de usuario final

4. Configuración de DNS: definir ajustes del servidor DNS para permitir solo tráfico legítimo y evitar la ejecución de servicios de DNS no seguros

5. Implementación de DNSSEC: agregar una capa de seguridad para DNS con la implementación de DNSSEC, es una buena práctica para reforzar la seguridad

6. Limitar la cantidad de direcciones IP disponibles para DHCP: asignar un límite de IPs disponibles disminuye el riesgo de conflictos entre IPs

7. Asignar Ips basadas en la dirección MAC: asignar una IP específica a dispositivos en relación a su dirección MAC, garantiza que solo dispositivos con la dirección IP autorizada reciban una asignación IP del DCHP

8. Limitar la duración de las asignaciones de DHCP: evitar que los dispositivos mantengan una IP durante mucho tiempo ayuda a liberar IPs, no usadas. También previene ataques de denegación de servicios

9. Configurar claves privadas SSH: configurar de buena forma los permisos de archivos y directorios con SSH, se recomienda utilizar autentificación de dos factores

10. Desactivar servicios innecesarios SHH: quitar la posibilidad de acceso remoto a usuarios root para evitar accesos no autorizados, ataques de fuerza bruta y denegación de servicios

11. Configurar portal cautivo: portal cautivo es una solución para brindar acceso limitado a usuarios autorizados en una red separada y controlada, encriptar las conexiones entre clientes y portal cautivo con certificado SSL, para que solicite la autentificación del usuario antes de permitir el acceso.

12. Configurar NTP: es indispensable que el Firewall solo permita tráfico NTP solo de fuentes autenticadas, limitar el acceso a NTP solo a dispositivos que requieran sincronizarse con la red

RESULTADOS DE INVESTIGACION

Tabla 2:Beneficios del Sistema Operativo de Red CentOS

Servidor	Características	Compatibilidad	Licencia
Windows Server	Multiusuario, entorno grafico amigable, soporte para ASP y servidor de hosting tradicional.	Admite todos los procesadores AMD EPYC	LICENCIA
CentOS	Destaca por su facilidad de uso, estable, seguro, fuerte supervisión, sostenible a largo plazo	Compatible con RHEL	LIBRE

Elaborado por: Carmen Muñoz

Tabla 3: Beneficios de PFsense

Característica	Sin Firewall	PFsense
Seguridad	La red está expuesta a ataques externos e internos	Protección contra intrusiones, filtrado de contenido, prevención de pérdida de datos y más
Control de Trafico	En una red sin firewall, se debe aplicar otras medidas de seguridad, se debe mantener un control cuidadoso del trafico	Capacidad de restringir el acceso a ciertos sitios web o aplicaciones, y la capacidad de priorizar el tráfico para garantizar que las aplicaciones críticas reciban el ancho de banda necesario
Funciones de Red Avanzada	Se debe implementar funciones como: enrutamiento dinámico, configurar VLAN, gestión de banda ancha, optimización de red	Capacidad de configurar VPN, equilibrio de carga, enrutamiento avanzado y más. funciones permiten a las organizaciones configurar redes más complejas y eficientes

Escalabilidad	Es difícil manejar grandes cantidades de tráfico y una gran cantidad de usuarios	Altamente Escalable. Manejar redes grandes y complejas.
Soporte Y Comunidad	Una red sin firewall no cuenta con un equipo de soporte capacitado y profesional que pueda ayudar en caso de presentarse problemas	Gran comunidad de usuarios y una amplia base de conocimientos. pueden encontrar respuestas a cualquier problema que tengan y obtener soporte de la comunidad.

Elaborado por: Carmen Muñoz

Tabla 4: Beneficios de Hiperconvergencia (Nutanix)

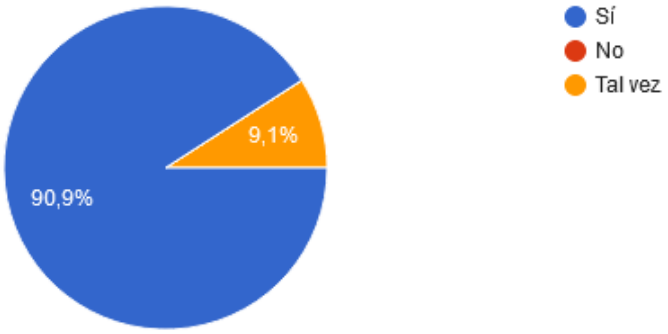
Característica	Sin Hiperconvergencia	Hiperconvergencia (Nutanix)
Infraestructura	Necesidad de comprar, Instalar y dar mantenimiento a los diferentes recursos que integran el sistema	La combinación de los recursos: Almacenamiento, Computo Y Red, simplifica la Infraestructura
Escalabilidad	Proceso de configuración e implementación de nuevos recursos de manera tediosa	Tolera incrementar los recursos según las necesidades de la empresa, de manera fácil y ágil, mediante la implementación de módulos preconfigurados
Costos	Requiere de costos de Implementación obligatorias para la red computacional	Significa ahorro en el costo total de sentar los cimientos de estructurar una red computacional
Flexibilidad	Implementar nuevos módulos requiere reajustar la configuración de los diferentes recursos de red	Los recursos se pueden asignar o reasignar según los cambios de la empresa
Rendimiento	**La comunicación entre recursos puede verse afectada en algún punto, por la falta de integración en la red**	**Elimina cuellos de botella que puedan suscitarse entre recursos de cómputo, almacenamiento y red lo que se evidencia en un mejor rendimiento**

INSTRUMENTO DE INVESTIGACION

ENCUESTA A USUARIOS DE RED UTB

1. ¿la seguridad informática es un factor relevante en su vida diaria?

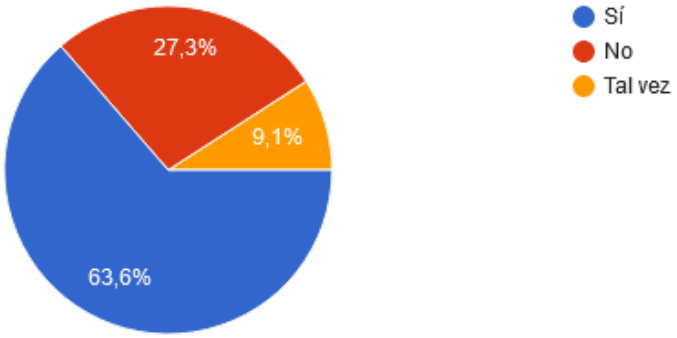
77 respuestas



Interpretación: se puede concluir que 90.9% de los usuarios de la red de la UTB consideran la seguridad informática como un factor presente en su vida diaria. Y solo un 9.1% dijo que no es muy necesario en sus vidas.

2. ¿usted tiene conocimiento sobre la función de un firewall?

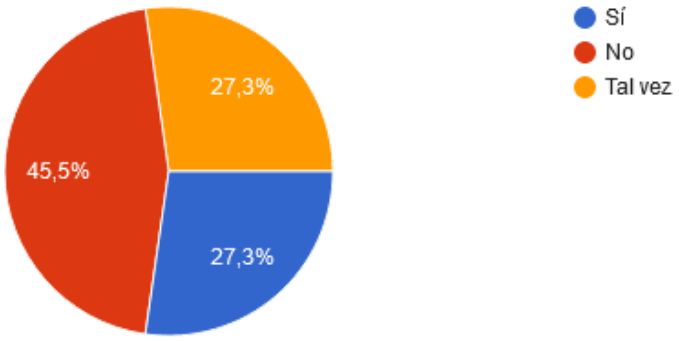
77 respuestas



Interpretación: según los usuarios de la Red UTB encuestados. El 63.6 % respondió que, sí conoce la función de un firewall dentro de una red, mientras que un 27.3 %, respondió que no tiene idea del tema, y un 9.1% dijo que tal vez saben un poco del tema, pero no es una idea clara.

3. ¿considera usted que la red de la Universidad Técnica de Babahoyo le ofrece la suficiente seguridad?

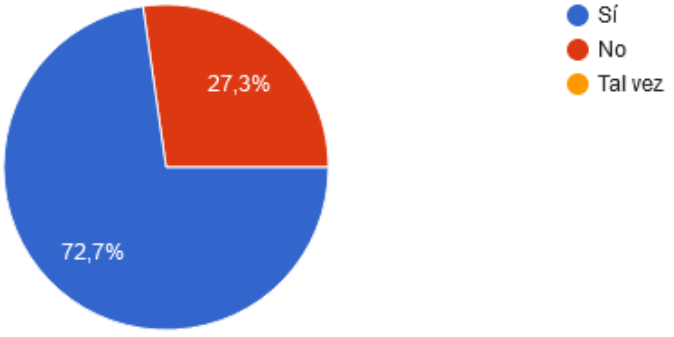
77 respuestas



Interpretación: según el grafico, 45.5% considera que la red UTB no es lo suficientemente segura, y tanto por el si o talvez se obtuvo una opinión dividida de 27.5% cada una, los resultados indican que los usuarios de la red no se sienten completamente seguros con el uso de la red UTB.

4. ¿tiene conocimiento usted sobre los softwares que imitan el funcionamiento de un ordenador físico, es decir crean entornos virtualizados?

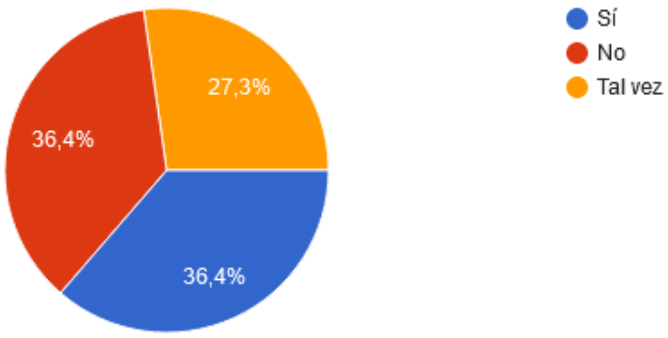
77 respuestas



Interpretación: según el grafico **el** 72.7% de los usuarios de la Red UTB si tiene conocimiento sobre softwares de Virtualización mientras que el 27.3 dijo no saber de qué se trataba dicho software.

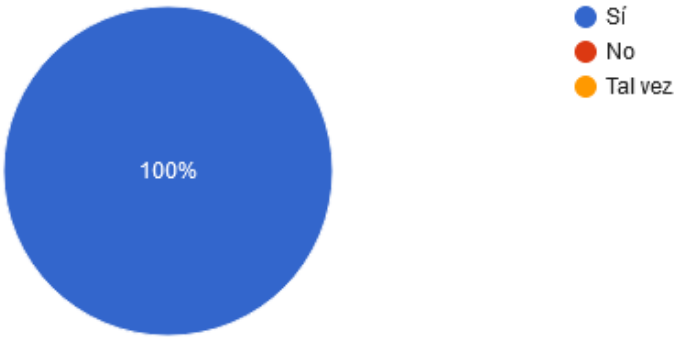
5. ¿opina usted que la red universitaria es lo suficientemente disponible para atender todas las peticiones de sus usuarios?

77 respuestas



6. ¿cree usted necesario actualizar el esquema de red de la Institución para mejorar la seguridad y disponibilidad?

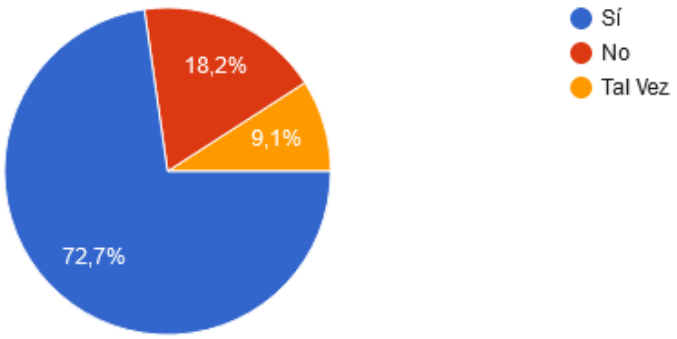
77 respuestas



Interpretación: se da a entender que el 100% de los usuarios de la red UTB encuestados está totalmente de acuerdo en que le red informática requiere modernizar su estructura de red para mejorar la seguridad y disponibilidad de la misma.

7. ¿confiaría en la implementación de herramientas de bajo costo para enriquecer la seguridad informática de la institución?

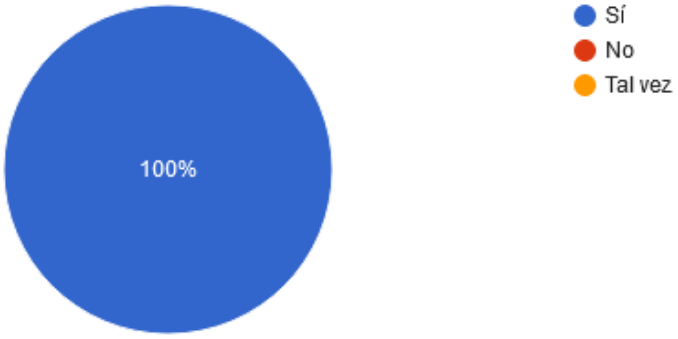
77 respuestas



Interpretación: según los resultados de la encuesta a los usuarios de la red UTB el 72.7% indica que confiaría en la implementación de una herramienta de costo reducido para enriquecer la seguridad informática de la Institución, mientras de un 18.2% definitivamente no confía en herramientas de bajo costo, el otro 9.1% no está muy seguro de su respuesta.

8. ¿cree usted que en la Institución se requiere combinar recursos de cómputo, almacenamiento, red y virtualización en un solo sistema integrado, para aumentar la conectividad?

77 respuestas



Interpretación: según los resultados de la encuesta realizada a los usuarios de la red UTB, se muestra que en su totalidad todos el 100% están de acuerdo en que la Institución requiere

integrar todos sus recursos, computo, almacenamiento , red y virtualización para aumentar la conectividad

DISCUSIÓN DE RESULTADOS

Al culminar con el análisis de la información obtenida de los miembros activos de la red informática de la Universidad técnica de Babahoyo se puso en evidencia que la institución requiere una actualización en la infraestructura de la red, para mitigar la preocupación sobre seguridad informática de los usuarios de la red, administrativos, profesores y estudiantes. se destacó que el uso de herramientas de bajo costo es imprescindible en el proceso de modernización. También se izó notar la Inquietudes acerca de la eficacia de las políticas de seguridad vigentes.

Es relevante señalar que se han creado tablas comparativas de tecnologías: Sistemas Operativos de Red, Firewall, Herramienta de Integración de Recurso Hiperconvergete con el propósito de identificar los beneficios que podrían obtenerse al implementar herramientas de bajo costo en la modernización de la infraestructura de red. Una vez finalizado el análisis correspondiente, se concluye que la implementación del proyecto es viable, ya que los beneficios son significativos y las capacidades de las herramientas gratuitas lo permiten.

CONCLUSIÓN

Una vez finalizado el correspondiente análisis de caso estudio mediante la recopilación de información a través de la metodología de investigación, se ha cuestionado la seguridad de la red informática vigente en la Universidad Técnica de Babahoyo, la carencia de un Firewall dedicado a la seguridad sumado a la falta de fundamentos de políticas de seguridad en la administración de sistemas .La Carencia de Firewall especializado en seguridad, junto con la falta de políticas fundamentales de seguridad en la gestión de sistemas, ha dado lugar a una baja calificación en cuanto a la seguridad de la red informática actual y ha generado una percepción de inseguridad para los usuarios. Por otro lado, la falta de integración entre los recursos computacionales, red y el almacenamiento conlleva desventajas tales como la falta de eficiencia y flexibilidad en el diseño de la red, lo que puede impedir su capacidad de adaptarse a las necesidades cambiantes de la institución a lo largo del tiempo.

El propósito de esta investigación es proponer una actualización de la infraestructura de la red a través de la implementación de un sistema de hiperconvergencia que permita la integración de los recursos de la red. Asimismo, se propone la incorporación del firewall pfSense en la red, en base a lo cual se han desarrollado políticas de seguridad que pueden mejorar la seguridad general de la institución.

la implementación de hiperconvergencia en red, pfSense y nuevas políticas de seguridad pueden contribuir a mejorar la eficiencia, flexibilidad y seguridad de la red informática de la institución, lo que puede resultar en una mejor calidad de servicio para los usuarios y una reducción de costos y riesgos para la organización.

RECOMENDACIONES

- Cambiar la infraestructura de red de una institución para utilizar herramientas de bajo costo como pfSense y Nutanix puede ser una excelente opción para mejorar la eficiencia, reducir costos y aumentar la seguridad. Es importante tener en cuenta que cualquier cambio en la infraestructura de red debe hacerse con cuidado y planificación cuidadosa para garantizar que la transición sea suave y no cause interrupciones en el funcionamiento de la organización.
- Implementar un Firewall dedicado a la seguridad y establecer políticas de seguridad claras y fundamentales en la administración de sistemas para mejorar la seguridad de la red informática actual. Esto puede incluir la identificación y prevención de amenazas, la gestión de usuarios y contraseñas, la monitorización en tiempo real de la red, entre otros aspectos.
- Definir e implementar nuevas políticas de seguridad específicas y adaptadas a las necesidades de la institución, lo que puede contribuir a mejorar la seguridad general de la red informática. Esto puede incluir establecer reglas claras y específicas sobre el acceso a los recursos de la red, la identificación y prevención de amenazas, la gestión de usuarios y contraseñas, entre otros aspectos.
- Realizar capacitaciones y entrenamiento al personal encargado de la administración de la red, para que estén al día en las mejores prácticas de seguridad y puedan implementar de manera adecuada las nuevas políticas y herramientas de seguridad en la red informática.

REFERENCIAS

Chakraborty, R., Ghosh, A., & Kumar Mandal, J. (2022). *Machine Learning Techniques and Analytics for Cloud Security*. Estados Unidos de America: Scrivener Publishing.

Aggarwal, M. (2018). *Network Security with pfSense.* Reino Unido: Packtpub.

Alegre Ramos, M. d. (2021). *Sistemas Operativos en Red.* Madrid-España: Ediciones Paraninfo, S.A.

Bottini, C. (7 de Abril de 2022). *redusers*. Obtenido de redusers: https://www.redusers.com/noticias/publicaciones/como-generar-certificados-https/

Botto-Tobar, M., Díaz Cadena, A., León-Acurio, J., & Montiel Díaz, P. (2019). *Advances in Emerging Trends and Technologies: Volume 1*. Babahoyo-Los Rios-Ecuador: Springer.

Coleman, D., & Westcott, D. (2012). *CWNA, Certified Wireless Network Administrator Official Study Guide.* Canada: Indianapolis.

Davis, D. (18 de Junio de 2019). *TechTarget SearchNetworking*. Obtenido de TechTarget SearchNetworking: https://searchnetworking.techtarget.com/es/definicion/VLAN-anidada

De Luz, S. (11 de Enero de 2023). *redeszone*. Obtenido de redeszone: https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

Deb Chowdhury, D. (2021). *NextGen Network Synchronization.* San Jose ,California USA: Switzerland AG.

Dembowski, K. (2003). *Hardware, Informacion sobre la totalidad, del hardware de rapido acceso.* Barcelona: Person Education.

Fernandez, L. (30 de Noviembre de 2022). *redeszone*. Obtenido de .redeszone: https://www.redeszone.net/tutoriales/internet/protocolo-snmp-que-es/

Ferrill, P., & Ferril, T. (2014). *Designing and Implementing a Server Infrastructure.* Estados Unidos de America: Microsoft Press.

Francois Campertier, J. (2016). *La Seguridad Informatica en la PYME.* Barcelona: Ediciones ENI.

Gerend, J., Downie, K., Ross, E., Prittie, I., & Mclllece, J. (3 de Marzo de 2023). *learn.microsoft*. Obtenido de learn.microsoft: https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top

Gonzalez, D. (2022). *El unico Libro de redes que necesitas.* New York: David Gozalez .

Hewlett-Packard Company. (30 de Agosto de 2021). *HP*. Obtenido de HP: https://www.hp.com/mx-es/shop/tech-takes/que-es-un-firewall-de-red-y-como-funciona

Liska, A., & Stowe, G. (2016). *DNS Security Domain Name System Defense.* Estados Unidos de America: Elsevier Book Aid Internacional.

Liu, C., & Albitz, P. (2006). *DNS and BIND.* Estados Unidos de America: Repkover.

Martha Irene Romero Castro, G. L. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Manabi-Ecuador: Area de Innovacion y desarrollo , S.L.

Mendrey, P., Verhoeven, T., & Angenendt, R. (2009). *The Definitive Guide to CentOS.* Estados Unidos de America: Candace English.

Negus, C., & Foster, E. (2009). *Fedora 11 And Red Hat Enterprise Linux.* Canada: Wiley Publishing Inc.

Ortega Candel, J. M. (2021). *Ciberceguridad Manual Practico.* España: Ediciones Paraninfo, S.A.

Preston, S. (09 de Junio de 2022). *akamai*. Obtenido de akamai: https://www.akamai.com/blog/trends/dnssec-how-it-works-key-considerations

Romero Castro, M., Figueroa Morán, G., Vera Navarrete, D., Álava Cruzatty, J., Parrales Anzúles, G., Álava Mero, C., . . . Castillo Merino, M. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Manabi-Ecuador: Area de Innovacion y desarrollo , S.L.

Simpson, T., & Novak, J. (2018). *Hands on Virtual Computing.* Estados Unidos De America: Cengage Learning.

Smyth, N. (2019). *CentOS 8 Essentials.* Estados Unidos de America: Payload Media.

Tanenbaum, A., & Wetherall, D. (2012). *Redes de Computadoras.* Mexico: Pearson Education.

Waschke, M. (2017). *Personal Cybersecurity: How to Avoid and Recover from Cybercrime.* Washington, USA: Acid Free Paper.

Zientara, D. (2018). *PFSense 2.4.* Reino Unido: packtpub.

ANEXOS

ANEXO 1:

ENCUESTAS REALIZADA A ESTUDIANTES DE LA UNIVERSIDAD TECNICA DE BABAHOYO

1. **¿la seguridad informática es un factor relevante en su vida diaria?**

SI ☐ NO ☐ TALVEZ ☐

2. **¿usted tiene conocimiento sobre la función de un firewall?**

SI ☐ NO ☐ TALVEZ ☐

3. **¿considera usted que la red de la Universidad Técnica de Babahoyo le ofrece la suficiente seguridad?**

SI ☐ NO ☐ TALVEZ ☐

4. **¿tiene conocimiento usted sobre los softwares que imitan el funcionamiento de un ordenador físico, es decir crean entornos virtualizados?**

SI ☐ NO ☐ TALVEZ ☐

5. **¿opina usted que la red universitaria es lo suficientemente disponible para atender todas las peticiones de sus usuarios?**

SI ☐ NO ☐ TALVEZ ☐

6.¿cree usted necesario actualizar el esquema de red de la Institución para mejorar la seguridad y disponibilidad?

SI ☐ NO ☐ TALVEZ ☐

7.¿confiaría en la implementación de herramientas de bajo costa para enriquecer la seguridad informática de la institución?

SI ☐ NO ☐ TALVEZ ☐

8.¿cree usted que en la Institución se requiere combinar recursos de cómputo, almacenamiento, red y virtualización en un solo sistema integrado, para aumentar la conectividad?

SI ☐ NO ☐ TALVEZ ☐

ANEXO 2:

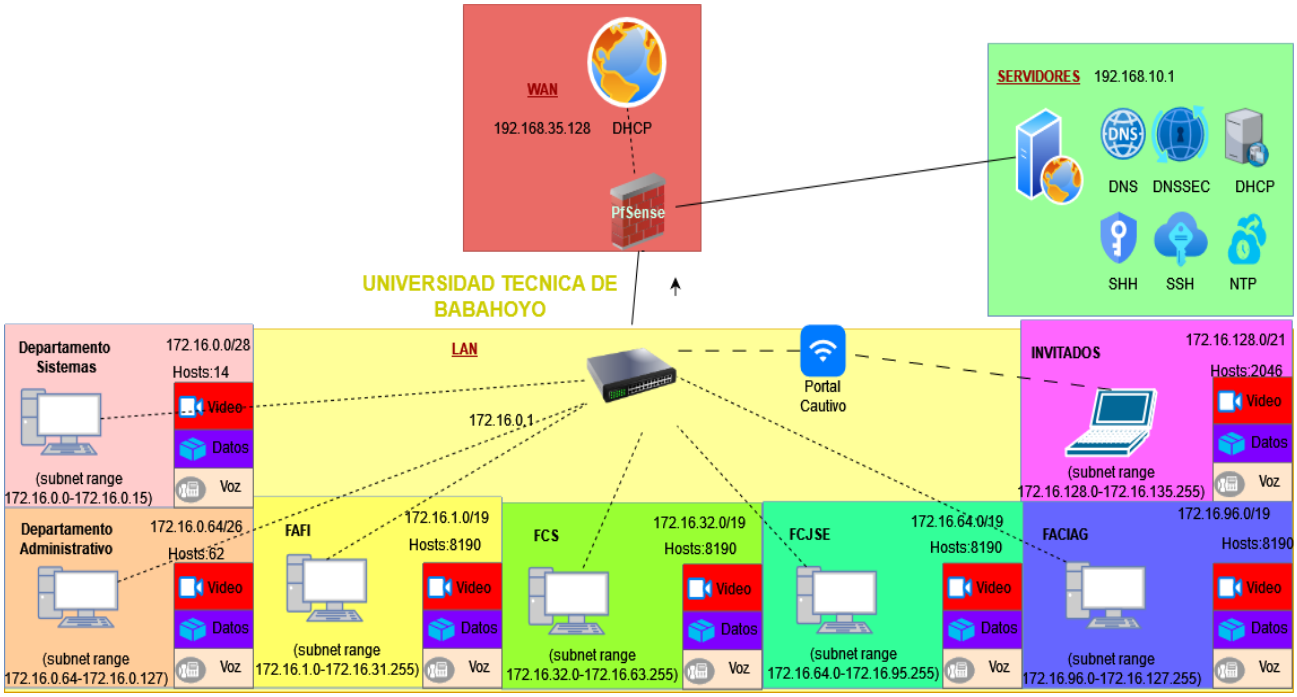
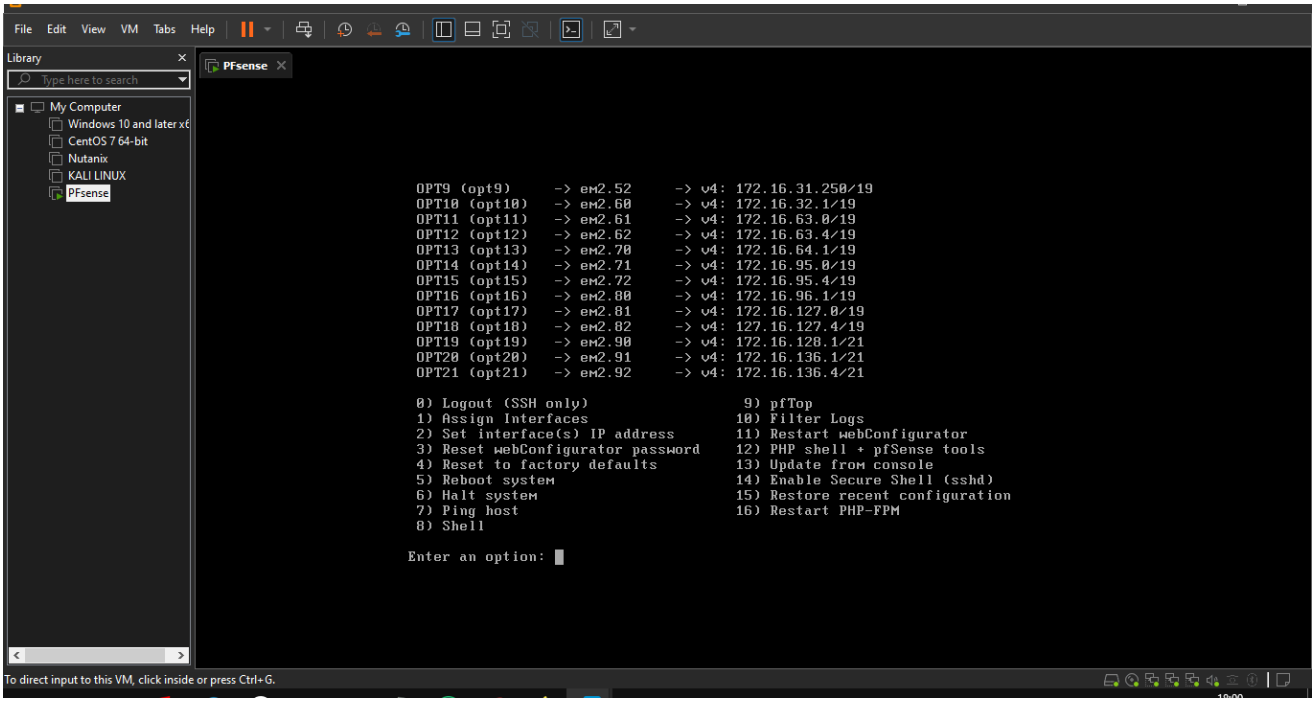


Ilustración 1: Red UTB Elaborado por: Carmen Muñoz

ANEXO 3:

Ilustración 2:consola de Pfsense



Elaborado por: Carmen Muñoz

ANEXO 4:

UNIVERSIDAD TÉCNICA DE BABAHOYO

Babahoyo,16 de marzo del 2023

Magister

Eduardo Galeas Guijarro

DECANO DE LA FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA

En su despacho

De mis consideraciones:

Yo **MUÑOZ VERA CARMEN ADRIANA**, con cedula de identidad **1207943059**, estudiante de octavo semestre de la carrera de ingeniería en sistemas de información, matriculada en el proceso de titulación periodo Diciembre 2022- Abril 2023, le solicito a usted de la manera más comedida Se sirva autorizar, el permiso respectivo para realizar mi caso de estudio en esta prestigiosa universidad, misma que se denomina: **SISTEMA DE CIBER SEGURIDAD PARA LA RED DE COMUNICACIÓN DE LA UNIVERSIDAD TECNICA DE BABAHOYO BASADO EN SISTEMAS DE CODIGO ABIERTO**, el cual es requisito indispensable para poder titularme.

Esperando una respuesta favorable, quedo de usted muy agradecida

Atentamente

Carmen Muñoz

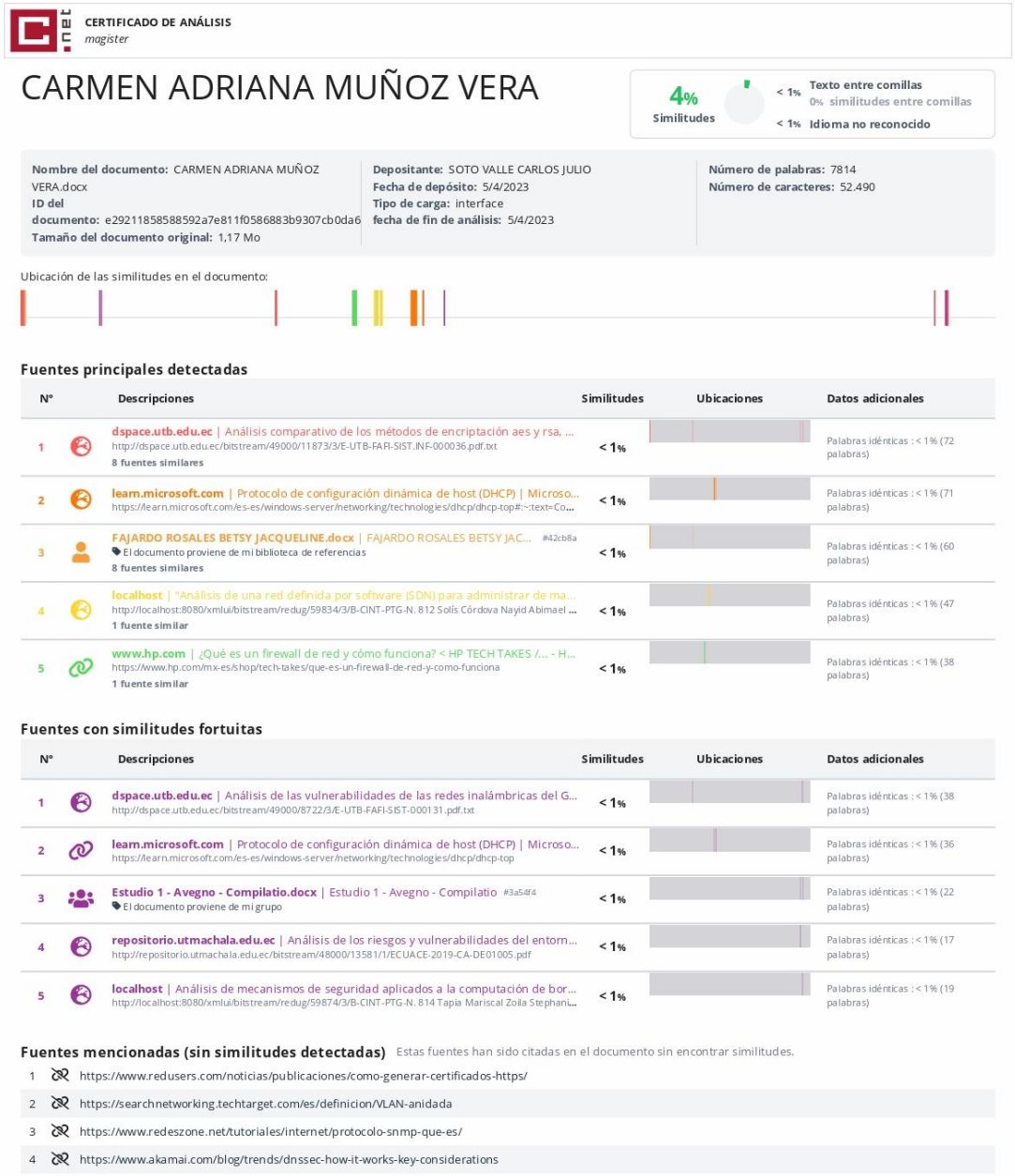
Muñoz Vera Carmen Adriana

120794305-9

RECIBIDO
UNIVERSIDAD TECNICA DE BABAHOYO
SECRETARIA FAFI
16-03-23 FECHA:
12:15 HORA:

AUTORIZADO
UNIVERSIDAD TÉCNICA DE BABAHOYO
DECANATO
FAFI

ANEXO 5



CERTIFICADO DE ANÁLISIS
magister

CARMEN ADRIANA MUÑOZ VERA

4% Similitudes

< 1% Texto entre comillas
0% similitudes entre comillas
< 1% Idioma no reconocido

Nombre del documento: CARMEN ADRIANA MUÑOZ VERA.docx
ID del documento: e29211858588592a7e811f0586883b9307cb0da6
Tamaño del documento original: 1,17 Mo

Depositante: SOTO VALLE CARLOS JULIO
Fecha de depósito: 5/4/2023
Tipo de carga: interface
fecha de fin de análisis: 5/4/2023

Número de palabras: 7814
Número de caracteres: 52.490

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**dspace.utb.edu.ec** | Análisis comparativo de los métodos de encriptación aes y rsa, ... http://dspace.utb.edu.ec/bitstream/49000/11873/3/E-UTB-FAFI-SIST.INF-000036.pdf.txt **8 fuentes similares**	< 1%		Palabras idénticas : < 1% (72 palabras)
2	**learn.microsoft.com** | Protocolo de configuración dinámica de host (DHCP) | Microso... https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top#:~:text=Co...	< 1%		Palabras idénticas : < 1% (71 palabras)
3	**FAJARDO ROSALES BETSY JACQUELINE.docx** | FAJARDO ROSALES BETSY JAC... #42cb8a El documento proviene de mi biblioteca de referencias **8 fuentes similares**	< 1%		Palabras idénticas : < 1% (60 palabras)
4	**localhost** | "Análisis de una red definida por software (SDN) para administrar de ma... http://localhost:8080/xmlui/bitstream/redug/59834/3/B-CINT-PTG-N. 812 Solís Córdova Nayid Abimael ... **1 fuente similar**	< 1%		Palabras idénticas : < 1% (47 palabras)
5	**www.hp.com** | ¿Qué es un firewall de red y cómo funciona? < HP TECH TAKES /... - H... https://www.hp.com/mx-es/shop/tech-takes/que-es-un-firewall-de-red-y-como-funciona **1 fuente similar**	< 1%		Palabras idénticas : < 1% (38 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**dspace.utb.edu.ec** | Análisis de las vulnerabilidades de las redes inalámbricas del G... http://dspace.utb.edu.ec/bitstream/49000/8722/3/E-UTB-FAFI-SIST-000131.pdf.txt	< 1%		Palabras idénticas : < 1% (38 palabras)
2	**learn.microsoft.com** | Protocolo de configuración dinámica de host (DHCP) | Microso... https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top	< 1%		Palabras idénticas : < 1% (36 palabras)
3	**Estudio 1 - Avegno - Compilatio.docx** | Estudio 1 - Avegno - Compilatio #3a54f4 El documento proviene de mi grupo	< 1%		Palabras idénticas : < 1% (22 palabras)
4	**repositorio.utmachala.edu.ec** | Análisis de los riesgos y vulnerabilidades del entorn... http://repositorio.utmachala.edu.ec/bitstream/48000/13581/1/ECUACE-2019-CA-DE01005.pdf	< 1%		Palabras idénticas : < 1% (17 palabras)
5	**localhost** | Análisis de mecanismos de seguridad aplicados a la computación de bor... http://localhost:8080/xmlui/bitstream/redug/59874/3/B-CINT-PTG-N. 814 Tapia Mariscal Zoila Stephani...	< 1%		Palabras idénticas : < 1% (19 palabras)

Fuentes mencionadas (sin similitudes detectadas)

Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://www.redusers.com/noticias/publicaciones/como-generar-certificados-https/
2 https://searchnetworking.techtarget.com/es/definicion/VLAN-anidada
3 https://www.redeszone.net/tutoriales/internet/protocolo-snmp-que-es/
4 https://www.akamai.com/blog/trends/dnssec-how-it-works-key-considerations