PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN.

MENCIÓN REDES DE COMUNICACIONES

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN REDES DE COMUNICACIONES

TÍTULO

"ESTUDIO PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL INFORMÁTICA PARA EL LABORATORIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DE LA FACULTAD DE INGENIERÍA DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR"

AUTOR:

ROBERTO CARLOS SALAZAR GUALOTO

QUITO, 2020 NOVIEMBRE

DEDICATORIA

Dedico el presente trabajo de titulación a mi padre Dios, mi piloto principal en cada una de las etapas de mi vida.

A mis madres Zenata (+) y Lolita que desde pequeño han llenado mis pasos de amor, paciencia y apoyo incondicional celestial y terrenalmente.

Roberto Carlos Salazar Gualoto

AGRADECIMIENTO

A mi padre Dios por permitirme cruzar cada uno de los obstáculos que se han presentado en este camino.

A mis madres Zenata (+) y Lolita por ser el motor de mi vida y no declinar en mi formación personal y profesional .

A la Pontifica Universidad Católica del Ecuador por permitirme cursar y culminar este sueño. Al Mtr. Javier Cóndor por la colaboración desinteresada en el desarrollo de mi tesis.

Roberto Carlos Salazar Gualoto

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente trabajo de titulación esta desarrollado para proporcionar un estudio para la implementación de un sistema de seguridad perimetral informática para el LTIC. Para esto se realiza la conceptualización necesaria referente a temas de seguridad informática y seguridad perimetral. El análisis de la situación actual de seguridad del LTIC que cubre el escaneo, análisis y resumen de vulnerabilidades, inteligencia de amenazas y resumen de puertos abiertos. El diseño del sistema de seguridad perimetral informática consta del análisis de los requerimientos del LTIC para seleccionar la tecnología de seguridad perimetral más eficiente y realizar su análisis comparativo de especificaciones técnicas y costos para concluir con el esquema de seguridad perimetral y la propuesta de una política de seguridad informática. Finalmente se implementa un prototipo del sistema de seguridad perimetral informática basado en la instalación y configuración de la plataforma de seguridad cibernética Check Point Gaia R81 emulando appliances 6000 como firewall de nueva generación y se realiza el análisis y resumen de vulnerabilidades post implementación de CPG-R81.

INTRODUCCIÓN

El motivo del presente trabajo de titulación es resolver la creciente necesidad de protección de la información, considerando que la hiper convergencia tecnológica que el mundo vive es el ecosistema propicio para la propagación de ciberataques o ataques a gran escala que se mueven rápidamente en las empresas. Estos ataques a medida que la tecnología evoluciona son más sofisticados y pasan por alto las soluciones de seguridad informática puntales implementadas en las empresas, es así el caso de los mecanismos de seguridad implementados en el LTIC, que protegen posibles amenazas basados en el uso de UTM Untangle y del antivirus McAfee.

Para mejorar la seguridad informática se presenta un estudio para el diseño del sistema de seguridad perimetral informática para el LTIC que aspira prevenir riesgos o amenazas que puede ser aprovechadas por los atacantes causando pérdidas significativas en la integridad, confidencialidad, disponibilidad y autenticidad de la información en la Red del LTIC. En efecto esto sustenta el problema de requerir un alto nivel de seguridad perimetral, para lo cual se basa en la identificación de amenazas y vulnerabilidades, definición de políticas de seguridad informática, diseño e implementación de un prototipo de un sistema de seguridad perimetral informático en la red de datos del LTIC.

Finalmente, el trabajo de titulación se encuentra estructurado en cinco capítulos, un apartado inicial de la descripción general del presente estudio y un apartado final de bibliografía y anexos. El primer capítulo hace referencia al fundamento teórico necesario para desarrollo del estudio, el segundo capítulo contiene el análisis de la situación actual de seguridad del LTIC, el tercer capítulo es el más importante contiene la información del diseño del sistema de seguridad perimetral informática el análisis de la tecnología de seguridad perimetral sus especificaciones técnicas y costos. El cuarto capítulo contiene la implementación de un prototipo de sistema de seguridad perimetral informática y el quinto y último capítulo consta de conclusiones y recomendaciones.

PLANTEAMIENTO DEL PROBLEMA

La Facultad de Ingeniera de la Pontificia Universidad Católica del Ecuador dispone del Laboratorio de Tecnologías de la Información y Comunicación conformado de infraestructura física e infraestructura de red cableada e inalámbrica para proveer comunicación e interconexión de los dispositivos de docentes y estudiantes a servicios que ofrece el internet e intranet. La infraestructura física se encuentra distribuida por 7 aulas de enseñanza, un cuarto de becaria, una cuarto de Data Center, dos estancias para uso investigativo, un cuarto de director, dos zonas de uso múltiple y una bodega.

Los procesos de enseñanza, aprendizaje e investigación al cual está atado un ambiente educativo como es el caso del LTIC obliga a estar acorde al avance tecnológico, estos constantes requerimientos de acceso a información de los servicios enlazados tanto a la intranet como al internet exponen a la red de datos a diferentes tipos de infiltraciones o ataques informáticos para los que el LTIC no cuenta con un mecanismo de seguridad informática para prevenir este tipos de riesgos que se incrementan diariamente a nivel mundial y que Ecuador no está exento de ellos. De acuerdo a esto se precisa que el LTIC no dispone de un sistema de seguridad perimetral informática para reducir el tiempo que se pueda tardar en mitigar cualquier tipo de ataque.

Debido a la carencia de mecanismos de seguridad informática y políticas de seguridad en el LTIC no existe una evaluación de las vulnerabilidades que pueda presentar la red de datos como MITM[1], spoofing[2], snnifing[3], keyloggers[4], denegación servicios DoS[5] o ataques más graves como la denegación de servicio distribuido DDoS[6].

El LTIC no posee un análisis de tecnologías de seguridad perimetral informática que pueda servir como mecanismo de seguridad para proteger la integridad, autenticidad y confidencialidad de la información y de los sistemas informáticos que dispone y que este se ajuste a sus necesidades y políticas de seguridad.

---

[1] MITM ataque Man in The Middle en inglés o en español ataque de Hombre en el medio que consiste en la interceptación de la comunicación entre dos equipos
[2] Spoofing uso de técnicas para la suplantación de identidad generalmente para uso malicioso.
[3] Snnifing es una técnica que permite escuchar todo lo que circula por la red.
[4] Keyloggers es una técnica que permite la captura de lo ingresado por el teclado mediante el uso de software.
[5] DoS ataque por denegación de servicios consisten en la inhabilitación el uso de sistema, una maquina u otro
[6] DDoS ataque por denegación de servicios distribuida es un tipo de ataque DoS

De esto se pueden identificar el siguiente problema principal:

- ✓ No se cuenta con un diseño de un sistema de seguridad perimetral informática que pueda servir para proteger el laboratorio de tecnologías de la información y comunicación (LTIC) de la Facultad de Ingeniera de la Pontificia Universidad Católica del Ecuador

Y los siguientes problemas secundarios:

- ✓ No se han determinado el tipo de amenazas o vulnerabilidades que se presentan en la red perimetral LTIC.
- ✓ No se ha identificado políticas de seguridad y/o mecanismos de defensa para proteger el laboratorio de tecnologías de la información y comunicación (LTIC).
- ✓ No se cuenta con tecnologías de seguridad perimetral informática que se pueden utilizar para mejor la seguridad informática del LTIC.
- ✓ No se dispone de un diseño pueda servir para la implementación de un sistema de seguridad perimetral informática para el LTIC.

En función de lo expuesto como problemática se plantean la siguiente pregunta de investigación principal:

- ✓ ¿Qué diseño de sistema de seguridad perimetral informática puede servir para proteger el laboratorio de tecnologías de la información y comunicación (LTIC) de la Facultad de Ingeniera de la Pontificia Universidad Católica del Ecuador?

Y las siguientes preguntas de investigación secundarias:

- ✓ ¿Qué tipo de amenazas o vulnerabilidades se presentan en la red del LTIC?
- ✓ ¿Qué políticas de seguridad y/o mecanismos de defensa se pueden definir para proteger el laboratorio de tecnologías de la información y comunicación (LTIC)?
- ✓ ¿Qué tecnologías de seguridad perimetral informática se pueden utilizar para mejor la seguridad informática del LTIC?
- ✓ ¿Qué diseño puede servir para la implementación de un sistema de seguridad perimetral informática para el LTIC?

OBJETIVOS

OBJETIVO GENERAL

Realizar un estudio para la implementación de un sistema de seguridad perimetral informática para el laboratorio de tecnologías de la información y comunicación (LTIC) de la Facultad de Ingeniera de la Pontificia Universidad Católica del Ecuador.

OBJETIVOS ESPECÍFICOS

- ✓ Analizar la red actual del LTIC para la identificación de amenazas y vulnerabilidades existentes en su red.
- ✓ Definir las políticas de seguridad y/o mecanismos de defensa para proteger el laboratorio de tecnologías de la información y comunicación (LTIC).
- ✓ Realizar un análisis de tecnologías para la seguridad perimetral informática que solvente las necesidades de seguridad de la red del LTIC.
- ✓ Realizar el diseño para la implementación de un sistema de seguridad perimetral informática para el LTIC.
- ✓ Implementar un prototipo de un sistema de seguridad perimetral informática propuesto como solución de seguridad para la red del LTIC.
- ✓ Evaluar la red del LTIC partiendo de la implementación de un prototipo de sistema de seguridad perimetral informática.

CAPITULO I

1. MARCO TEÓRICO

Esta sección cubre la conceptualización necesaria para el desarrollo de la investigación, partiendo de la definición de seguridad informática, vulnerabilidades, amenazas, hacking ético y políticas. Para finalizar con la conceptualización de seguridad perimetral, sus funciones y las herramientas de seguridad perimetral y clasificación.

1.1. SEGURIDAD INFORMÁTICA

Seguridad informática se puede definir como la disciplina enfocada en aplicar una serie de medidas, políticas, herramientas hardware y software para eludir o localizar el acceso no autorizado con el fin de proteger la confidencialidad, la disponibilidad y la integridad. (Romero, y otros, 2018). Estos últimos tres términos son conocidos según la Figura 1-1 como principios de la seguridad informática o triada CIA, (Romero, y otros, 2018, pág. 26 y 27) y (Christen, Gordijn, & Loi, 2020, pág. 13) los definen:

Figura 1-1 Principios de la Seguridad de la Información (Romero, y otros, 2018, pág. 25)

Confidencialidad consiste en evitar el acceso no autorizado a la información.

Integridad consiste en evitar o detectar que la información no se vea comprometida voluntariamente o involuntariamente.

Disponibilidad consiste en la capacidad de permanecer accesible la información en el momento y forma que los usuarios la necesiten.

Lo expresado anteriormente sobre seguridad informática hay que diferenciar de seguridad de la información debido que los términos se los pueden considerar iguales por perseguir la misma finalidad, pero conceptualmente son diferentes.

1.1.1 TIPOS DE SEGURIDAD INFORMÁTICA

Hay una variedad en la categorización de seguridad informática en este estudio nos enfocaremos en los tipos que cubre el objeto - protección según (Redacción APD, 2020):

Seguridad de Hardware se enfoca a proteger a los equipos de cómputo o dispositivos que se usan para escanear un sistema o para el control del tráfico de una red.
Seguridad de Software se enfoca a proteger las aplicaciones, y programas contra amenazas y otros tipos de riesgos informativos.
Seguridad de Red se enfoca en proteger toda actividad de la red incluido el software y hardware.

1.1.2 VULNERABILIDADES DE LA SEGURIDAD INFORMÁTICA

Vulnerabilidad es un término que describe una debilidad o fallo de diseño, de procedimiento de recursos, que podría usarse de alguna manera para comprometer equipos de cómputo, dispositivos, infraestructura de red y sistemas. Las vulnerabilidades pueden presentarse en diversas formas y tamaños en sistemas operativos, aplicaciones, infraestructura, protocolos, transporte y comunicaciones. (Hertzog, O'Gorman, & Aharoni, 2017) (Haber & HIbbert, 2018, pág. 5) y (Romero, y otros, 2018, pág. 30)

La identificación de las vulnerabilidades sigue múltiples estándares de seguridad en este estudio se usa los expuestos en la Tabla 1-1:

Nombre	Siglas	Descripción
Common Vulnerabilities and Exposure	CVE	Estándar para nombres de vulnerabilidad de seguridad de la información y descripciones
Common Vulnerability Scoring System	CVSS	Sistema matemático para evaluar el riesgo de la información y vulnerabilidades tecnológicas
Open Vulnerability Assessment Language	OVAL	Esfuerzo de la comunidad de seguridad de la información para estandarizar como evaluar e informar sobre el estado del equipo de cómputo o dispositivos
Open Web Application Security Project	OWASP	Comunidad en línea sin fines de lucro enfocadas para desarrollar aplicaciones web seguras proporcionando metodologías, herramientas y tecnología.

Tabla 1-1. Estándares de Seguridad para Identificación de Vulnerabilidades (Haber & HIbbert, 2018, pág. 7 y 9)

1.1.2.1 *Tipos de Vulnerabilidades*

Existe una variedad de vulnerabilidades en este punto se tratará las más conocidas y usadas para su explotación según (Romero, y otros, 2018, pág. 43 y 44).

Desbordamiento de buffer se refiere cuando un programa no controla la cantidad de datos que se copian en el buffer, si esa cantidad es superior a la capacidad del buffer los bytes sobrantes se almacenan en zonas de memoria adyacentes.

Errores de configuración se refiere al uso de contraseñas por defecto o uso de protocolos de encriptación obsoletos.

Errores web se refiere a los errores de validación de input, scripts inseguros, errores de configuración de aplicaciones.

Errores de protocolo se refiere a protocolos que fueron activados sin necesidad o sin tener en cuenta la seguridad, el diseño y crecimiento de la red.

1.1.2.2 *Gravedad de las Vulnerabilidades*

La clasificación de la gravedad de las vulnerabilidades se le puede referenciar de acuerdo a la Tabla 1-2:.

Gravedad	Definición
Critica	Vulnerabilidad que permite al atacante acceso limitado para controlar el sistema y acceso a datos confidenciales críticos
Alta	Vulnerabilidad capaz dar acceso al atacante a datos privados como configuraciones de seguridad e información parcial de archivos y / o acceso limitado a archivos.
Media	Vulnerabilidad que revelan información confidencial sobre sistemas que pueden usarse como base para futuros ataques
Baja	Vulnerabilidad que da información del sistema

Tabla 1-2. Gravedad de las Vulnerabilidades (Kou, 2019).

1.1.2.3 *Herramientas para el análisis de las Vulnerabilidades*

Actualmente existe una variedad de herramientas para el análisis de vulnerabilidades en el mercado en este estudio trataremos las más importantes.

Nessus es una herramienta de evaluación de vulnerabilidades que se controla mediante una interfaz web, permite a sus usuarios crear escaneos personalizados. Además, Nessus contiene plantillas de escaneo preconstruidas para varios tipos de industrias. Tenable, el creador de Nessus, ha indicado que es capaz de detectar más de 58,000 vulnerabilidades y exposiciones comunes (CVE). Nessus es compatible con varias plataformas, como Windows y Kali Linux, posee varias versiones como essentials y profesional. (Singh, 2019, pág. 54 y 55).

OpenVAS es una abreviatura de Open Vulnerability Assessment System. más que una herramienta de análisis es un framework completo de varios servicios, que ofrece una solución integral y poderosa de escaneo de vulnerabilidades y gestión de vulnerabilidades. OpenVAS tiene un conjunto de

pruebas de vulnerabilidad de red (NVT). Los NVT se llevan a cabo utilizando complementos, que se desarrollan utilizando el código Nessus Attack Scripting Language (NASL). Hay más de 50,000 NVT en OpenVAS, y se agregan nuevos NVT regularmente. (Rahalkar, 2019).

Legion es un framework de prueba de penetración de red semiautomático de código abierto que puede realizar tareas de detección, reconocimiento y evaluación de vulnerabilidades. Puede descubrir hosts en vivo en una red, recopilar información útil sobre hosts de destino y descubrir vectores de ataque de red contra sistemas de destino a través de diferentes módulos integrados como Nikto, NMAP, THC Hydra, whataweb, sslyzer, Vulners, dirbuster, SMBenum y webslayer. (Hackingloops, 2020).

GFI LanGuard es una herramienta que escanea y detecta las vulnerabilidades en la red mediante las bases de datos de comprobación como puede ser la OVAL (Open Vulnerability And Assessment Language). Funciona con una amplia variedad de dispositivos. Proporciona múltiples plantillas de reportes como, cumplimiento, análisis de vulnerabilidades, reportes técnicos, ejecutivos y de manera general. (Romero, y otros, 2018, págs. 80 - 82).

1.1.3 AMENAZAS DE LA SEGURIDAD INFORMÁTICA

Las amenazas son la posibilidad de ocurrencia de cualquier tipo de evento o acción con el fin de producir daño a un sistema o sobre los elementos de información de la seguridad informática. (Messier, 2018).

El ecosistema en el cual se enmarca las amenazas de la seguridad informática es muy variado, según (Chang & Hawamdeh, 2020) se divide en seis categorías.

1.1.3.1 *Ataques basados en Red*

Ataques basados en red son aquellos que se llevan a cabo debido a la conectividad de red los definimos en la Tabla 1-4 y Tabla 1-4.

Ataque	Descripción
Eavesdropping	O escucha es el ataque que intercepta el tráfico de la red para obtener información confidencial
Man-in-the-middle Session Hijacking	Ataque donde se interceptan o se secuestran una sesión entre cliente y servidor para secuestrar las comunicaciones
IP spoofing	Ataque que envía paquetes con la dirección IP de un anfitrión conocido y confiable
Replay	Ataque donde se cambia los datos de un paquete interceptado
Denial-of-service (DoS)	Ataque que tiene como objetivo interrumpir los recursos del sistema y los servicios
Teardrop attack	Ataque donde se cambian el campo de desplazamiento de longitud y la fragmentación de paquetes IP

Tabla 1-3. (a) Ataques basados en la red. (Chang & Hawamdeh, 2020, pág. 23 y 24)

Ataque	Descripción
Smurf attack	Ataque donde se suplantan la dirección IP de un equipo de cómputo o dispositivo objetivo y se renvía solicitudes de eco ICMP falsificadas
Ping-of-death attack	Ataque donde se envía paquetes IP fragmentados a un equipo de cómputo victima
Botnets	Ataque que por medio de software puede controlar de forma remota un equipo de cómputo o dispositivo
Internet-of-things (IoT) attacks	Ataque que utiliza tecnologías incrustadas en los dispositivos IoT para interactuar con entornos externos.
Brute-force password attacks	Ataque que usa un banco de palabras utilizadas al azar para descifrar las contraseñas de las victimas

Tabla 1-4. (b) Ataques basados en la red. (Chang & Hawamdeh, 2020, pág. 23 y 24)

1.1.3.2 *Ataques basados en internet en sitios web*

Ataques basados en internet en sitios web son ataques exitosos que requieren conocimiento los definimos en la Tabla 1-5:

Ataque	Descripción
Drive-by-downloads	Ataque donde se infecta los equipos de cómputo o dispositivos víctima con malware de varias maneras
SQL injection	Ataque que ejecuta consultas SQL a través de datos de entrada en el navegador a la base de datos.
Cross-site scripting (XSS) attack	Ataque donde explotan las vulnerabilidades de un sitio web
Buffer overflow against application security	Ataque donde se puede escribir datos falsos, entradas mal formadas o códigos maliciosos en el buffer de un programa para desbordarlo o exceder los límites del buffer

Tabla 1-5. Ataques basados en internet en sitios web. (Chang & Hawamdeh, 2020, pág. 24 y 25)

1.1.3.3 *Ataques de Malware*

Los ataques de malware se presentan en muchas formas, pueden ser devastadoras, destruyendo sectores de arranque o eliminando permanente los archivos de los sistemas, los definimos en la Tabla 1-6 y Tabla 1-7:

Ataque	Descripción
Macro virus	Virus que pueden infectar generalmente a productos Microsoft como Word o Excel
Boot sector or executable file infection	Virus que se adhieren a códigos ejecutables
Virus polimórficos y metamórficos	Virus que se pueden ocultar o mutar en diferentes códigos mediante algoritmos de cifrados o técnicas de comprensión
Caballos de Troya	No se replica como virus, pero puede ocultarse en un programa regular y establecer una puerta trasera para la explotación de los atacantes en un momento posterior.
Bombas Lógicas	Malware que puede ser activado por una condición lógica especifica en una fecha y hora especifica
Gusanos	Son programas autocontenidos que pueden propagarse por correo electrónico o archivos adjuntos

Tabla 1-6. (a) Ataques de Malware. (Chang & Hawamdeh, 2020, pág. 25 y 26)

Ataque	Descripción
Ransomware	Malware que utiliza la criptografía para bloquear el acceso de las victimas a sus dispositivos encriptando sus archivos hasta que se pague el rescate para liberar las claves de descifrado
Spyware o Adware	Malware que puede instalarse sin saberlo en el navegador de una víctima para recopilar información de los usuarios como su historial de navegación para espiar o perfilar marketing y publicidad

Tabla 1-7. (b) Ataques de Malware. (Chang & Hawamdeh, 2020, pág. 25 y 26)

1.1.3.4 *Ingeniería Social*

La ingeniera social es otra forma de explotación engañosa que se puede implementar para obtener credenciales de acceso no autorizado se clasifican de acuerdo a Tabla 1-8.

Ataque	Descripción
Phishing	Ataque en el que se pueden enviar correos electrónicos a una serie de víctimas esperando que las mismas entreguen credenciales personales o información.
Spear Phishing	Ataque que pueden usar trucos psicológicos para crear falsos correos y enviar a victimas especificas con el fin de engañarles y obtener información confidencial.
Parming	Ataque que redirige el tráfico de navegación de los usuarios de internet a un sitio web falso para engañarlos y obtener información personal.

Tabla 1-8. Ataques de Ingeniería Social. (Chang & Hawamdeh, 2020, pág. 26 y 27)

1.1.3.5 *Amenaza Interna*

Las amenazas internas se han convertido en uno de los problemas organizacionales más complejos se clasifican de acuerdo a la Tabla 1-9.

Amenaza	Descripción
Intencionada	Amenazas que se ejecutan con mala intención para comprometer o robar información confidencial.
No intencionada	Amenazas que se producen por errores o descuidos o ingeniería social para obtener información confidencial o credenciales de acceso.

Tabla 1-9. Amenazas Internas (Chang & Hawamdeh, 2020, pág. 27)

1.1.3.6 *Ataques coordinados*

Los ataques coordinados son otro problema más perverso que afecta a la organización, utilizan el engaño y la coordinación involucrando a personal interno o externo, dominios sociales y tecnológicos para que las organizaciones no puedan funcionar ni confiar una en la otra. (Chang & Hawamdeh, 2020, pág. 27 y 28).

1.1.4 HACKING ÉTICO

Hacking Ético del inglés ethical hacking se refiere al uso no violento de una tecnología (pentesting) en demanda de una causa, política u otro tipo. A menudo es legal y moralmente ambiguo. (Maurushat, 2019, pág. 7).

1.1.4.1 *Beneficios del Hacking Ético*

Existe una variedad de beneficios, pero este estudio resume los principales de acuerdo a (Chakraborty, Chakrabarti, & Balas, 2019, pág. 217):

- ✓ Defender la seguridad nacional y luchar contra el terrorismo.
- ✓ Evitar que los atacantes informáticos malintencionados accedan al sistema informático.
- ✓ Disponer de medidas preventivas aceptables para evitar infracciones de seguridad.

1.1.4.2 *Fases del Hacking Ético*

El Hacking ético actúa a partir de un orden lógico según la Figura 1-2 y lo define (Singh, 2019, págs. 25 - 27) y (Astudillo, 2018):

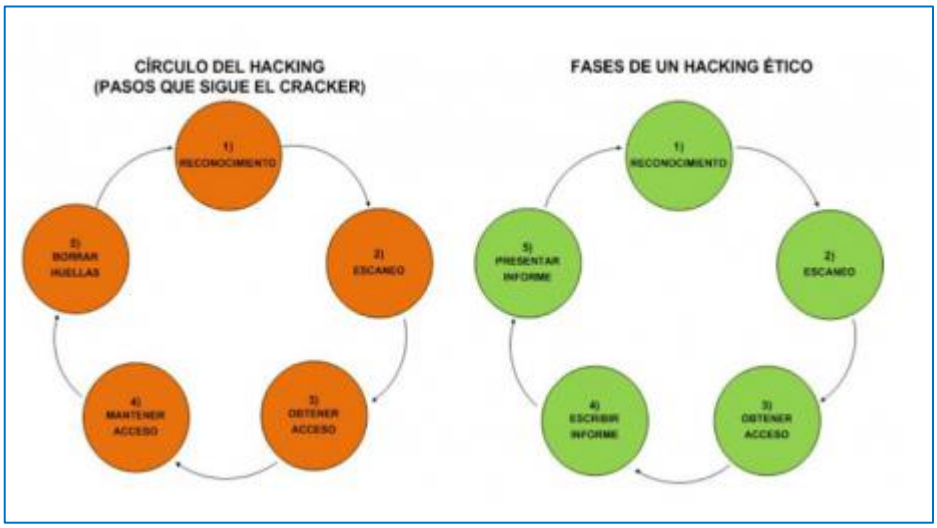

Figura 1-2.Fases de Hacking Ético (Astudillo, 2018, pág. 11)

Reconocimiento o recopilación de la información es la primera fase en donde el atacante se centra en adquirir información significativa sobre el posible objetivo (cliente o víctima).

Esta fase tiene dos tipos de reconocimiento según (Guitérrez Salazar, 2019, pág. 140 y 185):

Reconocimiento Pasivo consiste en la obtención de información sin la interacción directa con el objetivo (cliente o victima).

Reconocimiento Activo consiste en la obtención de información con la interacción directa del objetivo (cliente o victima).

Exploración o Escaneo esta fase se refiere a hacer uso de la información recolectada en la fase anterior para crear perfiles del objetivo, sus sistemas, la red e infraestructura.

Obtención del acceso o explotación esta fase se refiere al uso de la información de las fases anteriores para explotar el objetivo, mediante la explotación exitosa de las vulnerabilidades, ejecutar remotamente el objetivo y obtener acceso.

Mantener el acceso esta fase se garantiza tener acceso al sistema o red de la víctima en cualquier momento.

Presentar Informe esta fase se refiere a llevar a cabo la detección y eliminación de rastros que demuestran la intrusión y de esta manera no ser descubiertos y seguir con el acceso al objetivo sin dejar sospechas, por esta razón es también conocida como limpieza de huellas o cubrir pistas.

1.1.4.3 *Tipos de Hacking Ético*

Existe una diversa tipificación de hacking ético, este estudio trata los tipos de hacking ético dependiendo de donde se ejecutan las pruebas de instrucción según (Astudillo, 2018, pág. 11).

Hacking Ético Externo este tipo de hacking se lo realiza sobre la infraestructura de red expuesta al internet o también conocida como red pública del cliente.

Hacking Ético Interno este tipo de hacking se ejecuta en la red interna del cliente y sirve para encontrar más huecos de seguridad que en la contraparte externa.

1.1.4.4 *Tipos de Hackers Éticos*

Existe diferentes filosofías de clasificación de hackers, pero este estudio trata los principales en función de su intención, del sistema de piratería y según (Guitérrez Salazar, 2019, pág. 55) y (Maurushat, 2019, pág. 20) se tiene:

Hackers de Sombrero Blanco conocido también como el hacker bueno a pesar que tiene capacidades destructivas son contratados para comprobar la seguridad de un sistema y hacer las recomendaciones de seguridad.

Hackers de Sombrero Negro es el tipo de hacker cuya misión principal es comprometer la seguridad de la información con la finalidad de obtener beneficios personales.

Hacker de Sombrero Gris este tipo de hacker es alguien que aplica los dos tipos de hacker anteriores y ataca para probarse a sí mismo o para mejorar la seguridad en general probando que existe una falla.

1.1.4.5 *Modalidades de Hacking*

El servicio de hacking ético se puede ejecutar en una de las tres modalidades que se mencionan a continuación, este terminó también es conocido como tipos de penetración o pruebas de penetración según (Guitérrez Salazar, 2019, pág. 91 y 92), (Astudillo, 2018, pág. 12) y (Singh, 2019, pág. 21 y 22):

Black Box Hacking o hacking de caja negra o prueba lápiz, se refiere a la modalidad que se aplica para hacer pruebas de penetración o intrusión externas, donde el cliente no dará ninguna o muy poca información, ni acceso interno, esta modalidad es la más costosa, difícil, y solo es realizada por pentesters experimentados.

Gray Box Hacking o hacking de caja gris, se refiere a la modalidad que se aplica para hacer pruebas de penetración o intrusión externas e internas, donde el cliente brinda cierta información o nivel de acceso interno a la institución u organización, este tipo de modalidad es el más usado y efectivo para mejorar la seguridad empresarial.

White Box Hacking o hacking de caja blanca o caja transparente abierta y lógica, se refiere a la modalidad que se aplica para hacer pruebas de penetración o intrusión internas, donde el cliente proporciona toda la información y credenciales de diversos grados sobre lo que se vaya a auditar, de esta manera se puede examinar la gran cantidad de datos disponibles para identificar minuciosamente todas las vulnerabilidades.

1.1.5 POLÍTICAS DE SEGURIDAD INFORMÁTICA

Las políticas de seguridad informática son declaraciones formales de las reglas o directrices organizacionales y practicas óptimas que deben cumplir los usuarios que tienen acceso a los activos de tecnologías e información de una organización o institución. (Carisio, 2020), (Misfud, 2020) y (EducaAragon, 2020).

1.1.5.1 *Tipos de políticas de seguridad informática*

Las políticas de seguridad se pueden dividir en tres tipos o categorías según (ATEB, 2020, pág. 13):

Las políticas regulatorias señalan estándares asociados que deben seguir para una política definida de cumplimiento obligatorio tanto en leyes y reglamentos específicos para la organización o institución.

Las políticas consultivas señalan a los empleados los comportamientos y actitudes que deben apegarse y evitar. Define además como procesar la información confidencial.

Las políticas informativas mantienen informados a los empleados de las organizaciones de ciertos tópicos relevantes.

1.1.5.2 *Mecanismos de seguridad*

Los mecanismos de seguridad se dividen en tres grupos de acuerdo a la Tabla 1-10:

Mecanismo	Definición
Prevención	Evitar desviaciones a la política de seguridad.
Detección	Detectar las desviaciones si se producen violaciones o intentos de violaciones a la seguridad.
Recuperación	Accionar luego de ocurrir una violación de seguridad para que el sistema vuelva a su normal funcionamiento.

Tabla 1-10. Mecanismos de seguridad. (Misfud, 2020)

1.1.5.3 *Etapas de las políticas de seguridad informática*

Las políticas de seguridad informática se definen en cuatro etapas según (EducaAragon, 2020):

La definición de las necesidades de seguridad es el primer escalón a la hora de establecer una política de seguridad, cuyo objetivo es determinar las necesidades mediante la elaboración de un análisis de vulnerabilidades y posibles amenazas.

La implementación de una política de seguridad consiste en establecer los métodos y mecanismos diseñados para que el sistema o empresa sea segura y la aplicación de las reglas definidas en la política de seguridad.

Realizar una auditoría de seguridad sirve para validar las medidas de protección adoptadas en el diseño de la política de seguridad.

La definición de las acciones trata de prever y planificar medidas a tomarse cuando se detecte una amenaza, se conoce como etapa de reacción.

1.2. SEGURIDAD PERIMETRAL INFORMÁTICA

La Seguridad Perimetral Informática se define como un concepto emergente que agrupa todos los elementos de red que establecen la barrera defensiva para aislar la red local interna y la propia red local de servicio de las entradas externas. En resumen, es el perímetro de seguridad que posibilita manejar y controlar el acceso a la red interna de la organización. (Castellanos Crespo, 2020, pág. 5).

1.2.1 FUNCIONES DE LA SEGURIDAD PERIMETRAL INFORMÁTICA

La Seguridad Perimetral Informática debe abarcar las siguientes funciones básicas para proteger la red de datos de acuerdo (Abad Domingo, 2018, pág. 139):

- ✓ Rechazo de las conexiones desde clientes externos a servicios esencialmente sensibles.
- ✓ Discrimina los diferentes tipos de tráfico, diferenciando el tráfico que provine de la LAN de la red externa. (Uso de políticas diferentes en el tratamiento del tráfico).
- ✓ Selecciona el tráfico procedente o dirigido hacia determinados nodos de la red.
- ✓ Proporciona un punto único de conexión con el exterior.
- ✓ Redirecciona el tráfico de entrada permitiendo hacia los sistemas alojados en la propia red de perímetro o en la red interna (Rechaza el tráfico prohibido).
- ✓ Oculta los servicios vulnerables (No son Visibles a la red externa).
- ✓ Oculta información sobre las características de la red interna (nombres de sistemas, topología de red, cuentas de usuarios, dispositivos de red, etc.)

1.2.2 HERRAMIENTAS DE SEGURIDAD PERIMETRAL INFORMÁTICA

Hay una variedad de herramientas de seguridad perimetral informática, en este estudio se hace la revisión bibliográfica de las más importantes.

1.2.2.1 *CORTAFUEGOS*

Cortafuegos o Firewall es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad. (Cisco, 2020) y (Abad Domingo, 2018).

La utilización de un cortafuegos es necesaria cuando queremos proteger zonas de la red, de ataques que provengan del exterior o ataques que se originen en el interior de la organización o institución.

Tipos de Cortafuegos

Filtrado de paquetes estático, sin estado stateless es el modo de filtrado más básico de un cortafuegos, consiste en el rechazo o aceptación en función de alguno o varios de los campos de un

paquete. Este tipo de filtrado resuelve la mayoría de necesidades (Abad Domingo, 2018, pág. 143). Cuenta con dos modos básicos para la configuración de reglas de acuerdo a la Tabla 1-11 y conocidos como políticas.

Tipo de Política	Descripción
Restrictiva	Denegar todo tráfico por defecto, salvo el que se acepta explícitamente.
Permisiva	Aceptar todo el tráfico, salvo el que se deniegue explícitamente.

Tabla 1-11. Tipos de Políticas (Chicano Tejada, 2014, pág. 236) y (Abad Domingo, 2018, pág. 143)

Filtrado dinámico de paquetes o statefull se refiere al tipo de filtrado donde las reglas se crean y se destruyen dinámicamente, tiene varias ventajas por ser un mecanismo confiable para filtrar el tráfico, aunque también posee un inconveniente pues su operación de filtrado está basada en la cabecera del paquete, por esta razón algunos dispositivos de filtrado combinan el filtrado estático y dinámico. (Abad Domingo, 2018, pág. 145).

Cortafuegos de inspección de estado usa los tipos de filtrado mencionado preliminarmente y construye una tabla en la que registra el estado de las conexiones activas en cada momento. Opera inspeccionando el primer paquete de una conexión y registra los datos de la conexión iniciada, después dejan pasar el resto de paquetes de esta conexión mientras que se rechazan todos los paquetes que no se relaciona con una conexión activa, el cortafuegos dispara temporizadores que informan cuando caduca una conexión. (Abad Domingo, 2018, pág. 145).

Cortafuegos basados en proxy este tipo de cortafuego opera en capas superiores de la arquitectura de red por lo general desde la aplicación o superior. Básicamente existen dos tipos de cortafuegos basados en proxy esto se describe según la Tabla 1-12:

Tipos de Cortafuegos Basados en Proxy	Modo de Operación
Pasarelas de Nivel de Aplicación	El usuario solicita el servicio requerido a la pasarela identificada por una dirección IP y por un número de puerto de servicio. La pasarela solicita la identificación del sistema cliente que se pretende conectar. El usuario responde a la petición de autentificación presentada por la pasarela. Si es correcto la pasarela conecta con el sistema remoto y comienza un dialogo de intercambio de datos.
Pasarelas a nivel de circuito	Los servicios se solicitan a un único puerto por donde el proxy recoge las peticiones de sus clientes. Las pasarelas opcionalmente autentifican al usuario. Si todo es correcto el proxy conecta al servicio solicitado. Luego de validar la conexión no se inspección el contenido de ningún paquete.

Tabla 1-12. Tipos de Cortafuegos basados en proxy. (Abad Domingo, 2018, pág. 146 y 147)

Arquitectura de cortafuegos

En este estudio se presenta las principales arquitecturas de un enfoque perimetral en la Tabla 1-13:

Arquitectura	Descripción
Screenning Router	Un router realiza la función de filtrado de paquetes, posee dos interfaces de red para la red interna y red externa). Intercepta todo el tráfico (entrada y salida) y lo redirige a su destinatario en función de las reglas de filtrado.
Dual-Homed Host	Un equipo servidor (host bastión dual-homed) realiza tareas de filtrado y enrutamiento mediante al menos dos tarjetas de red se conecta lógica y físicamente a segmentos de red separados.
Screened Host	Compuesto por un router para el filtrado de paquetes y un servidor (host bastión) para el filtrado de conexiones a nivel de circuito y aplicación, de esta manera se dirige todo el tráfico de la red externa al servidor y es el único al que se accede desde fuera de la red local ya que se permite ciertos tipos de conexiones y protocolos
Screened Subnet	Conocida como Zona Desmilitarizada (DMZ) se refiere que el cortafuegos se base en el uso de router de filtrado de paquetes en el host bastión y la red interna, en el host bastión se encontrará entre los dos routers (interno y externo, uno se encuentra entre la red perimetral y la red externa y el otro entre la red perimetral y la red interna).

Tabla 1-13. Arquitecturas de cortafuegos (Costas Santos, 2006, pág. 169), (Chicano Tejada, 2014, págs. 252 - 254) y (Abad Domingo, 2018, págs. 148 - 152)

Otras Arquitecturas

Luego de la revisión de la literatura de las arquitecturas básicas y principales se deriva las siguientes variaciones para cubrir las necesidades según la Tabla 1-14Tabla 1-13:

Variación de Arquitecturas	Descripción
Varios Host Bastion o más	Uso de varios host bastion para aumentar el rendimiento de los servicios, obtener servicios de apoyo con introducción de redundancia y separar los servicios, determina la necesidad de niveles distintos de seguridad.
Red perimetral con un solo router	Crea una red perimetral utilizando un solo router que cumpla las funciones de un router externo y otro interno a la vez, procesa el tráfico y filtrado de la red interna como externa.
Host Bastion como router externo	Conexión de dos redes mediante dos interfaces diferentes, de esta forma el filtrado de paquetes y de servicios proxys los ejecuta el mismo host.

Tabla 1-14.Variación de Arquitecturas de Cortafuegos (Chicano Tejada, 2014, pág. 257 y 258).

1.2.2.2 *RED PRIVADA VIRTUAL (VPN)*

Red Privada Virtual del inglés Virtual Private Network VPN es una tecnología de red utilizada para conectar una o varias computadoras a una red privada utilizando Internet mediante canales públicos seguros que permiten el acceso de empleados desde sus hogares a recursos corporativos (Welivesecurity, 2020) y (Abad Domingo, 2018).

Arquitecturas VPN

Las arquitecturas básicas de VPN de acuerdo a la Tabla 1-15 son tres:

Arquitecturas VPN	Descripción
VPN de acceso remoto o Road Warrior	Permite conectarse directamente a la red local o de la empresa desde sitios remotos mediante internet.
VPN punto a punto o Site-to-Site	Permite conectar ubicaciones remotas con la sede central de la organización mediante un vínculo permanente a internet.
VPN Over LAN	Emplea la misma red de área local LAN de la empresa como medio de conexión dentro de la misma empresa.

Tabla 1-15. Arquitecturas de VPN. (Abad Domingo, 2018, pág. 154) (Costas Santos, 2006, pág. 145 y 146)

Protocolos

Las VPN usan protocolos como medio de protección de esta manera cifra los datos que envía y recibe, los principales protocolos según (Goujon, 2020) y (Costas Santos, 2006, pág. 146) son los referidos en la Tabla 1-16:

Protocolos	Descripción
IPsec	Protocolo que permite mejorar la seguridad a través de algoritmos de cifrado robustos y un sistema de autentificación más exhaustivo, mediante dos métodos de encriptado, modo transporte y modo túnel.
PPTP/MPPE	Point to Point Tunneling Protocol es un protocolo desarrollado por un consorcio formado por varias empresas, soporta varios protocolos VPN utilizando el protocolo Microsoft Point to Point Encryption.
L2TP/Ipsec	Protocolo capaz de proveer el nivel de protección de IPsec sobre el protocolo de túnel L2TP.

Tabla 1-16. Protocolos de VPN (Goujon, 2020) y (Costas Santos, 2006, pág. 146)

1.2.2.3 *SISTEMA DE DETECCIÓN DE INTRUSIONES (IDS)*

Sistema de Detección de Intrusiones es un software de seguridad cuya función es detectar accesos no autorizados en una red de ordenadores para lo cual genera algún tipo de alerta o log para que pueda ser gestionado por el administrador de red correspondiente. (Siemlab, 2020), (Abad Domingo, 2018)

Clasificación de IDS

Los sistemas de detección de intrusos se clasifican de acuerdo a la Tabla 1-17 y Tabla 1-18:

IDS	Descripción
IDS basados en Red	Monitorea el tráfico de red en un segmento o dispositivo y analiza la red y la actividad de los protocolos para identificar actividades sospechosas.
IDS basados en Host	IDS basado en abonado de la red se refiere a un equipo que monitorea las características del dispositivo y los eventos que ocurren en él.
IDS basado en Conocimiento	Se refiere a una base de datos de perfiles de vulnerabilidades de sistemas ya conocidos para identificar intentos de intrusión activos.

Tabla 1-17. (a) Clasificación de los IDS (Escrivá Gascó, Romero Serrano, Ramada, & Onrubia Pérez, 2013, pág. 184), (Infotecs, 2020) y (Abad Domingo, 2018, pág. 158)

IDS	Descripción
IDS basado en Comportamiento	Se refiere al análisis de comportamiento del tráfico siguiendo una línea base o estándar de actividad normal del sistema para la identificación de los intentos de intrusiones.
IDS Activo	Se refiere al momento en que se determina el bloqueo automáticamente de ataques o actividades sospechosas que sean de su conocimiento sin la necesidad de la intervención humana.
IDS Pasivo	Se refiere al monitorear el tráfico que pasa a través de él identificando potenciales ataques o anormalidades y basados en ellos generar alertas para administradores y equipos de seguridad.

Tabla 1-18.(b) Clasificación de los IDS (Escrivá Gascó, Romero Serrano, Ramada, & Onrubia Pérez, 2013, pág. 184), (Infotecs, 2020) y (Abad Domingo, 2018, pág. 158)

Detección de Anomalías en un IDS

Detección de anomalías o también conocido como detecciones fallidas se refiere al hecho de la actividad intrusiva, constituye un conjunto de anomalías expuestas en la detección. La mayoría de las actividades intrusivas resulta de la suma de otras actividades individuales así las intrusiones pueden clasificarse según la Tabla 1-19:

Intrusiones	Descripción
Falsos negativos	Conocidos como intrusivas, pero no anómalas se refiere intrusiones que dan una falsa sensación de seguridad del sistema.
Falsos Positivos	Conocidos como no intrusivas, pero anómalas se refiere a las intrusiones que el sistema indica erróneamente la existencia de intrusión por lo tanto deben minimizarse.
Negativos Verdaderos	Conocidos como no intrusiva ni anómala se refiere a la actividad que no es intrusiva y el sistema indica como tal.
Positivo Verdaderos	Conocidas como intrusiva y anómala se refiere a la actividad que es intrusiva y es detectada por el sistema y que requieren acciones para mitigar los ataques.

Tabla 1-19. Clasificación de Actividades Intrusivas (Infotecs, 2020) y (Abad Domingo, 2018, pág. 157)

Características del IDS

Un sistema de detección de intrusos según (Infotecs, 2020) debe contar con las siguientes características:

- ✓ Funcionar continuamente sin supervisión humana.
- ✓ Tolerante a fallos.
- ✓ Resistente a perturbaciones.
- ✓ Imponer mínima carga sobre el sistema.
- ✓ Observar desviación sobre el comportamiento estándar.
- ✓ Fácilmente adaptable al sistema operativo ya instalado.
- ✓ Hacer frente a los cambios de comportamiento del sistema.

- ✓ Identificar de donde proviene los ataques que sufren.
- ✓ Difíciles de vulnerar y suministrar a los especialistas de seguridad cierta tranquilidad.

1.2.2.4 *SISTEMA DE PREVENCIÓN DE INTRUSIONES (IPS)*

Sistema de Prevención de Intrusiones evita que los ataques o intrusiones pueden afectar a las redes, mantiene el sistema actualizado y alerta frente a las amenazas (Pandasecurity, 2020) y (Abad Domingo, 2018).

La utilidad del sistema de prevención de intrusos es monitorear actividades para identificar comportamientos maliciosos, sospechosos e indebidos a fin de reaccionar ante ellos en tiempo real. Los IPS fueron creados como una alternativa de seguridad para los cortafuegos y los IDS, de esto muchas características son similares o heredadas. (Escrivá Gascó, Romero Serrano, Ramada, & Onrubia Pérez, 2013, pág. 184) y (Infotecs, 2020).

Los IPS toman decisiones de control de acceso basados en el contenido de tráfico y de manera proactiva establece políticas de seguridad para proteger el equipo o la red de posibles ataques. (Escrivá Gascó, Romero Serrano, Ramada, & Onrubia Pérez, 2013, pág. 184) y (Infotecs, 2020).

Clasificación de los IPS

Los IPS se pueden clasificarse por el método que realizan la detección y por la tecnología, esto se detalla en la Tabla 1-20:

Clasificación IPS		Descripción
De acuerdo al Método de Detección	**IPS basado en firmas**	Usa una base de firmas que reflejan patrones conocidos de ataques de seguridad en un dispositivo o red.
	IPS basado en Anomalías	Conocido como basado en perfil, intenta identificar un comportamiento diferente que se desvié de alguna forma de la actuación normal del dispositivo o red.
	IPS basado en Políticas	Usa políticas de seguridad que reconocen el tráfico definido por el perfil establecido permitiendo o descartando paquetes de datos, es muy similar su forma de funcionamiento a un cortafuegos.
	IPS basado en detección por Honeypot	Usa un equipo que a primera vista parezca vulnerable e interesante para un ataque y mediante esta forma obtener evidencia de la forma de actuar para implementar medidas para mitigar los ataques.
De acuerdo a su Tecnología	**IPS basado en Host**	Se refiere que el host monitoree las características de un dispositivo o de un abonado de la red en particular para detectar actividades dentro del mismo.
	IPS basado en Red	Se refiere a realizar el monitoreo sobre el tráfico que fluye a través de segmentos particulares, se analizan protocolos de red, de transporte, y de aplicación para identificar actividades sospechosas.
	IPS de Nueva Generación	Permite tener visibilidad sobre el comportamiento de red, perfiles de los equipos dentro de la infraestructura de comunicación y la identidad de los usuarios y las aplicaciones que están en uso de tal forma que esta información sirva para mitigar automáticamente.

Tabla 1-20. Clasificación de los IPS (Infotecs, 2020).

1.2.2.5 *HONEYPOT*

Honeypot conocido como tarro de miel o sistema de detección y engaño, es una implementación de tecnología informática o de red diseñado para detectar, desviar o contrarrestar amenazas de seguridad. Para ello está configurado expresamente con servicios de red ficticios con el fin de llamar la atención a los ciber atacantes y de esta manera engañarlos o llevarlos a ejecutar rutinas maliciosas. (T-Systems, 2020), (Abad Domingo, 2018) y (Haber & HIbbert, 2018).

Clasificación de Honeypot

Los honeypot se pueden clasificar por el método de despliegue y por la interacción según la Tabla 1-21:

Clasificación de Honeypot		Descripción
Por el Método de Despliegue	Production Honeypot	Usado en empresas y organizaciones con el fin de investigar los motivos de los ciberdelincuentes para desviar y mitigar el riesgo de ataques en la propia red.
	Research Honeypot	Se usa por organizaciones sin fines de lucro o instituciones educativas con el fin de investigar los motivos y las tácticas, se las comunica al hacker para apuntar las diferentes redes, más usado para el tema investigativo.
Por Interacción	Honeypot de Alta Interacción	Se refiere a que la imitación de sistema operativo o aplicaciones es real a los que ofrecen un servidor.
	Honeypot de Baja Interacción	Se refiere a que la imitación simula un sistema operativo o aplicaciones con funciones a la medida que se produzca un ataque.

Tabla 1-21. Clasificación Honeypot (T-Systems, 2020), (Abad Domingo, 2018, pág. 160) y (Rodríguez, 2020)

1.2.2.6 *ANTIVIRUS*

Antivirus es un software de seguridad especial cuyo objetivo es brindar una mejor protección, a través de múltiples capas de protección detecta, bloquea y elimina malware y protege a los usuarios sin afectar el rendimiento y velocidad de los dispositivos. (Eset, 2020) (Softwarelab, 2020), (Koret & Bachaalany, 2015, pág. 3) y (Abad Domingo, 2018).

La utilidad del antivirus es escanear los dispositivos de almacenamiento para encontrar y eliminar virus de los dispositivos y redes. (Moes, 2020)

Clasificación de Antivirus

Los antivirus se pueden clasificar de acuerdo a la siguiente categoría según la Tabla 1-22:

Clasificación	Descripción
Antivirus Autónomo	Herramienta especializada para detectar y eliminar ciertos virus, algunas de las veces pueden ser portables, están diseñados para recibir actualizaciones con nuevas definiciones diarias.
Paquetes de Seguridad	Capaces de detectar y eliminar virus y vienen equipados para contrarrestar malware con el fin de proporcionar una protección absoluta para el dispositivo. Algunos de ellos traen funciones adicionales como gestión de contraseñas.
Antivirus en la nube	Análisis de archivos en la nube en lugar del ordenador permitiendo una respuesta más rápida.

Tabla 1-22. Clasificación de Antivirus (Moes, 2020)

1.2.2.7 *UNIFIED THREAT MANAGEMENT UTM*

La utilidad de una UTM o Gestión Unificada de Amenazas está basada en integrar en un único dispositivo un conjunto de soluciones de seguridad perimetral, son conocidas como sistemas all-in-one o appliances. (Abad Domingo, 2018, pág. 164).

Son la tendencia actual en las pequeñas empresas por el ahorro de costos en soluciones de seguridad. (Escrivá Gascó, Romero Serrano, Ramada, & Onrubia Pérez, 2013, pág. 185).

Filosofía de la UTM

La filosofía de una UTM es procesar y analizar todo el contenido antes de que ingresa a la red corporativa de esta manera limpia la red de malware, de páginas webs maliciosas mediante filtros avanzados. (Firewalls Hardware, 2020).

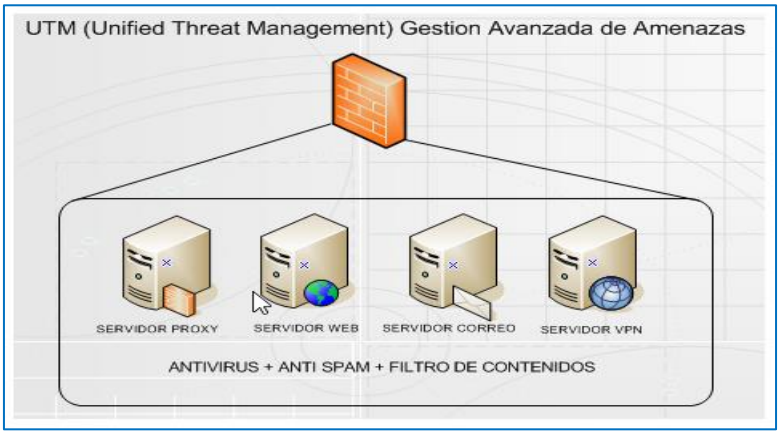

Figura 1-3. UTM (Firewalls Hardware, 2020)

CAPITULO II

2. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA SEGURIDAD INFORMÁTICA DEL LTIC

Esta sección cubre el análisis de la situación actual de la seguridad del LTIC, resumen y análisis de la gravedad de las vulnerabilidades escaneadas mediante software de escaneo Nessus profesional, OpenVAS, Legion y GFI LandGuard de la red externa e interna del LTIC, inteligencias de amenazas y resumen de puertos abiertos.

2.1. SITUACIÓN ACTUAL DE LA INFRAESTRUCTURA DEL LTIC

El avance tecnológico que se experimenta a diario vivir, originó el crecimiento en la infraestructura del LTIC para proporcionar distintos servicios tecnológicos a los estudiantes, docentes, personal administrativo y a terceros (público en general).

La infraestructura física del LTIC cuenta con 6 aulas laboratorios, 2 aulas para investigación, una sala de servidores, una sala para proyectos formativos y de investigación, una oficina para el director y otra para el ayudante del LTIC, una bodega de equipos y un área comunal, las aulas cuenta con una identificación numérica que va desde el 201 hasta la 215.

La infraestructura tecnológica del LTIC sigue un esquema tradicional de una red que consiste en tres servidores marca Hewlett-Packard, modelos ProLiant DL 380 G6, ProLiant DL 380 G9 y ProLiant DL 380 G10, cuatro equipos de comunicación switch marca Cisco, 3 modelo SG300X-48 y uno SG500X-48P, red cableada basada en la topología tipo estrella de acuerdo al estándar ANSI/TIA/EIA-568-B y ANSI/TIA/EIA-569-A para el cableado horizontal y vertical, cuenta con 20 puntos de red por aula laboratorio (aulas: 201, 202, 203, 204, 214 y 215) y 20 puntos de red en la área comunal, 90 computadoras de escritorio marca HP, procesador Intel Core I7, 9 computadoras de escritorio marca HP procesador Intel Core 2 Quad todas ellas con sistema operativo Windows 10 Pro y 15 computadoras portátiles, el data center cuenta con sistema UPS para garantizar el funcionamiento de los servidores en el caso de pérdida de energía.

El acceso físico al área de data center, las oficinas y aulas del LTIC es considerado restringido con excepción del director, ayudante, pasantes y becarios o previa solicitud de acceso autorizada por el director del LTIC y en el caso de las aulas el acceso a estudiantes y docentes se realiza de acuerdo a los horarios prestablecidos según la carga horaria.

El LTIC maneja un segmento de red LAN con direccionamiento IP en el rango 172.16.0.1 a 172.16.1.255 manejado por un servicio de DHCP tanto para la red cableada como para la inalámbrica, además dispone de una IP pública 186.5.66.122 en la cual se encuentra alojada el portal web de la facultad, portal web de Anuros PUCE, portal web del III Congreso Internacional de Sistemas Inteligentes y Nuevas Tecnologías y página web de Consulta de Notas de la Facultad.

La seguridad del LTIC está compuesta por un servidor UTM CAMEO Untangle, que maneja la protección contra robo de información sensible, prevención de intrusiones y filtrado web, conjuntamente trabaja con un servidor controlador de dominio (sistemas.local) que además funciona como servidor DNS, un servidor de licenciamiento que permite actualizaciones del antivirus McAfee y actualizaciones del sistema operativo, un servidor proxy, un servidor LimeSurvey, un servidor para programación avanzada, un servidor para el portal web de anuros, un servidor el portal web de III Congreso, un servidor del portal web de la Facultad , un servidor HP Integrated Lights-Out 2 para actualización de firmware y uso de equipos remotos de equipos Hewlett-Packard, estos servidores se encuentran virtualizados mediante la plataforma VMware. Además, cuenta con un enlace de Internet proporcionado por la Dirección de Informática de la PUCE, con ancho de banda de 70 Mbps cuyo proveedor ISP es Megadatos como lo muestra la Figura 2-1 del test de velocidad realizado desde el equipo A214-20.

Figura 2-1. Test de velocidad Speedtest (Salazar Gualoto, 2020)

Los puntos de acceso inalámbrico que existe en el área física del LTIC no están a cargo del mismo, pertenecen a la Dirección de Informática de la PUCE estos equipos cuentan con una red WLAN de nombre “La Puce” para proporcionar a los usuarios movilidad y acceso a los servicios tecnológicos y otros recursos de la facultad y universidad respectivamente.

2.2. ANÁLISIS INICIAL DE VULNERABILIDADES DE LA RED LTIC

Para el análisis inicial de las vulnerabilidades de la red del LTIC se realizó hacking ético basado en la metodología caja gris con las herramientas, Nessus profesional, OpenVAS, Legion y GFI LandGuard, los resultados se presentan en las siguientes secciones.

Se realizó la identificación de los equipos activos y se encontró los equipos que se describen en la Tabla 2-1, basados en esta información se realizó el análisis de las vulnerabilidades.

IP	Sistema Operativo	Nombre de Equipo	Tipo de Equipo
172.16.0.1	Microsoft Windows Server 2008		
172.16.0.2		win-proxy	Máquina virtual
172.16.0.4			Máquina virtual
172.16.0.5	Microsoft Windows Server 2012 R2 Standard	win-domaincontroller	
172.16.0.6	Microsoft Windows Server 2012 R2 Standard		Máquina virtual
172.16.0.7	Microsoft Windows Server 2012 R2 Standard	Winproyint	
172.16.0.8	Microsoft Windows Server 2012 R2 Standard	Serverlicenciamiento	Máquina virtual
172.16.0.10	Microsoft Windows Server 2012 R2 Standard	win-progava	Máquina virtual
172.16.0.12	Microsoft Windows Server 2012 R2 Standard	ayudanteltic-ubuntu	Máquina virtual
172.16.0.17			Máquina virtual
172.16.0.18	Microsoft Windows Server 2012 R2 Standard	win-webserver	Máquina virtual
172.16.0.19	dell power vault md3 series storage array		
172.16.0.20	Linux Kernel 4.15 en Ubuntu 18.04 (bionic)		Máquina virtual
172.16.0.21	Linux Kernel 2.6 ubuntu	moodleubuntu.	Máquina virtual
172.16.0.41	CISCO IOS 12.0	Switchap	Router
172.16.0.42	CISCO IOS 12.0		Router
172.16.0.43	CISCO IOS 12.0	switchc0fc6e	Router
172.16.0.44	CISCO IOS 12.0	switchd1a3e1	Router
172.16.0.54	CISCO IOS 15	Switch	
172.16.0.58	Conmutador 3Com 4500 de 26 puertos	4500	Swicth
172.16.0.92	Windows 10 Pro 6.3	a214-20	Hewlett Packard
172.16.0.93	Conmutador 3Com 4500 de 26 puertos	4500	Switch
172.16.0.95	Conmutador 3Com 4500 de 26 puertos	4500	Switch
172.16.0.190	Windows 10 Pro 6.3	a202-07	Hewlett Packard
172.16.1.52	HP Integrated Lights-Out	ilohnf0gmqzk0f3	HP ProLiant DL380 G6
172.16.1.76		Proxy	

Tabla 2-1. Equipos Activos Red LAN LTIC (Salazar Gualoto, 2020)

2.2.1 ANÁLISIS CON NESSUS PROFESIONAL

Se realizo un escaneo de la red del LTIC mediante el uso del software Nessus Profesional los informes completos para mayor detalle se encuentran en el Anexo 1 y 2. A continuación se presenta un resumen procesado de los resultados.

2.2.1.1 *Análisis de la Red Externa puceing.edu.ec*

Nessus Profesional determinó los siguientes resultados por gravedad de acuerdo a la Figura 2-2 de la red externa puceing.edu.ec y que se describen en el resumen de análisis por gravedad.

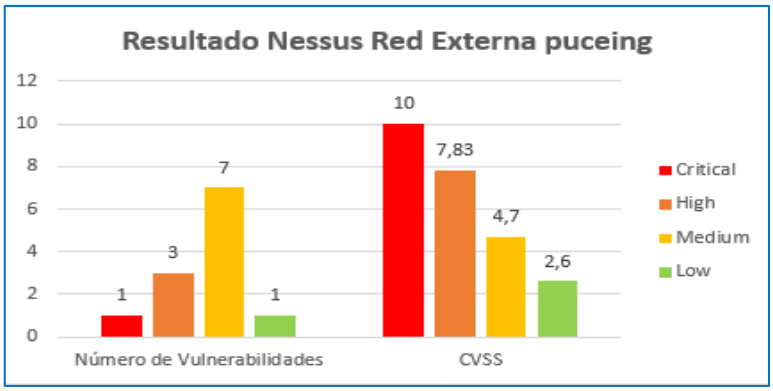

Figura 2-2. Resultado de Vulnerabilidades Puceing, Nessus (Salazar Gualoto, 2020)

RESUMEN DE ANÁLISIS POR GRAVEDAD

Vulnerabilidades de Seguridad por Gravedad Critical

CVSS	Plugin	Origen y Vulnerabilidad
10.0	58987	PHP Unsupported Version Detection

Tabla 2-2.Resumen Vulnerabilidades Gravedad Critical Puceing Nessus (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad High

CVSS	Plugin	Origen y Vulnerabilidad
8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
7.5	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.

Tabla 2-3.Resumen Vulnerabilidades Gravedad High Puceing, Nessus (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Medium

CVSS	Plugin	Origen y Vulnerabilidad
5.0	33270	ASP.NET DEBUG Method Enabled
5.0	40984	Browsable Web Directories
5.0	11213	HTTP TRACE / TRACK Methods Allowed
5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
4.3	136929	JQuery 1.2 < 3.5.0 Multiple XSS
4.3	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability
4.3	85582	Web Application Potentially Vulnerable to Clickjacking

Tabla 2-4. Resumen Vulnerabilidades Gravedad Medium Puceing, Nessus (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Low

CVSS	Plugin	Origen y Vulnerabilidad
2.6	26194	Web Server Transmits Cleartext Credentials

Tabla 2-5. Resumen Vulnerabilidades Gravedad Low Puceing, Nessus (Salazar Gualoto, 2020)

2.2.1.2 *Análisis de la Red Interna del LTIC*

Nessus profesional encontró las siguientes vulnerabilidades por gravedad como se observa en la Figura 2-3 en la red interna del LTIC y que se describen en el resumen de análisis por gravedad.

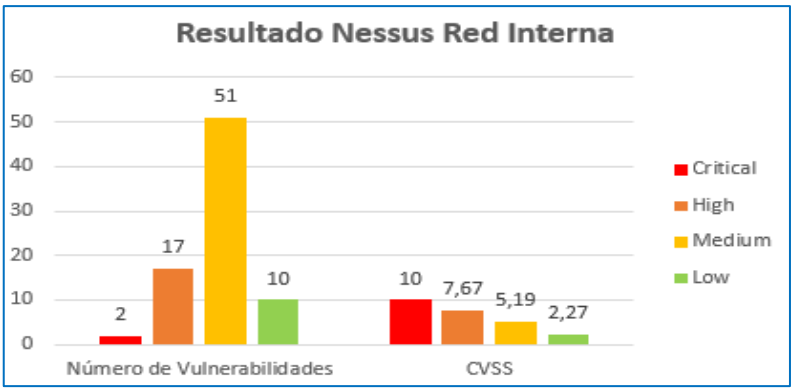

Figura 2-3. Resultado de Vulnerabilidades Red Interna, Nessus (Salazar Gualoto, 2020)

RESUMEN DE ANÁLISIS POR GRAVEDAD

Vulnerabilidades de Seguridad por Gravedad Critical

CVSS	Plugin	Origen y Vulnerabilidad	IP
10.0	58987	PHP Unsupported Version Detection	172.16.0.7, 172.16.0.18, 172.16.0.92
10.0	136890	Telnetd - Remote Code Execution (CVE-2020-10188)	172.16.0.93

Tabla 2-6. Resumen Vulnerabilidades por Gravedad Critical Red Interna, Nessus (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad High

CVSS	Plugin	Origen y Vulnerabilidad	IP
8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities	172.16.0.18, 172.16.0.92
8.5	119766	PHP 7.2.x < 7.2.13 Multiple vulnerabilities	172.16.0.7
8.5	122821	PHP 7.0.x < 7.0.33 Multiple vulnerabilities	172.16.0.7
7.8	80101	IPMI v2.0 Password Hash Disclosure	172.16.1.52
7.8	122257	iLO 2 <= 2.23 Denial of Service Vulnerability	172.16.1.52
7.5	10882	SSH Protocol Version 1 Session Key Retrieval	172.16.0.54
7.5	41028	SNMP Agent Default Community Name (public)	172.16.0.58, 172.16.0.93, 172.16.0.95
7.5	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	172.16.0.7
7.5	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities	172.16.0.92
7.5	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow	172.16.0.92
7.5	121353	PHP 7.2.x < 7.2.14 Multiple vulnerabilities.	172.16.0.7
7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.	172.16.0.18, 172.16.0.92
7.5	123828	PHP 7.2.x < 7.2.16 Multiple vulnerabilities.	172.16.0.7
7.5	128148	Flexera FlexNet Publisher < 11.16.2 Multiple Vulnerabilities	172.16.0.6, 172.16.0.8
7.5	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.	172.16.0.7, 172.16.0.18, 172.16.0.92
7.2	123642	Apache 2.4.x < 2.4.39 Multiple Vulnerabilities	172.16.0.7, 172.16.0.18, 172.16.0.92
7.1	20007	SSL Version 2 and 3 Protocol Detection	172.16.0.6, 172.16.0.54

Tabla 2-7. Resumen Vulnerabilidades por Gravedad High Red Interna, Nessus (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Medium

CVSS	Plugin	Origen y Vulnerabilidad	IP
6.8	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities	172.16.0.92
6.8	122060	Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	172.16.0.7, 172.16.0.92
6.4	51192	SSL Certificate Cannot Be Trusted	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.41, 172.16.0.42, 172.16.0.43, 172.16.0.44, 172.16.0.54, 172.16.0.92, 172.16.0.190
6.4	57582	SSL Self-Signed Certificate	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.41, 172.16.0.42, 172.16.0.43, 172.16.0.44, 172.16.0.54, 172.16.0.92, 172.16.0.190
6.4	101788	Apache 2.4.x < 2.4.27 Multiple Vulnerabilities	172.16.0.7, 172.16.0.92
6.4	123754	PHP 7.2.x < 7.2.17 Multiple vulnerabilities.	172.16.0.7
6.4	124763	PHP 7.2.x < 7.2.18 Heap-based Buffer Overflow Vulnerability.	172.16.0.7
6.4	125639	PHP 7.2.x < 7.2.19 Multiple Vulnerabilities.	172.16.0.7
6.4	128033	Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	172.16.0.7, 172.16.0.18, 172.16.0.92
6.4	134162	PHP 7.2.x < 7.2.28 / PHP 7.3.x < 7.3.15 / 7.4.x < 7.4.3 Multiple Vulnerabilities	172.16.0.7
6.1	104743	TLS Version 1.0 Protocol Detection	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.92, 172.16.0.190
5.8	42263	Unencrypted Telnet Server	172.16.0.54, 172.16.0.58, 172.16.0.93, 172.16.0.95
5.8	50686	IP Forwarding Enabled	172.16.0.1, 172.16.0.44, 172.16.0.58, 172.16.0.93, 172.16.0.95
5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	172.16.0.12
5.8	125642	OpenSSL 1.1.0 < 1.1.0k Vulnerability	172.16.0.7
5.8	127131	PHP 7.2.x < 7.2.21 Multiple Vulnerabilities.	172.16.0.7
5.8	135290	Apache 2.4.x < 2.4.42 Multiple Vulnerabilities	172.16.0.7, 172.16.0.18, 172.16.0.92
5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	172.16.0.1, 172.16.0.5, 172.16.0.8, 172.16.0.12
5.0	10061	Echo Service Detection	172.16.0.6, 172.16.0.10
5.0	10198	Quote of the Day (QOTD) Service Detection	172.16.0.6, 172.16.0.10
5.0	11213	HTTP TRACE / TRACK Methods Allowed	172.16.0.1, 172.16.0.7, 172.16.0.18, 172.16.0.92
5.0	15901	SSL Certificate Expiry	172.16.0.7, 172.16.0.12, 172.16.0.18, 172.16.0.41, 172.16.0.42, 172.16.0.43, 172.16.0.44, 172.16.0.54, 172.16.0.92
5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm	172.16.0.1, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.12, 172.16.0.18, 172.16.0.41, 172.16.0.43, 172.16.0.44, 172.16.0.54, 172.16.0.92
5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.54, 172.16.0.92, 172.16.0.190
5.0	45411	SSL Certificate with Wrong Hostname	172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18
5.0	57608	SMB Signing not required	172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.190
5.0	76474	SNMP 'GETBULK' Reflection DDoS	172.16.0.58, 172.16.0.93, 172.16.0.95
5.0	103838	Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)	172.16.0.7, 172.16.0.92
5.0	104408	OpenSSL 1.0.x < 1.0.2m RSA/DSA Unspecified Carry Issue	172.16.0.92
5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS	172.16.0.18, 172.16.0.92
5.0	111788	Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	172.16.0.7, 172.16.0.18, 172.16.0.92
5.0	121355	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	172.16.0.7, 172.16.0.18, 172.16.0.92
5.0	132726	OpenSSL 1.0.2 < 1.0.2u Procedure Overflow Vulnerability	172.16.0.18, 172.16.0.92
5.0	135926	PHP 7.2.x < 7.2.30 Multiple Vulnerabilities	172.16.0.7

Tabla 2-8. (a) Resumen Vulnerabilidades por Gravedad Medium Red Interna, Nessus (Salazar Gualoto, 2020)

CVSS	Plugin	Origen y Vulnerabilidad	IP
5.0	136741	PHP 7.2.x < 7.2.31 / 7.3.x < 7.3.18, 7.4.x < 7.4.6 Denial of Service (DoS)	172.16.0.7
4.3	26928	SSL Weak Cipher Suites Supported	172.16.0.54
4.3	57690	Terminal Services Encryption Level is Medium or Low	172.16.0.1, 172.16.0.5, 172.16.0.8, 172.16.0.12
4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	172.16.0.1, 172.16.0.5, 172.16.0.12, 172.16.0.92
4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.54
4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	172.16.0.6, 172.16.0.54
4.3	105291	OpenSSL 1.0.2 < 1.0.2n Multiple Vulnerabilities	172.16.0.92
4.3	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities	172.16.0.92
4.3	109945	OpenSSL 1.0.x < 1.0.2o Multiple Vulnerabilities	172.16.0.92
4.3	112119	OpenSSL 1.0.x < 1.0.2p Multiple Vulnerabilities	172.16.0.18, 172.16.0.92
4.3	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability	172.16.0.18, 172.16.0.92
4.3	117500	PHP 7.2.x < 7.2.10 Transfer-Encoding Parameter XSS Vulnerability	172.16.0.7
4.3	117807	Apache 2.4.x < 2.4.35 DoS	172.16.0.7, 172.16.0.18, 172.16.0.92
4.3	121383	OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities	172.16.0.18, 172.16.0.92
4.3	121384	OpenSSL 1.1.0 < 1.1.0j Multiple Vulnerabilities	172.16.0.7
4.3	122504	OpenSSL 1.0.x < 1.0.2r Information Disclosure Vulnerability	172.16.0.18, 172.16.0.92
4.3	136929	JQuery 1.2 < 3.5.0 Multiple XSS	172.16.0.6, 172.16.0.7, 172.16.0.20

Tabla 2-9. (b) Resumen Vulnerabilidades por Gravedad Medium Red Interna, Nessus (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Low

CVSS	Plugin	Origen y Vulnerabilidad	IP
3.3	10663	DHCP Server Detection	172.16.0.5
3.3	11197	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)	172.16.0.58, 172.16.0.93, 172.16.0.95
2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant	172.16.0.1, 172.16.0.5, 172.16.0.8, 172.16.0.12
N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	172.16.0.6, 172.16.0.41, 172.16.0.43, 172.16.0.44
2.6	70658	SSH Server CBC Mode Ciphers Enabled	172.16.0.1, 172.16.0.2, 172.16.0.4, 172.16.0.17, 172.16.0.54, 172.16.0.58, 172.16.0.95, 172.16.1.52, 172.16.1.76
2.6	71049	SSH Weak MAC Algorithms Enabled	172.16.0.54, 172.16.0.58, 172.16.0.95, 172.16.1.52
2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.92
1.9	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability	172.16.0.92
1.9	128115	OpenSSL 1.0.2 < 1.0.2t Multiple Vulnerabilities	172.16.0.18, 172.16.0.92
1.9	128117	OpenSSL 1.1.0 < 1.1.0l Multiple Vulnerabilities	172.16.0.7

Tabla 2-10. Resumen Vulnerabilidades por Gravedad Low Red Interna, Nessus (Salazar Gualoto, 2020)

2.2.2 ANÁLISIS CON OPENVAS

El escaneo de la red del LTIC mediante el uso de software libre OpenVas o Greenbone Vulnerability Management (GVM11) de Greenbone Networks sobre Kali Linux obtuvo los siguientes resultados.

2.2.2.1 *Análisis de la Red Externa puceing.edu.ec*

En la red externa puceing.edu.ec OpenVAS determinó las siguientes vulnerabilidades por gravedad como muestra la Figura 2-4 y que se describen en el resumen de análisis por gravedad

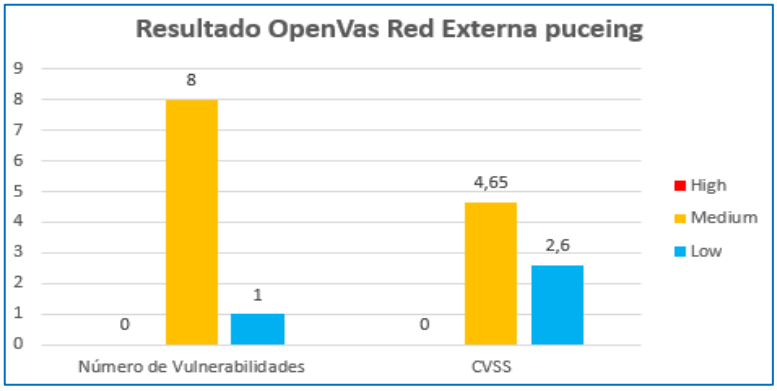

Figura 2-4. Resultado de Vulnerabilidades Puceing, OpenVAS (Salazar Gualoto, 2020)

RESUMEN DE ANÁLISIS POR GRAVEDAD

Vulnerabilidades de Seguridad por Gravedad Medium

CVSS	Origen y Vulnerabilidad
5.8	HTTP Debugging Methods (TRACE/TRACK) Enabled
5.0	WordPress / WordPress MU Multiple Vulnerabilities - July09
5.0	WordPress Multiple Vulnerabilities - July09
4.8	Cleartext Transmission of Sensitive Information via HTTP
4.3	SSL/TLS: Report Weak Cipher Suites
4.3	SSH Weak Encryption Algorithms Supported
4.0	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
4.0	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Tabla 2-11.Resumen Vulnerabilidades Gravedad Medium Puceing, OpenVAS (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Low

CVSS	Origen y Vulnerabilidad
2.6	TCP timestamps

Tabla 2-12. Resumen Vulnerabilidades Gravedad Low Puceing, OpenVAS (Salazar Gualoto, 2020)

2.2.2.2 *Análisis de la Red Interna del LTIC*

El análisis de la red interna del LTIC, OpenVAS obtuvo las siguientes vulnerabilidades por gravedad como se muestra en la Figura 2-5 y que se describen en el resumen de análisis por gravedad.

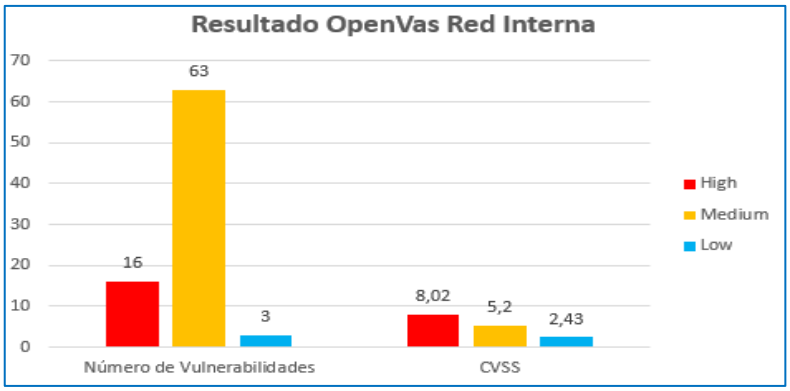

Figura 2-5. Resultado de Vulnerabilidades Red Interna, OpenVAS (Salazar Gualoto, 2020)

RESUMEN DE ANÁLISIS POR GRAVEDAD

Vulnerabilidades de Seguridad por Gravedad High

CVSS	Origen y Vulnerabilidades	Ip
10.0	Check for Discard Service	172.16.0.6, 172.16.0.10
10.0	OpenSSL End of Life Detection (Windows)	172.16.0.7
10.0	PHP End Of Life Detection (Windows)	172.16.0.7
8.5	PHP Multiple Vulnerabilities - Dec18 (Windows)	172.16.0.7
7.8	Apache HTTP Server Multiple Vulnerabilities (Windows)	172.16.0.7
7.5	Oracle MySQL 8.0.x < 8.0.18 Security Update (2019-5072832) – Windows	172.16.0.7
7.5	phpinfo() output Reporting	172.16.0.7
7.5	PHP Multiple Vulnerabilities - Feb19 (Windows)	172.16.0.7
7.5	Apache HTTP Server Denial-Of-Service Vulnerability June17 (Windows)	172.16.0.7
7.5	PHP Integer Overflow Vulnerability Aug18 (Windows)	172.16.0.7
7.5	PHP Multiple Vulnerabilities - Mar19 (Windows)	172.16.0.7
7.5	Oracle MySQL 8.0.x < 8.0.19 Security Update (cpuapr2020) – Windows	172.16.0.7
7.5	Apache HTTP Server Multiple Vulnerabilities June17 (Windows)	172.16.0.7
7.5	PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Windows)	172.16.0.7
7.5	Deprecated SSH-1 Protocol Detection	172.16.0.54
7.1	Oracle MySQL 8.0.x < 8.0.20 Security Update (cpuapr2020) – Windows	172.16.0.7

Tabla 2-13. Resumen Vulnerabilidades por Gravedad High Red Interna, OpenVAS (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Medium

CVSS	Origen y Vulnerabilidades	IP
6.8	Microsoft SQL Server Elevation of Privilege Vulnerability (2984340) – Remote	172.16.0.6
6.8	PHP 'PHP-FPM' Denial of Service Vulnerability (Windows)	172.16.0.7
6.8	Oracle MySQL 8.0.x < 8.0.17 Security Update (2019-5072835) – Windows	172.16.0.7
6.8	XAMPP < 7.2.29, 7.3 < 7.3.16, 7.4 < 7.4.4 Configuration Vulnerability	172.16.0.7
6.8	PHP Multiple Vulnerabilities - Sep19 (Windows)	172.16.0.7

Tabla 2-14. (a) Resumen Vulnerabilidades por Gravedad Medium Red Interna, OpenVAS (Salazar Gualoto, 2020)

CVSS	Origen y Vulnerabilidades	IP
6.8	Apache HTTP Server Multiple Vulnerabilities Apr18 (Windows)	172.16.0.7
6.8	PHP Heap Use-After-Free Vulnerability - Sep19 (Windows)	172.16.0.7
6.5	Oracle MySQL 8.0.x < 8.0.21 Security Update (cpujul2020) – Windows	172.16.0.7
6.4	Apache HTTP Server Memory Access Vulnerability (Windows)	172.16.0.7
6.4	PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Windows)	172.16.0.7
6.4	PHP < 7.2.26 Multiple Vulnerabilities - Dec19 (Windows)	172.16.0.7
6.4	Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Windows)	172.16.0.7
6.0	Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Windows)	172.16.0.7
6.0	Apache HTTP Server Stack Overflow Vulnerability (Windows)	172.16.0.7
5.8	HTTP Debugging Methods (TRACE/TRACK) Enabled	172.16.0.7
5.8	OpenSSL: ChaCha20-Poly1305 with long nonces (CVE-2019-1543) (Windows)	172.16.0.7
5.8	Apache HTTP Server Multiple Vulnerabilities (Windows)	172.16.0.7
5.8	PHP Multiple Vulnerabilities - Aug19 (Windows)	172.16.0.7
5.8	Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Windows)	172.16.0.7
5.8	PHP < 7.2.29 Multiple Vulnerabilities - Mar20 (Windows)	172.16.0.7
5.8	Oracle MySQL 5.3.x < 5.3.14, 8.0.x < 8.0.18 Security Update (2019-5072832) – Windows	172.16.0.7
5.5	Oracle MySQL 5.7.x < 5.7.27, 8.0.x < 8.0.17 Security Update (2019-5072835) – Windows	172.16.0.7
5.5	Oracle MySQL 5.x < 5.6.45, 5.7.x < 5.7.27, 8.0.x < 8.0.17 Security Update (2019-5072835) – Windows	172.16.0.7
5.0	DCE/RPC and MSRPC Services Enumeration Reporting	172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.190
5.0	Check for Quote of the day Service (TCP)	172.16.0.6, 172.16.0.10
5.0	echo Service Reporting (TCP + UDP)	172.16.0.6, 172.16.0.10
5.0	PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Windows)	172.16.0.7
5.0	PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Windows)	172.16.0.7
5.0	PHP < 7.2.32, 7.3 < 7.3.20, 7.4 < 7.4.8 libcurl Vulnerability - May20 (Windows)	172.16.0.7
5.0	SSL/TLS: Untrusted Certificate Authorities	172.16.0.7
5.0	Apache HTTP Server 'mod_http2 null pointer dereference' DoS Vulnerability (Windows)	172.16.0.7
5.0	PHP < 7.2.28 Multiple Vulnerabilities - Feb20 (Windows)	172.16.0.7
5.0	Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Windows)	172.16.0.7
5.0	Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Windows)	172.16.0.7
5.0	Apache HTTP Server < 2.4.39 mod_http2 DoS Vulnerability (Windows)	172.16.0.7
5.0	SSL/TLS: Certificate Expired	172.16.0.7, 172.16.0.42, 172.16.0.43, 172.16.0.44
5.0	PHP < 7.2.31, 7.3 < 7.3.18, 7.4 < 7.4.6 Multiple DoS Vulnerabilities - May20 (Windows)	172.16.0.7
5.0	Apache HTTP Server < 2.4.38 HTTP/2 DoS Vulnerability (Windows)	172.16.0.7
5.0	Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Windows)	172.16.0.7
5.0	PHP Memory Disclosure Vulnerability (Windows)	172.16.0.7
5.0	GoAhead Server HTTP Header Injection Vulnerability	172.16.0.42, 172.16.0.43, 172.16.0.44
4.9	Apache HTTP Server < 2.4.39 mod_http2 DoS Vulnerability (Windows)	172.16.0.7

Tabla 2-15. (b) Resumen Vulnerabilidades por Gravedad Medium Red Interna, OpenVAS (Salazar Gualoto, 2020)

CVSS	Origen y Vulnerabilidades	IP
4.8	Cleartext Transmission of Sensitive Information via HTTP	172.16.0.1, 172.16.0.7, 172.16.0.44, 172.16.0.54
4.8	FTP Unencrypted Cleartext Login	172.16.0.10
4.8	Telnet Unencrypted Cleartext Login	172.16.0.54, 172.16.0.58, 172.16.0.93, 172.16.0.95
4.6	Oracle MySQL 5.7.x < 5.7.28, 8.0.x < 8.0.18 Security Update (2019-5072832) – Windows	172.16.0.7
4.3	SSH Weak Encryption Algorithms Supported	172.16.0.1, 172.16.0.2, 172.16.0.4, 172.16.0.17, 172.16.0.54, 172.16.0.58, 172.16.0.93, 172.16.0.95, 172.16.0.176
4.3	SSL/TLS: Report Weak Cipher Suites	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.54, 172.16.1.52
4.3	OpenSSL: Timing vulnerability in ECDSA signature generation (CVE-2018-0735) (Windows)	172.16.0.7
4.3	Apache HTTP Server Denial of Service Vulnerability Apr18 (Windows)	172.16.0.7
4.3	OpenSSL: Timing vulnerability in DSA signature generation (CVE-2018-0734) (Windows)	172.16.0.7
4.3	OpenSSL 1.0.2, 1.1.0, 1.1.1 Multiple Vulnerabilities – Windows	172.16.0.7
4.3	Apache HTTPD HTTP/2 'SETTINGS' Data Processing DoS Vulnerability (Windows)	172.16.0.7
4.3	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	172.16.0.54, 172.16.1.52
4.3	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	172.16.0.54, 172.16.1.52
4.0	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.1.52
4.0	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	172.16.0.1, 172.16.0.7, 172.16.0.43, 172.16.0.44, 172.16.1.52
4.0	Oracle MySQL 8.0.x < 8.0.20 Security Update (cpujul2020) – Windows	172.16.0.7
4.0	Oracle MySQL 5.7.x < 5.7.27, 8.0.x < 8.0.17 Security Update (2019-5072832) – Windows	172.16.0.7
4.0	Oracle MySQL 8.0.x < 8.0.17 Security Update (2019-5072832) – Windows	172.16.0.7
4.0	Oracle MySQL 8.0.x < 8.0.19 Security Update (cpujan2020) – Windows	172.16.0.7
4.0	Oracle MySQL 8.0.x < 8.0.18 Security Update (cpujan2020) – Windows	172.16.0.7
4.0	Oracle MySQL 5.6.0 < 5.6.46, 5.7.x < 5.7.28, 8.0.x < 8.0.18 Security Update (2019-5072832) – Windows	172.16.0.7

Tabla 2-16. (c) Resumen Vulnerabilidades por Gravedad Medium Red Interna, OpenVAS (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Low

CVSS	Origen y Vulnerabilidades	IP
2.6	TCP timestamps	172.16.0.1, 172.16.0.2, 172.16.0.4, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.17, 172.16.0.176
2.6	SSH Weak MAC Algorithms Supported	172.16.0.54, 172.16.0.58, 172.16.0.93, 172.16.0.95
2.1	Oracle MySQL 5.6.x < 5.6.45, 5.7.x < 5.7.27, 8.0.x < 8.0.17 Security Update (2019-5072832) – Windows	172.16.0.7

Tabla 2-17.Resumen Vulnerabilidades por Gravedad Low Red Interna, OpenVAS (Salazar Gualoto, 2020)

2.2.3 ANÁLISIS CON LEGION

El escaneo de la red del LTIC mediante el uso del software libre Legion sobre kali linux obtuvo los siguientes resultados.

2.2.3.1 *Análisis de la Red Externa puceing.edu.ec*

En la red externa puceing.edu.ec Legion determinó los siguientes resultados por gravedad como se muestra en la Figura 2-6 y que se describen en el resumen de análisis por gravedad.

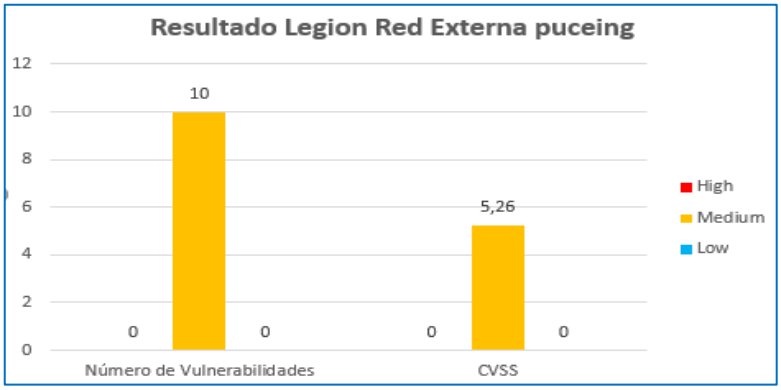

Figura 2-6. Resultado de Vulnerabilidades Puceing, Legion (Salazar Gualoto, 2020)

RESUMEN DE ANÁLISIS POR GRAVEDAD

Vulnerabilidades de Seguridad por Gravedad Medium

CVSS	Vulnerabilidad	Producto	Versión
5.0	CVE-2018-15919	openssh	7.4
5.0	CVE-2017-15906	openssh	7.4
4.3	CVE-2020-14145	openssh	7.4
6.4	CVE-2019-10082	http_server	2.4.39
6.0	CVE-2019-10097	http_server	2.4.39
5.8	CVE-2020-1927	http_server	2.4.39
5.8	CVE-2019-10098	http_server	2.4.39
5.0	CVE-2020-1934	http_server	2.4.39
5.0	CVE-2019-10081	http_server	2.4.39
4.3	CVE-2019-10092	http_server	2.4.39

Tabla 2-18. Resumen Vulnerabilidades por Gravedad Medium Puceing, Legion (Salazar Gualoto, 2020)

2.2.3.2 *Análisis de la Red Interna del LTIC*

El análisis de la red interna del LTIC, Legion obtuvo las siguientes vulnerabilidades por gravedad como se muestra en la Figura 2-7 y que se describen en el resumen de análisis por gravedad.

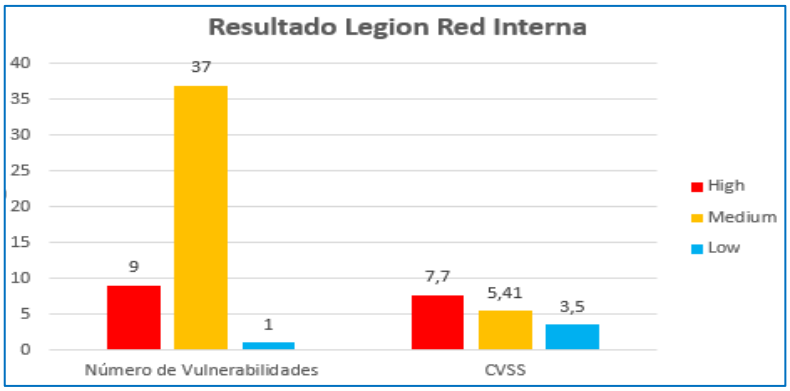

Figura 2-7. Resultado de Vulnerabilidades Red Interna, Legion (Salazar Gualoto, 2020)

Resumen de Análisis por Gravedad

Vulnerabilidades de Seguridad por Gravedad High

CVSS	Vulnerabilidad	Producto	Versión	IP
8.5	CVE-2015-1763	sql_server	2014	172.16.0.6
7.1	CVE-2015-1762	sql_server	2014	172.16.0.6
7.2	CVE-2019-0211	http_server	2.4.34	172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
9.0	CVE-2019-9193	postgresql	96	172.16.0.7
7.5	CVE-2017-7546	postgresql	96	172.16.0.7
7.5	CVE-2017-3169	http_server	2.4.25	172.16.0.7
7.5	CVE-2017-7668	http_server	2.4.25	172.16.0.7
7.5	CVE-2017-3167	http_server	2.4.25	172.16.0.7
7.5	CVE-2017-7679	http_server	2.4.25	172.16.0.7

Tabla 2-19. Resumen Vulnerabilidades por Gravedad High Red Interna, Legion (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Medium

CVSS	Vulnerabilidad	Producto	Versión	IP
6.4	CVE-2019-10082	http_server	2.4.39	172.16.0.1, 172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.12, 172.16.0.12, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
6.0	CVE-2019-10097	http_server	2.4.39	172.16.0.1, 172.16.0.7, 172.16.0.7, 172.16.0.12, 172.16.0.12, 172.16.0.18, 172.16.0.18
5.8	CVE-2019-10098	http_server	2.4.39	172.16.0.1, 172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.12, 172.16.0.12, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
5.8	CVE-2020-1927	http_ server	2.4.39	172.16.0.1, 172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.12, 172.16.0.12, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
5.0	CVE-2019-10081	http_server	2.4.39	172.16.0.1, 172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.12, 172.16.0.12, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
5.0	CVE-2020-1934	http_server	2.4.39	172.16.0.1, 172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.12, 172.16.0.12, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
5.0	CVE-2017-15906	openssh	7.4	172.16.0.1, 172.16.0.2, 172.16.0.4, 172.16.0.17, 172.16.1.76
5.0	CVE-2018-15919	openssh	7.4	172.16.0.1, 172.16.0.2, 172.16.0.4, 172.16.0.17, 172.16.1.76
4.3	CVE-2019-10092	http_server	2.4.39	172.16.0.1, 172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.12, 172.16.0.12, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
4.3	CVE-2020-14145	openssh	7.4	172.16.0.1, 172.16.0.2, 172.16.0.4, 172.16.0.17, 172.16.1.76
6.5	CVE-2016-7250	sql_server	2014	172.16.0.6
6.5	CVE-2015- 1761	sql_server	2014	172.16.0.6

Tabla 2-20. (a) Resumen Vulnerabilidades por Gravedad Medium Red Interna, Legion (Salazar Gualoto, 2020)

CVSS	Vulnerabilidad	Producto	Versión	IP
6.5	CVE-2019-1068	sql_server	2014	172.16.0.6
6.5	CVE-2016-7253	sql_server	2014	172.16.0.6
6.5	CVE-2020-0618	sql_server	2014	172.16.0.6
5.0	CVE-2017-8516	sql_server	2014	172.16.0.6
4.3	CVE-2014-1820	sql_server	2014	172.16.0.6
6.0	CVE-2019-0217	http_server	2.4.34	172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
5.0	CVE-2018-17199	http_server	2.4.34	172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
5.0	CVE-2019-0220	http_server	2.4.34	172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
5.0	CVE-2019-0196	http_server	2.4.34	172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
4.9	CVE-2019-0197	http_server	2.4.34	172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
4.3	CVE-2018-11763	http_server	2.4.34	172.16.0.7, 172.16.0.7, 172.16.0.7, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
6.5	CVE-2018-1058	postgresql	96	172.16.0.7
6.4	CVE-2018-1115	postgresql	96	172.16.0.7
5.0	CVE-2017-7486	postgresql	96	172.16.0.7
4.0	CVE-2017-7547	postgresql	96	172.16.0.7
4.0	CVE-2017-7548	postgresql	96	172.16.0.7
6.8	CVE-2017-15715	http_server	2.4.25	172.16.0.7, 172.16.0.21, 172.16.0.92, 172.16.0.92
6.8	CVE-2018-1312	http_server	2.4.25	172.16.0.7, 172.16.0.21, 172.16.0.92, 172.16.0.92
6.4	CVE-2017-9788	http_server	2.4.25	172.16.0.7, 172.16.0.92, 172.16.0.92
5.0	CVE-2018-1333	http_server	2.4.25	172.16.0.7, 172.16.0.18, 172.16.0.18, 172.16.0.21, 172.16.0.92, 172.16.0.92
5.0	CVE-2017-15710	http_server	2.4.25	172.16.0.7, 172.16.0.21, 172.16.0.92, 172.16.0.92
5.0	CVE-2017-9798	http_server	2.4.25	172.16.0.7, 172.16.0.92, 172.16.0.92
5.0	CVE-2017-7659	http_server	2.4.25	172.16.0.7
5.0	CVE-2018-8011	http_server	2.4.33	172.16.0.18, 172.16.0.18
5.0	CVE-2017-9789	http_server	2.4.26	172.16.0.92, 172.16.0.92

Tabla 2-21. (b) Resumen Vulnerabilidades por Gravedad Medium Red Interna, Legion (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Low

CVSS	Vulnerabilidad	Producto	Versión	IP
3.5	CVE-2018-1283	http_server	2.4.25	172.16.0.7, 172.16.0.21, 172.16.0.92, 172.16.0.92

Tabla 2-22. Resumen Vulnerabilidades por Gravedad Low Red Interna, Legion (Salazar Gualoto, 2020)

2.2.4 ANÁLISIS CON GFI LANDGUARD

El escaneo de la red del LTIC mediante el uso del software GFI LandGuard obtuvo los siguientes resultados.

2.2.4.1 *Análisis de la Red Interna del LTIC*

El análisis de la red interna del LTIC, GFI LandGuard obtuvo las siguientes vulnerabilidades por gravedad como muestra en la Figura 2-8 y que se describen en el resumen de análisis por gravedad.

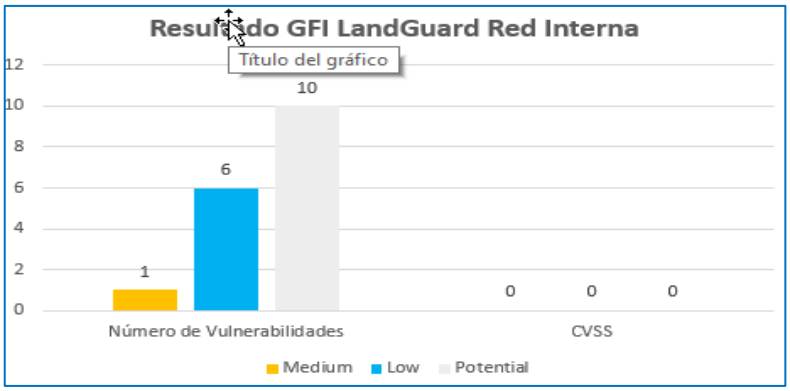

Figura 2-8. Resultado de Vulnerabilidades Red Interna, GFI LandGuard (Salazar Gualoto, 2020)

RESUMEN DE ANÁLISIS POR GRAVEDAD

Vulnerabilidades de Seguridad por Gravedad Medium

CVSS	Origen y Vulnerabilidad	IP
-	SSH server accepts Version 1.x connections	172.16.0.54

Tabla 2-23. Resumen Vulnerabilidades por Gravedad Medium Red Interna, GFI LandGuard (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Low

CVSS	Origen y Vulnerabilidad	IP
-	Service running: DNS	172.16.0.1
-	Service running: HTTP	172.16.0.1, 172.16.0.20, 172.16.0.21, 172.16.0.54, 172.16.0.93, 172.16.0.92, 172.16.0.2, 172.16.0.19
-	Service running: HTTPS	172.16.0.1, 172.16.0.54, 172.16.0.92, 172.16.0.19
-	Service running: MySQL	172.16.0.1
-	Service running: SSH	172.16.0.17, 172.16.0.20, 172.16.0.4, 172.16.0.54, 172.16.0.93, 172.16.0.2
-	Service running: Telnet	172.16.0.54, 172.16.0.93

Tabla 2-24. Resumen Vulnerabilidades por Gravedad Low Red Interna, GFI LandGuard (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Potential

CVSS	Origen y Vulnerabilidad	IP
-	Open port commonly used by Trojans: TCP 81	172.16.0.1, 172.16.0.20
-	Open port commonly used by Trojans: TCP 2002	172.16.0.1
-	Open port commonly used by Trojans: TCP 2004	172.16.0.1
-	Open port commonly used by Trojans: TCP 2005	172.16.0.1
-	PHP module running (web server)	172.16.0.92
-	PHP is installed on this web server.	172.16.0.92
-	SSL enabled (web server)	172.16.0.92
-	Open port commonly used by Trojans: TCP 2080	172.16.0.8
-	Open port commonly used by Trojans: TCP 1005	172.16.0.10
-	Open port commonly used by Trojans: TCP 1008	172.16.0.10

Tabla 2-25. Resumen Vulnerabilidades por Gravedad Potential Red Interna, GFI LandGuard (Salazar Gualoto, 2020)

2.2.5 RESUMEN GENERAL DE VULNERABILIDADES

Al procesar los resultados del escaneo de las vulnerabilidades con Nessus profesional, OpenVAS, Legion y GFI LandGuard se determinó lo siguiente:

2.2.5.1 *Red Externa puceing.edu.ec*

En la red externa según la Figura 2-9 se encontró que; Nessus profesional determinó 12 vulnerabilidades con un promedio de CVSS de 5.75, Legion encontró 10 vulnerabilidades con un promedio de CVSS de 5.26 y OpenVAS encontró 9 vulnerabilidades con un promedio de CVSS de 4.42.

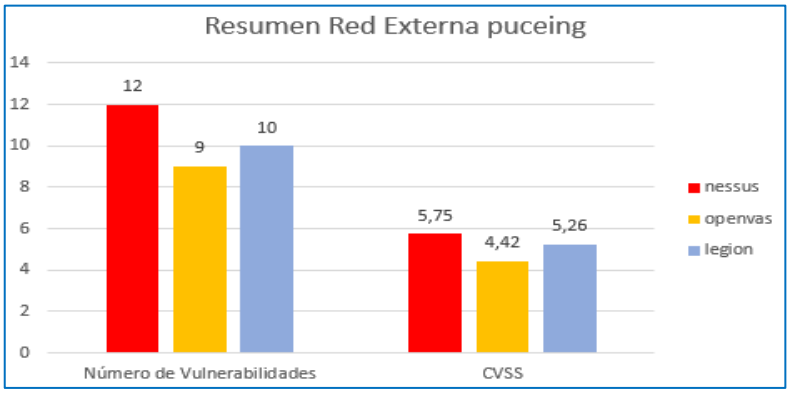

Figura 2-9. Resumen Final de Vulnerabilidades Red Externa LTIC (Salazar Gualoto, 2020)

2.2.5.2 *Red Interna del LTIC*

En la red interna del LTIC de acuerdo a la Figura 2-10 se encontró que; OpenVAS determinó 82 vulnerabilidades con un promedio de CVSS de 5.65, Nessus Profesional encontró 80 vulnerabilidades con un promedio de CVSS de 5.47, Legion encontró 47 vulnerabilidades con un promedio de CVSS de 5.81 y GFI LandGuard encontró 17 vulnerabilidades sin un valor promedio de CVSS.

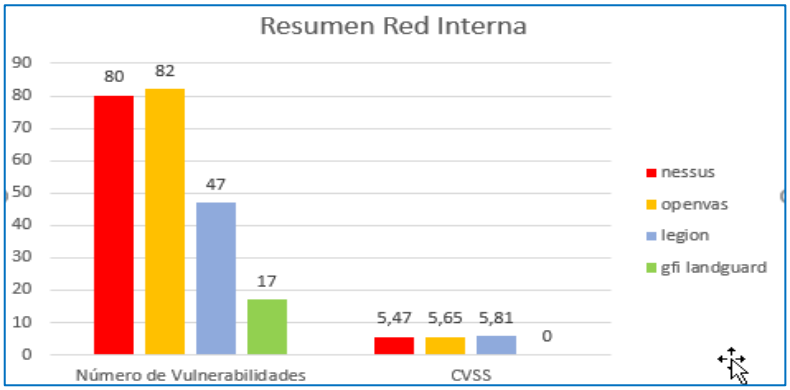

Figura 2-10. Resumen Final de Vulnerabilidades Red Interna LTIC (Salazar Gualoto, 2020)

2.2.6 INTELIGENCIA DE AMENAZAS

En el sitio web ZONE-H lugar donde se registra los ataques informáticos, se encontró que la red externa del LTIC (puceing.edu.ec) fue atacada. Se registró que el servidor web apache fue víctima y se creó una página espejo donde consta el nombre del hacker Hmei7 que realizo el ataque tal como se muestra en la Figura 2-11. En caso de requerir mayor información puede realizar la consulta y obtener a mayor detalle dicho registro en el link http://www.zone-h.org/.

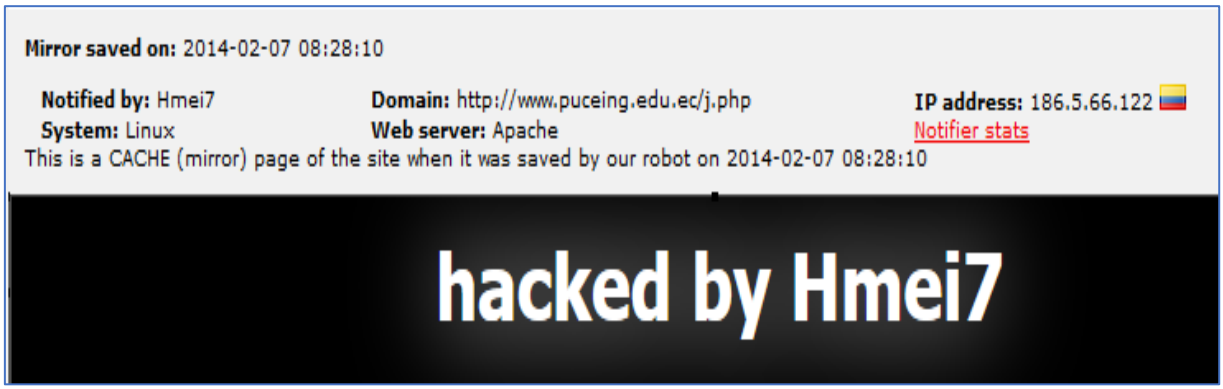

Figura 2-11. Ataque a la red externa del LTIC por Hacker Hmei7 (http://www.zone-h.org/)

Revisada la literatura de cada una de las vulnerabilidades encontradas en el punto anterior mediante el escaneo con Nessus Profesional, OpenVas, Legion y GFI LandGuard, se determinó que la red del LTIC se encuentra expuesta a las siguientes amenazas como se muestra en la Tabla 2-26.

Amenaza (Ataque)	IP
Ataques de Colisión	172.16.0.6, 172.16.0.8, 172.16.0.18, 172.16.0.43, 172.16.0.54, 172.16.0.92
Attacking SSL when using RC4	172.16.0.1, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.12, 172.16.0.54
Clickjacking	puceing.edu.ec
DDoS	172.16.0.58, 172.16.0.93, 172.16.0.95
Desbordamiento de búfer	172.16.0.7, 172.16.0.18, 172.16.0.92, 172.16.0.93
Desbordamiento de procedimiento	172.16.0.18
DoS	puceing.edu.ec, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.18, 172.16.0.58, 172.16.0.92, 172.16.1.52
Ejecución remota de código	172.16.0.6
Etherleak	172.16.0.58, 172.16.0.93, 172.16.0.95
Inyección de código malicioso	puceing.edu.ec, 172.16.0.7, 172.16.0.18, 172.16.0.92
Inyección de comandos	172.16.0.92
Lectura de buffer	puceing.edu.ec
Man-In-The-Middle (MiTM)	puceing.edu.ec, 172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.12, 172.16.0.18, 172.16.0.41, 172.16.0.42, 172.16.0.43, 172.16.0.44, 172.16.0.54, 172.16.0.92, 172.16.0.190
Sobre lectura de buffer	puceing.edu.ec, 172.16.0.7, 172.16.0.18, 172.16.0.92

Tabla 2-26. Resumen de Amenazas (Ataques) de la Red del LTIC

Conjuntamente a la inteligencia de amenazas se identificó que en el servidor 172.16.0.12 la aplicación phpMyAdmin no se encuentra protegida por autentificación de usuario y contraseña, esto permite tener acceso a la base de datos del portal web del III Congreso Internacional de Sistemas Inteligentes y Nuevas Tecnologías como se muestra en la Figura 2-12 en donde se puede observar los datos de la tabla wp_cf7_vdata_entry que registra los usuarios a participar en el congreso.

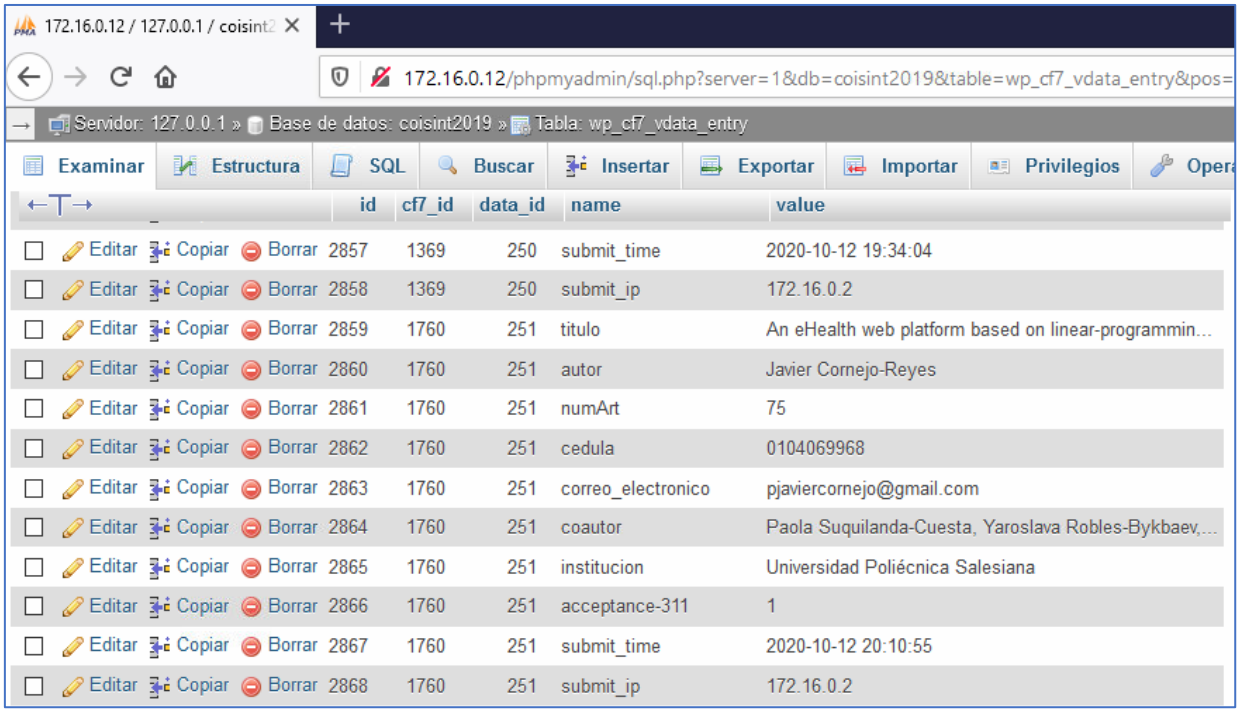

Figura 2-12. Datos de la tabla wp_cf7_vdata_entry de PhpMyAdmin sin protección de usuario u contraseña. (Salazar Gualoto, 2020).

2.2.7 RESUMEN DE PUERTOS ABIERTOS

Mediante el escaneo de la red se evidencio que la red del LTIC tiene abiertos los puertos que se describen a continuación.

2.2.7.1 *Puertos Abiertos Red Externa*

En la red externa del LTIC se encontró los siguientes puertos abiertos según la Tabla 2-27 y Tabla 2-28.

Puerto	Protocolo	IP
24	Tcp	puceing.edu.ec
53	Tcp	puceing.edu.ec
80	Tcp	puceing.edu.ec
81	Tcp	puceing.edu.ec
443	Tcp	puceing.edu.ec
2000	Tcp	puceing.edu.ec

Tabla 2-27. (a) Puertos Abiertos de la Red Externa. (Salazar Gualoto, 2020)

Puerto	Protocolo	IP
2001	Tcp	puceing.edu.ec
2002	Tcp	puceing.edu.ec
2003	Tcp	puceing.edu.ec
2004	Tcp	puceing.edu.ec
2005	Tcp	puceing.edu.ec
3306	Tcp	puceing.edu.ec
8001	Tcp	puceing.edu.ec
9001	Tcp	puceing.edu.ec
11000	Tcp	puceing.edu.ec
15000	Tcp	puceing.edu.ec

Tabla 2-28. (b) Puertos Abiertos de la Red Externa. (Salazar Gualoto, 2020)

2.2.7.2 *Puertos Abierto Red Interna*

En la red interna del LTIC se encontró los siguientes puertos abiertos según la Tabla 2-29, Tabla 2-30 y Tabla 2-31.

Puerto	Protocolo	IP
7	Tcp	172.16.0.6, 172.16.0.10
9	Tcp	172.16.0.6, 172.16.0.10
13	Tcp	172.16.0.6, 172.16.0.10
17	Tcp	172.16.0.6, 172.16.0.10
19	Tcp	172.16.0.6, 172.16.0.10
21	Tcp	172.16.0.10
22	Tcp	172.16.0.2, 172.16.0.4, 172.16.0.17, 172.16.0.20, 172.16.0.54, 172.16.0.58, 171.16.0.93, 172.16.0.95, 172.16.1.52, 172.16.1.76
23	Tcp	172.16.0.54, 172.16.0.58, 171.16.0.93, 172.16.0.95
24	Tcp	172.16.0.1
42	Tcp	172.16.0.5
53	Tcp	172.16.0.1, 172.16.0.5
67	Udp	172.16.0.19
68	Udp	172.16.0.58, 171.16.0.93, 172.16.0.95
80	Tcp	172.16.0.1, 172.16.0.2, 172.16.0.6, 172.16.0.7, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.19, 172.16.0.20, 172.16.0.21, 172.16.0.41, 172.16.0.42, 172.16.0.43, 172.16.0.44, 172.16.0.54, 172.16.0.58, 172.16.1.92, 172.16.0.95, 172.16.0.190, 172.16.1.52, 172.16.1.76
81	Tcp	172.16.0.1, 172.16.0.20
88	Tcp	172.16.0.5
135	Tcp	172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.1.92, 172.16.0.190
137	Udp	172.16.0.19
139	Tcp	172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.190
161	Udp	172.16.0.19, 171.16.0.93
162	Udp	172.16.0.95
389	Tcp	172.16.0.5

Tabla 2-29. (a) Puertos Abiertos en la Red Interna. (Salazar Gualoto, 2020)

Puerto	Protocolo	IP
427	Tcp/Udp	172.16.0.19
443	Tcp	172.16.0.1, 172.16.0.7, 172.16.0.12, 172.16.0.18, 172.16.0.19, 172.16.0.41, 172.16.0.42, 172.16.0.43, 172.16.0.44, 172.16.0.54, 172.16.1.92, 172.16.0.190, 172.16.1.52
445	Tcp	172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18
464	Tcp	172.16.0.5
515	Tcp	172.16.0.19
546	Udp	172.16.0.19
593	Tcp	172.16.0.5
631	Tcp	172.16.0.19
636	Tcp	172.16.0.5
1005	Tcp	172.16.0.10
1008	Tcp	172.16.0.10
1024	Udp	172.16.0.58, 171.16.0.93, 172.16.0.95
1433	Tcp	172.16.0.6, 172.16.0.10, 172.16.1.92
1488	Tcp	172.16.0.6
1645	Udp	172.16.0.58, 171.16.0.93, 172.16.0.95
1646	Udp	172.16.0.58, 171.16.0.93, 172.16.0.95
1688	Tcp	172.16.0.8, 172.16.0.18
1801	Tcp	172.16.0.10
1812	Udp	172.16.0.58, 171.16.0.93, 172.16.0.95
1900	Udp	172.16.0.19
2000	Tcp	172.16.0.1
2001	Tcp	172.16.0.1
2002	Tcp	172.16.0.1
2003	Tcp	172.16.0.1
2004	Tcp	172.16.0.1
2005	Tcp	172.16.0.1
2080	Tcp	172.16.0.8
2103	Tcp	172.16.0.6, 172.16.0.10
2105	Tcp	172.16.0.6, 172.16.0.10
2107	Tcp	172.16.0.6, 172.16.0.10
2383	Tcp	172.16.0.6
3205	Tcp	172.16.0.6, 172.16.0.10
3268	Tcp	172.16.0.5
3269	Tcp	172.16.0.5
3306	Tcp	172.16.0.1, 172.16.0.7, 172.16.0.12, 172.16.0.18
3389	Tcp	172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.1.92, 172.16.0.190
3580	Tcp	172.16.0.8
3702	Udp	172.16.0.19
4080	Tcp	172.16.0.8
4443	Tcp	172.16.0.8
5001	Udp	172.16.0.58, 171.16.0.93, 172.16.0.95

Tabla 2-30. (b) Puertos Abiertos en la Red Interna. (Salazar Gualoto, 2020)

Puerto	Protocolo	IP
5200	Tcp	172.16.0.19
5353	Udp	172.16.0.19
5432	Tcp	172.16.0.7, 172.16.0.10
5800	Tcp	172.16.1.92
5900	Tcp	172.16.1.92
6000	Udp	172.16.0.19
6443	Tcp	172.16.0.8
7000	Udp	172.16.0.19
8001	Tcp	172.16.0.1
8018	Tcp	172.16.0.19
9100	Tcp	172.16.0.19
10000	Tcp	172.16.0.7
10200	Udp	172.16.0.19
10201	Udp	172.16.0.19
11801	Tcp	172.16.0.6
17990	Tcp	172.16.1.52
27000	Tcp	172.16.0.6, 172.16.0.8
27009	Tcp	172.16.0.5
58499	Udp	172.16.0.19

Tabla 2-31. (c) Puertos Abiertos en la Red Interna. (Salazar Gualoto, 2020)

CAPÍTULO III

3. DISEÑO DEL SISTEMA DE SEGURIDAD PERIMETRAL

Esta sección cubre el diseño del sistema de seguridad perimetral informático, requerimientos de seguridad del LTIC, selección de tecnología de seguridad perimetral, análisis comparativo de tecnología de seguridad perimetral firewall de nueva generación, esquema del sistema de seguridad perimetral propuesto para el LTIC.

3.1. REQUERIMIENTOS DE SEGURIDAD DEL LTIC

En el capítulo II luego revisar la situación actual de seguridad del LTIC se encontró varias deficiencias en la red del LTIC entre las principales deficiencias están las siguientes:

- ✓ El servicio phpMyAdmin que administra la base de datos del portal web del III Congreso se encuentra configurado sin autentificación por usuario y contraseña, esto permite acceder a la información de esta base de datos de cualquier parte de la red.
- ✓ Existe puertos TCP y UDP abiertos sin ser utilizados, los mismos pueden ser usados comúnmente por troyanos.
- ✓ Servicios levantados innecesariamente como DNS, HTTP, HTTPS, SSH, MySQL.
- ✓ Equipos de cómputo fuera del dominio sistemas.local
- ✓ Servidores y equipos de cómputo que cuentan con versiones desactualizadas de aplicaciones, encriptación y servicios.

Adicional de estas deficiencias se detectó que no se realiza un análisis de logs, no se cuenta con aplicaciones para gestión y monitoreo de equipos de cómputo, que los servicios de DHCP, DNS, Directorio Activo, servicio de licenciamiento y antivirus no cuentan con un respaldo es decir que si uno de estos servicios sufre una avería estaría no disponible para la red del LTIC.

Las deficiencias expuestas anteriormente en la red del LTIC, permiten ejecutar potenciales amenazas (ataques) a la infraestructura, aplicaciones web, red y sistema de seguridad. A esto le agregamos el promedio de CVSS que nos determina un vector de ataque superior a 5.00. Por tanto, esto evidencia la necesidad de un sistema de seguridad perimetral.

Los requerimientos para un de sistema de seguridad perimetral informático en el LTIC se enmarcan en los siguientes factores:

- ✓ Una variedad de amenazas (ataques) pueden afectar a los portales web de facultad, de Anuros, III Congreso y demás aplicativos webs. El sistema de seguridad del LTIC conformado por un UTM Untangle no permite una visibilidad integral, seguridad avanzada y protección contra amenazas ya que el UTM solo nos muestra un dashboard sobre el estado de la red.

- ✓ El control del acceso al internet de los estudiantes, docentes y otros usuarios cuenta con proxy y proxy reverso para realizar dicho control, esto menora los tiempos de respuesta por el tráfico y la saturación de los servicios.

- ✓ La protección de la información contenida en las bases de datos, como el caso del portal web del III Congreso donde los datos se encuentran expuestos por lo que es indispensable controlar la manipulación o fuga de información debido que no se cuenta con una política de seguridad.

- ✓ Es necesario también prever para futuras aplicaciones web los ataques de DDoS, DoS, Clickjacking, MitM y otros para evitar pérdidas de información y entregar una disponibilidad considerable a los usuarios.

3.2. SELECCIÓN DE TECNOLOGÍA DE SEGURIDAD PERIMETRAL

Establecidos los requerimientos en el punto anterior es posible sintetizar la necesidad de un sistema de seguridad perimetral informático dimensionado con una tecnología especialista en protección perimetral que permita al LTIC tener una defensa en profundidad, asegurar la red y mitigar las amenazas.

Las características de esta tecnología deben permitir la protección de la red centrados en la inspección de todo el tráfico incluyendo aplicaciones, amenazas, visión de la red desde la frontera y control de contenido. Considerando lo expresado la tecnología que sustenta las necesidades del LTIC es el Firewall de Nueva Generación el cual brinda los siguientes beneficios según (Cortes, 2020, pág. 5):

- ✓ Habilitación de forma segura, a aplicaciones, usuarios y contenidos mediante la clasificación de todo el tráfico, la determinación del caso de uso empresarial y la asignación de políticas con el fin de permitir y proteger el acceso a las aplicaciones pertinentes.
- ✓ Mitigación de amenazas eliminando aplicaciones no deseadas para reducir la superficie de impacto y aplicación de políticas de seguridad selectivas para bloquear exploits de vulnerabilidades, virus, spyware, botnets y malware desconocido (APT).

- ✓ Protección para los centros de datos por medio de la validación de aplicaciones, el aislamiento de datos, el control sobre las aplicaciones no apropiadas y la prevención de amenazas de alta velocidad.
- ✓ Protección a los entornos de computación en la nube pública y privada con una mayor visibilidad y control; implementación, aplicación y manutención de políticas de seguridad al mismo ritmo que sus máquinas virtuales.
- ✓ Adopción de una informática móvil segura extendiendo la plataforma de seguridad empresarial a los usuarios y dispositivos independientemente de su ubicación.

3.3. ANÁLISIS COMPARATIVO DE TECNOLOGÍA DE SEGURIDAD PERIMETRAL FIREWALL DE NUEVA GENERACIÓN

La estrategia para la evaluación de la tecnología de seguridad perimetral firewall de nueva generación se basa en usar el Cuadrante Mágico para Firewalls de Red según la empresa (GARTNER, 2020) que analiza las capacidades de los proveedores de firewall dividiéndole en cuatro grandes cuadrantes como se muestra en la Figura 3-1:

Figura 3-1. Cuadrante Mágico de Firewall de Red (GARTNER) noviembre 2019

Cuadrante Lideres conformado por los proveedores que crean productos que cumplen con los requisitos empresariales, poseen una gran cuota de mercado, lideran la innovación y ofrecen nuevas funciones para protección de sus clientes ante amenazas emergentes. (GARTNER, 2020).

Cuadrante Challengers conformado por proveedores que ha logrado una sólida base de clientes, que no lideran pero que tienen capacidades diferenciadas de próxima generación o que se limitan a colocar productos de seguridad con prioridades bajas. (GARTNER, 2020).

Cuadrante Visionarios conformado por proveedores que lideran la innovación, pero se limitan a uno o dos casos de implementación de firewall, carecen de una base de ventas o medios financieros para competir. (GARTNER, 2020).

Cuadrante Jugadores de Nicho conformado por proveedores que tiene su base de instalación principal o son prominentes en un caso de uso en particular. Usan una base limitada de clientes y muestran poca innovación. (GARTNER, 2020).

De la investigación realizada por Gartner, en este estudio se ha considerado los siguientes proveedores (GARTNER, 2020):

Check Point un proveedor de seguridad global puro que ofrece un modelo de precios simples con dispositivos que vienen en opciones de paquetes de suscripciones y fuente de inteligencia de amenazas. (GARTNER, 2020).

Cisco un gran proveedor de redes, infraestructura y seguridad ofrece una amplia cartera de soluciones, inteligencia e investigación de amenazas, funciones avanzadas de protección contra malware e integración de IDPS. (GARTNER, 2020).

Fortinet es un proveedor de red y seguridad, cuyo producto FortiGate es muy popular y considerado el más vendido, posee soporte TLS 1.3. (GARTNER, 2020).

Gartner en revisión y comparación de los productos de los tres proveedores de firewall de red, Check Point con sus productos Next Generation Firewall, CloudGuard IaaS, Check Point SandBlast Network, Cisco con sus productos Cisco ASA, Cisco Meraki MX appliances, Cisco Firepower y Fortinet con sus productos FortiGate: Next Generation Firewall (NGFW) según la Tabla 3-1 (Gartner, 2020) destaca lo siguiente:

- ✓ En la clasificación general por pares los productos de Fortinet reciben 4,7 estrellas en correlación con 4,5 estrellas de Check Point y 4,3 estrellas de Cisco. Al igual que la voluntad de recomendar los productos de Fortinet con un 95%, seguido de Check Point de 86% y Cisco con un 73%.
- ✓ En las capacidades del producto Fortinet recibe una puntuación de capacidad general de 4,8 y Check Point y Cisco 4,6.
- ✓ En la experiencia del cliente, se tiene diversas puntaciones como evaluación y contratación donde Fortinet recibe 4,6, Check Point 4,5 y Cisco 4,4; puntación de flexibilidad de precios Fortinet 4,6, Cisco 4,3 y Check Point 4,1; puntuación de integración e implementación Fortinet 4,7, Check Point 4,5 y Cisco 4,3; puntuación de facilidad de implementación Fortinet 4,7, Cisco y Check Point 4,2; puntuación de servicio de ayuda Fortinet 4,5, Cisco 4,4 y Check Point 4.3; puntuación de oportunidad de la respuesta del proveedor Fortinet 4,7, Cisco y Check Point 4,4; y la puntuación de calidad de soporte técnico Fortinet 4,6, Cisco 4,4 y Check Point 4,3.

Evaluación de proveedor	**Check Point**	**Cisco**	**Fortinet**
Calificación general por pares	**4.5 (333 reseñas)**	**4.3 (15 evaluaciones)**	**4.7 (158 evaluaciones)**
Distribución de calificaciones	5 estrellas 59%	5 estrellas 47%	5 estrellas73%
	4 estrellas 36%	4 estrellas 40%	4 estrellas 22%
	3 estrellas 5%	3 estrellas 13%	3 estrellas 3%
	2 estrellas 0%	2 estrellas 0%	2 estrellas 1%
	1 estrella 1%	1 estrella 0%	1 estrella 1%
Voluntad de recomendar	86% Sí	73% Sí	95% Sí
¿Capacidades del producto			
Puntuación de capacidad general	**4,6** (333)	**4,6** (15)	**4,8** (158)
Experiencia del cliente			
Evaluación y contratación	**4,5** (333)	**4,4** (15)	**4,5** (158)
Flexibilidad de precios	**4,1** (231)	**4,3** (12)	**4,6** (130)
Integración e implementación	**4,5** (333)	**4,3** (15)	**4,7** (158)
Facilidad de implementación	**4,2** (249)	**4,2** (12)	**4,7** (135)
Servicio de ayuda	**4,3** (333)	**4,4** (15)	**4,5** (158)
Oportunidad de la respuesta del proveedor	**4,4** (252)	**4,4** (12)	**4,7** (133)
Calidad del soporte técnico	**4,3** (252)	**4,74**(12)	**4,6** (134)

Tabla 3-1. Comparación de productos de Check Point, Cisco y Fortinet (Gartner, 2020)

De acuerdo al análisis realizado por la empresa Gartner los proveedores Fortinet y Check Point pertenecen al cuadrante de líderes y el proveedor Cisco pertenece al cuadrante challengers. Estos proveedores presentan los mejores equipos de firewall de nueva generación para cumplir con los requerimientos del LTIC, para este estudio se escogió los NGFW para empresas medianas y se realiza el análisis de las especificaciones de estos equipos.

El Proveedor Check Point con el equipo Check Point Quantum 6600 Plus un firewall de nueva generación, de acuerdo a su datasheet (CHECK POINT, 2020), permite a las empresas implementar capacidades de prevención de amenazas en todos los puntos de su infraestructura, escalando la seguridad de acuerdo con las necesidades comerciales cambiantes, acelera la eficiencia de operaciones de seguridad para prevenir y bloquear incluso los ataques más avanzados antes que puedan interrumpir las actividades de la empresa y este modelo se muestra en la Figura 3-2.

Figura 3-2. NGFW Check Point Quantum 6600 Plus datasheet (CHECK POINT, 2020)

El Proveedor Cisco con el equipo Cisco Firepower 2130 un firewall de nueva generación, de acuerdo a su datasheet (CISCO, 2020), pertenece a la familia de cuatro plataformas de seguridad NGFW que se centran en brindar resistencia empresarial de las amenazas a través de una defensa superior, con una innovadora arquitectura de CPU dual multinúcleo para optimizar funciones de firewall, criptográfico, inspección de amenazas, posee estándar de construcción de equipos de red (NEBS). Esta plataforma pude ejecutar Cisco ASA Firewall o Cisco Firepower Threat Defense y su modelo se muestra en la Figura 3-3.

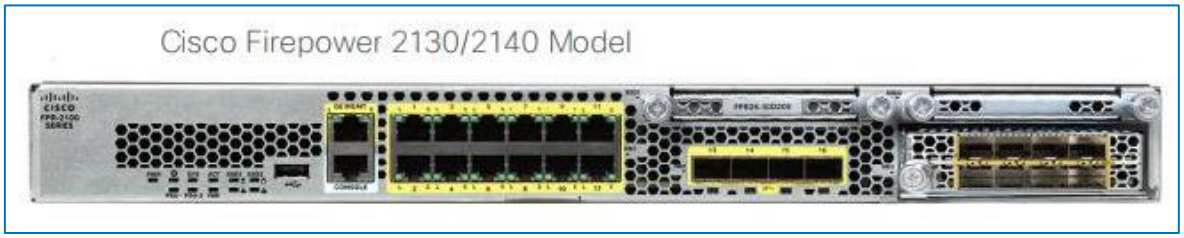

Figura 3-3. NGFW Cisco Firepower Modelo 2110/2120 datasheet (CISCO, 2020)

El proveedor Fortinet con el equipo de la serie Fortigate 300E un firewall de nueva generación que de acuerdo a su datasheet (FORTINET, 2020) proporciona una solución SDWAN segura, escalabre y centrada en la aplicación, protege contra amenazas cibernéticas con aceleración del sistema en un chip, proporciona una estrecha integración de red a la nueva generación de seguridad y su modelo se muestra de acuerdo a la Figura 3-4.

Figura 3-4. NGFW Fortinet Fortigate serie 300E datasheet (FORTINET, 2020)

Los tres equipos presentan las siguientes características conforme a sus datasheets y se los expone en la Tabla 3-2 y Tabla 3-3.

Características	**Check Point Quantum 6600 Plus**	**Cisco Firepower 2130**	**Fortinet FortiGate 300E**
Rendimiento del Sistema			
IPS	10,14 Gbps	5 Gbps (NGIPS)	5 Gbps
NGFW	6,2 Gbps	5 Gbps	3,5 Gbps
Prevención contra amenazas	3,7 Gbps		3 Gbps
Firewall	18 Gbps	10 Gbps	
Interfaces y Módulos			
Interfaces GE RJ45	18	12	16
Ranuras GE SFP	4	4	16
Ranuras 10GE SFP	4	1	
Ranura 10G FTW		1	
Puertos de administración RJ45 GE			2
Puertos USB		1	2
Puerto de consola RJ45		1	1
Almacenamiento local	1 unidad SSD 240 GB	1 unidad 200 GB	No
Transceptores incluidos			2x SFP (SX 1 GE)
Rendimiento y Capacidad del sistema			
Rendimiento del firewall IPv4 (1518/512/64 bytes, UDP)	32 Gbps	10 Gbps	32/32/20 Gbps
Rendimiento del firewall IPv6 (1518/512/64 bytes, UDP)			32/32/20 Gbps
Latencia del firewall (64 bytes, UDP)		No	3 µs
Rendimiento del firewall (paquete por segundo)			30 Mpps
Sesiones simultáneas (TCP)	4 millones	2 millones	4 millones
Nuevas sesiones / segundo (TCP)	116000	40000	300000
Políticas de firewall			10000
Filtrado URL		280 millones	
Rendimiento de VPN IPsec (512 bytes) 1	4,9 Gbps	1,6 Gbps (1024B)	20 Gbps
Túneles VPN IPsec de puerta de enlace a puerta de enlace		7500	2000
Túneles VPN de IPsec de cliente a puerta de enlace			50000

Tabla 3-2. (a) Comparativo de equipos NGFW datasheet (CHECK POINT, 2020), (CISCO, 2020), (FORTINET, 2020)

Características	Check Point Quantum 6600 Plus	Cisco Firepower 2130	Fortinet FortiGate 300E
Rendimiento de VPN SSL			2,5 Gbps
Usuarios concurrentes de SSL-VPN (Máximo recomendado, modo túnel)			5000
Rendimiento de inspección SSL (IPS, HTTPS promedio)			3,9 Gbps
CPS de inspección SSL (IPS, HTTPS promedio)			2500
Sesión concurrente de inspección SSL (IPS, HTTPS promedio)			340 000
Rendimiento de control de aplicaciones (HTTP 64K)			7 Gbps
Rendimiento CAPWAP (1444 bytes, UDP)			5 Gbps
Dominios virtuales (predeterminado / máximo)			10/10
Número máximo de FortiSwitches admitidos			72
Número máximo de FortiAP (total / túnel)	1024/4096		512/256
Número máximo de FortiTokens			5000
Memoria	16 GB		
CPU	1 x 6x núcleos físicos		
Configuraciones de alta disponibilidad	Activo-Activo L2, Activo-Pasivo L2 y L3	Activo-activo y activo -en espera	Activo-activo, activo-pasivo, agrupación
Dimensiones y potencia			
Alto x Ancho x Largo (pulgadas)	17,2 x 20 x 1,73	1,73 x 16,90 x 19,76	1,75 x 17,0 x 15,0
Alto x Ancho x Largo (mm)	438 x 508 x 44	44 x 42 x 502	44,45 x 432 x 380 16,1 libras (7,3 kg)
Peso	17,4 libras (7,9 kg)	19.4 libras (8,8 kg)	16,1 libras (7,3 kg)
Factor de forma (compatible con estándares EIA / no EIA)	1RU	1RU	1RU
Potencia de salida máxima de CA		400W	
Potencia de salida máxima DC		350W	
Consumo de energía (promedio / máximo)	84W / 122W		90 W / 173 W
Entrada de energía	100 V - 240 V, 47 - 63 Hz	100 V - 240 V AC, 50 - 60 Hz	100 V - 240 V CA, 50 - 60 Hz
Corriente (máxima)		6ª	6ª
Disipación de calor	416 BTU / h		570 BTU / h
Ventilación		1 ventilador intercambiable en caliente	
Fuentes de alimentación redundantes (intercambiables en caliente)	2 x AC o DC	1+1 AC or DC	Opcional
Entorno Operativo y certificaciones			
Temperatura de funcionamiento	0° a 40° C	0° a 40° C	0° a 40 ° C
Temperatura de almacenamiento	- 20° a 70° C	- 20° a 70° C	-35 a 70 ° C
Humedad	5 al 95%	10 - 85% sin condensación	10–90% sin condensación
Nivel de ruido		56 dBA	48 Dba
Altitud operativa		10000 pies	Hasta 7,400 pies (2,250 m)
Conformidad	FCC,RCM / C-Tick ,VCCI, CE,UL,CB, TUV GS	CE, UL, EN, IEC, AS/NZS	FCC Parte 15 Clase A, RCM, VCCI, CE, UL / cUL, CB
Certificaciones			Laboratorios ICSA: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6 / IPv6

Tabla 3-3. (b) Comparativo de equipos NGFW datasheet (CHECK POINT, 2020), (CISCO, 2020), (FORTINET, 2020)

Entre los principales funciones y beneficios de los firewalls de nueva generación según los datasheets se tiene:

El equipo Quantum 6600 de la marca Check Point según su datasheet presenta los siguientes funciones y beneficios (CHECK POINT, 2020):

- ✓ Prevención de alto calibre con seguridad unificada. Check Point SandBlast Network es una caja de arena resistente a la evasión, brinda protección de día cero contra amenazas avanzadas y desconocidas.
- ✓ Expansión bajo demanda con hiperescalidad. El equipo Quantum 6600 incluye todas las tecnologías de seguridad, incluido el paquete de software SandBlast (sandboxing) durante un año.
- ✓ Monitoreo y administración remota. La tarjeta Lights-Out-Management (LOM) proporciona administración fuera de banda para diagnosticar, iniciar, reiniciar y administrar de forma remota
- ✓ Opciones de alto rendimiento. El adquirir el paquete plus incorpora 4 puertos de fibra, gestión de luces apagadas, mayor memoria.
- ✓ Reduce el tiempo de gestión de operaciones hasta un 80%.

El equipo Firepower 2130 de la marca Cisco según su datasheet presenta las siguientes funciones y beneficios (Cisco, 2020):

- ✓ NGFW centrado en amenazas. Mejora la recuperabilidad comercial y rendimiento con una defensa superior ante amenazas, control granular de aplicaciones, protección contra malware, reducción de tiempo para la detección y corrección, reducción de la complejidad de administración.
- ✓ Densidad de puertos y rendimiento optimizados. Firewall de 5 Gbps, 24 puertos de 1 GE, en factor forma 1RU.
- ✓ Arquitectura innovadora. El equipo posee una arquitectura exclusiva de 2 CPU, Activar las funciones de protección contra amenazas no afecta el rendimiento del firewall.
- ✓ Administración para satisfacer las necesidades. Consume incluso menos tiempo de configuración y menos costoso de administrar.

El equipo Fortigate 300E de la marca Fortinet según su datasheet presenta las siguientes funciones y beneficios (FORTINET, 2020):

- ✓ Reduce la complejidad y maximiza su ROI. Al integrar las capacidades de seguridad de protección contra amenazas en un solo dispositivo de seguridad de red de alto rendimiento, impulsado por la Unidad de procesamiento de seguridad (SPU) de Fortinet.
- ✓ Visibilidad total de los usuarios. Dispositivos y aplicaciones en toda la superficie de ataque y aplicación de políticas de seguridad constante independientemente de la ubicación de los activos.
- ✓ Protección contra las vulnerabilidades explotables de la red. Con IPS validado por la industria que ofrece baja latencia y rendimiento de red optimizado.
- ✓ Bloqueo automáticamente de las amenazas. En el tráfico descifrado utilizando el rendimiento de inspección SSL más alto de la industria, incluido el último estándar TLS 1.3 con cifrados obligatorios Bloqueo de manera proactiva los ataques sofisticados recién descubiertos en tiempo real con los laboratorios.
- ✓ FortiGuard con tecnología de inteligencia artificial y los servicios avanzados de protección contra amenazas incluidos en Fortinet Security Fabric.

Otro punto a considerar dentro del análisis de firewalls de nueva generación son los costos para implementar un equipo de esta tecnología de seguridad perimetral. En este estudio se tomó en consideración los valores referenciales de un partner en el país, los cuales se presentan en la Tabla 3-4.

Equipo	**Check Point**	**Cisco**	**Fortinet**
	Quantum 6600 Plus	Firepower 2130	FortiGate 300E
Costo referencial del equipo	$ 45000,00	$ 31000,00	$ 10400,00
Costo referencial de licencia Anual	$ 18020,00	$ 3000,00	$ 4100,00
Costos de instalación y configuración	$ 25,00/hora 4 horas		
Costo referencial de mantenimiento anual	$ 25,00/hora 2 horas		
Costo referencial de capacitación	$ 25,00/hora 24 horas		
Total	**$ 63770,00**	**$ 34750,00**	**$ 15250,00**

Tabla 3-4. Costos Referenciales de Equipos NGFW (TOTALTEK)

3.4. ESQUEMA DEL SISTEMA DE SEGURIDAD PERIMETRAL PROPUESTO PARA EL LTIC

3.4.1 TOPOLOGÍA IDEAL

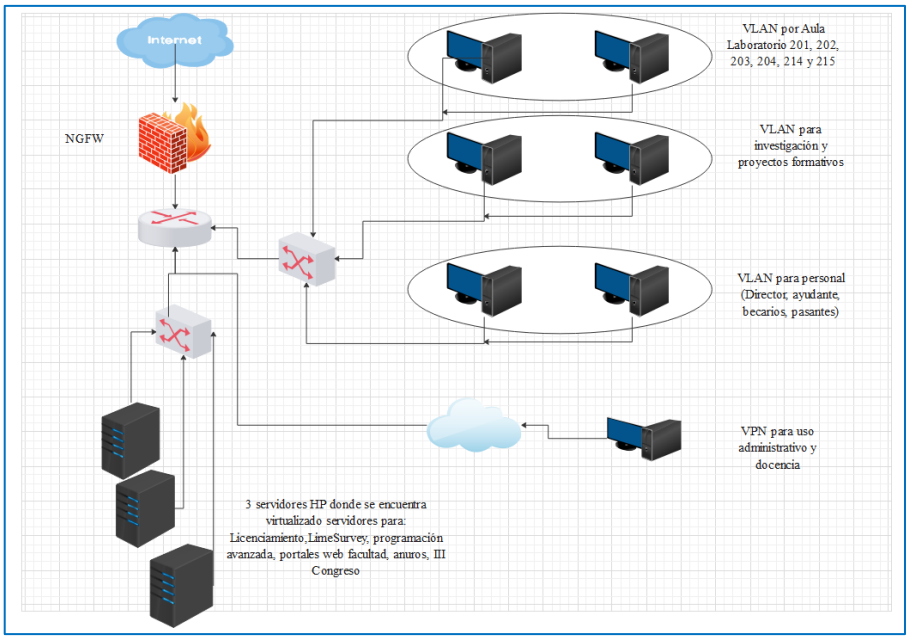

Figura 3-5. Topología Ideal Sistema de Seguridad Perimetral (Salazar Gualoto, 2020)

Luego de la evaluación de la tecnología seleccionada para el sistema de seguridad perimetral informática es necesario proponer la topología ideal de seguridad para el LTIC conformada por los siguientes elementos:

- ✓ Firewall de nueva generación (Check Point Quantum 6600 plus o Cisco Firepower 2130 o Fortinet Fortigate 300E)
  - Permite al administrador la gestión simple, ágil y unificada, a través de un solo panel para proporcionar la eficiencia superior en el manejo de las políticas.
  - Permite la protección hiperactiva en tiempo real contra amenazas conocidas, desconocidas y más avanzadas. Aprovecha la inteligencia de amenazas para bloquear amenazas en todas las plataformas para evitar penetración en la red.
- ✓ Segmentación de la red LAN por medio de la creación de VLANs
  - VLAN por aula laboratorio (201, 202, 203, 204, 214 y 215)
  - VLAN para investigación, proyectos formativos.
  - VLAN para personal administrativo (director, ayudante, becarios y pasantes)
- ✓ VPN para uso administrativo y por el personal docente.

3.4.2 TOPOLOGÍA PROPUESTA

La topología propuesta para el LTIC está conformada de acuerdo a la Figura 3-6 y está basada en factores técnicos, de gestión, administración, instalación y configuración de equipos, partners en el país, servicio de soporte ,capacitación y costos económicos.

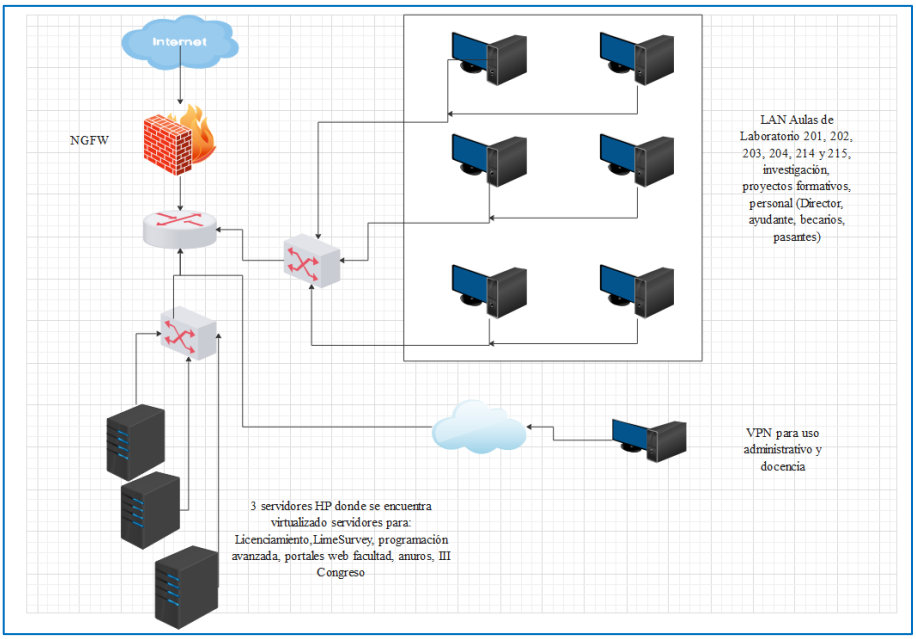

Figura 3-6. Topología Propuesta Sistema de Seguridad Perimetral (Salazar Gualoto, 2020)

Los elementos que forman parte de la topología propuesta son:

- ✓ Firewall de nueva generación (Check Point Quantum 6600 plus o Cisco Firepower 2130 o Fortinet Fortigate 300E)

El firewall de nueva generación proporciona una visibilidad integral y seguridad avanzada de capa 7 que incluye protección contra amenazas prevención de intrusiones, filtrado web y control de aplicaciones.

Permite al administrador la gestión simple, ágil y unificada, a través de un solo panel para proporcionar la eficiencia superior en el manejo de las políticas.

3.5. POLÍTICA DE SEGURIDAD Y/O MECANISMOS DE DEFENSA

Un aspecto que complementa este estudio es la política de seguridad y/o mecanismos defensa para lo cual se propone una política de seguridad que se describe con mayor detalle en el anexo 6

CAPÍTULO IV

4. IMPLEMENTACIÓN Y EVALUACIÓN DEL PROTOTIPO DE SISTEMA DE SEGURIDAD PERIMETRAL

Esta sección cubre la implementación de un prototipo de sistema de seguridad perimetral informática con la tecnología firewall de nueva generación mediante la plataforma virtual Check Point Gaia R81 donde se emula la appliences 6000, para ello se realiza la selección de tecnología, la instalación y configuración de la plataforma de seguridad cibernética Check Point Gaia R81 y la evaluación de las vulnerabilidades post implementación de CPG-R81.

4.1. SELECCIÓN DE LA TECNOLOGÍA DE SEGURIDAD PERIMETRAL

La tecnología de seguridad perimetral, firewall de nueva generación analizada en el capítulo 3 proporcionan varios beneficios e implementar cualquiera de ellas mejora la seguridad informática del LTIC. En este estudio como prototipo de sistema de seguridad perimetral en el LTIC se ha escogido las funcionalidades del proveedor Check Point con su equipo Quantum 6600, porque brinda múltiples facilidades para simular el equipo firewall de nueva generación y probar sus funcionalidades mediante su plataforma de seguridad cibernética Check Point Gaia R81.

Check Point Gaia R81 es un software de gestión de seguridad y prevención de amenazas. Ofrece simplicidad y consolidación sin concesiones en toda la empresa para tratar de implementar las últimas tecnologías y seguridad para proteger la organización o diseñar políticas de seguridad de manera experta. (Check Point Gaia, 2020).

La implementación de Check Point Gaia versión R81 requiere de los siguientes requisitos mínimos básicos según la Tabla 4-1 para la instalación del servidor abierto.

Componente	**Requisitos Hardware**
Procesador	Intel Pentium IV, 2,6 GHz o equivalente
# de Núcleos del CPU	4
Memoria	8 GB
Disco Duro	110 GB

Tabla 4-1. Requisitos mínimos para Check Point Gaia R81 (Check Point Gaia Realase Notes, 2020)

Adicional de la máquina virtual se requiere la instalación de smart console que es compatible con:

- ✓ Windows 10 (todas las ediciones), Windows 8.1 (Pro) y Windows 7 (SP1, Ultimate, Professional y Enterprise)
- ✓ Windows Server 2019, 2016, 2012, 2008 (SP2) y 2008 R2 (SP1)

4.2. INSTALACIÓN DE CHECK POINT GAIA R81

La instalación y configuración de la plataforma de seguridad cibernética Check Point Gaia R81 se la puede revisar con mayor detalle en el Anexo 10, allí se encuentra paso a paso la creación de la máquina virtual, la instalación y configuración del sistema operativo Check Point Gaia R81, la instalación de Smart Console y la emulación de la appliances 6000 como NGFW sobre el Check Point Gaia R81.

4.3. POLÍTICAS DE APPLIANCES 6000 SOBRE CHECK POINT GAIA R81

El funcionamiento de NGFW está basado en la agregación de políticas para ello se implementó en la appliances 6000 sobre Check Point Gaia R81 las siguientes políticas

4.3.1 POLÍTICAS DE CONTROL DE ACCESO

La creación de políticas de control de acceso requiere la definición de "Address Ranges", en el menú derecho de Smart Console, aquí se agrega el rango de direcciones que usa el LTIC como se muestra en la Figura 4-1.

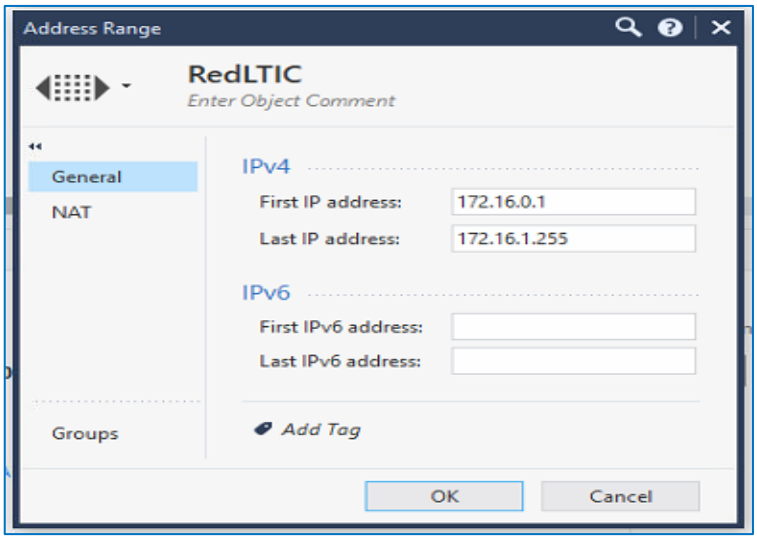

Figura 4-1. Agregación de Rango de Direcciones en Smart Console de CPG-R81 (Salazar Gualoto, 2020)

Una vez creada el rango de direcciones del LTIC dar clic en el menú izquierdo en "Security Policies" y agregar las reglas para control de acceso en este caso se creó cuatro reglas básicas para probar el funcionamiento del equipo Check Point Gaia R81emulando appliances 6000. Esta políticas se describen así, en la Figura 4-2 se presenta la regla por defecto de negar todo, en la Figura 4-3 consta la regla de permitir el acceso de la Red del LTIC al Internet, en la Figura 4-4 consta la regla para permitir acceso a la Red del LTIC a la Red del LTIC y finalmente en la Figura 4-5 se presenta la regla de permitir el acceso de Internet a la Red del LTIC.

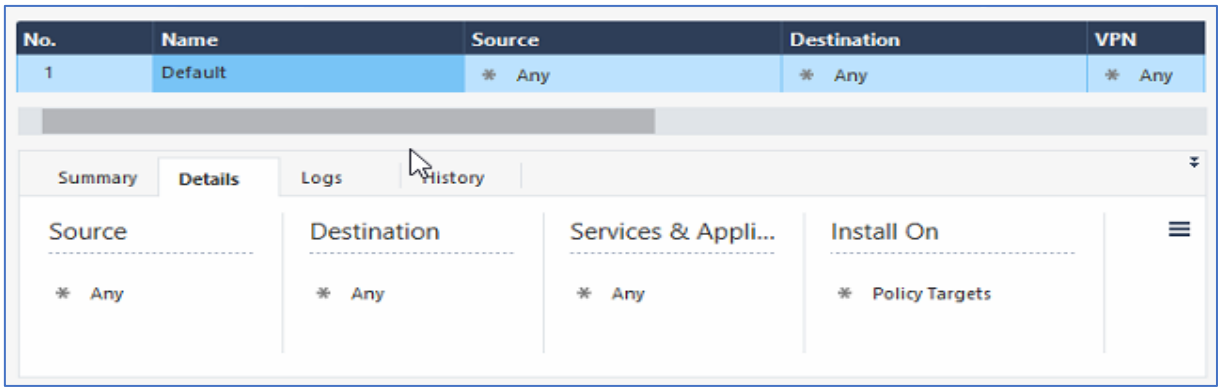

Figura 4-2. Reglas Default de control de acceso de CPG-R81 (Salazar Gualoto, 2020)

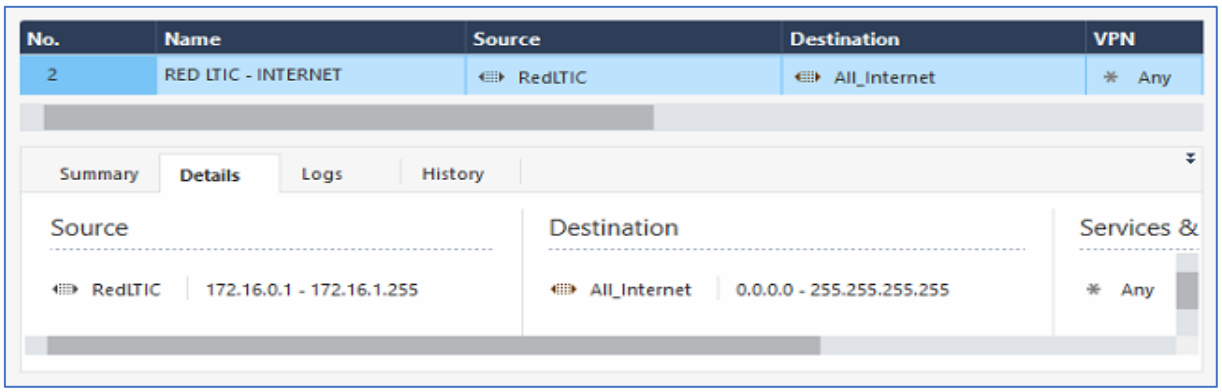

Figura 4-3. Reglas Red LTIC – Internet de control de acceso de CPG-R81 (Salazar Gualoto, 2020)

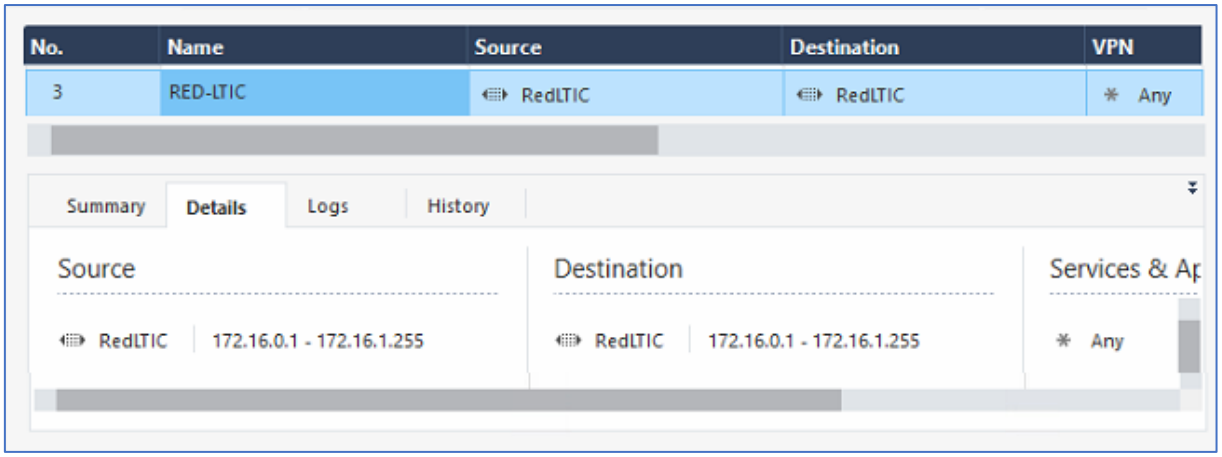

Figura 4-4. Reglas Red LTIC – Red LTIC de control de acceso de CPG-R81 (Salazar Gualoto, 2020)

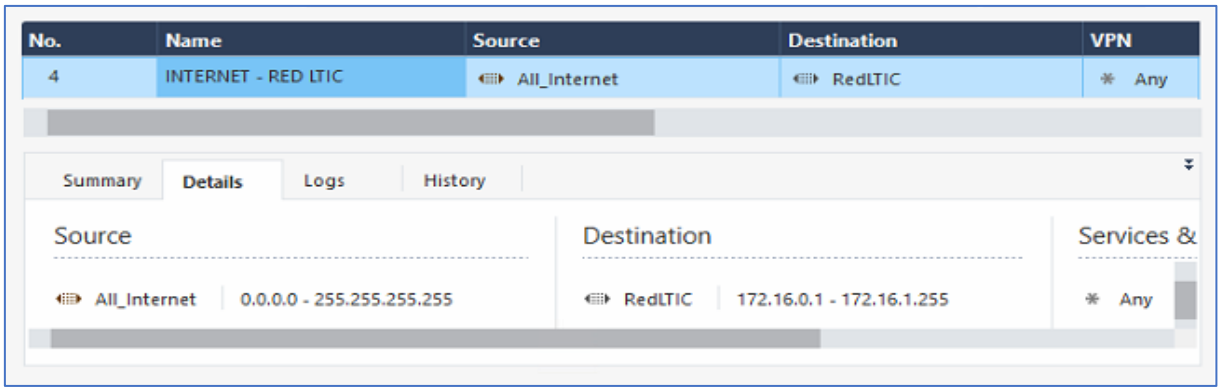

Figura 4-5. Reglas Internet – Red LTIC de control de acceso de CPG-R81 (Salazar Gualoto, 2020)

Una vez ingresada las reglas para guardar en esta plataforma hay que dar clic en el botón Publish en el menú superior como se muestra en la Figura 4-6

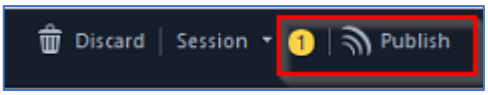

Figura 4-6. Opción Publish de CPG-R81 (Salazar Gualoto, 2020)

Para publicar finalmente dar clic en el botón Publish como se muestra en la Figura 4-7

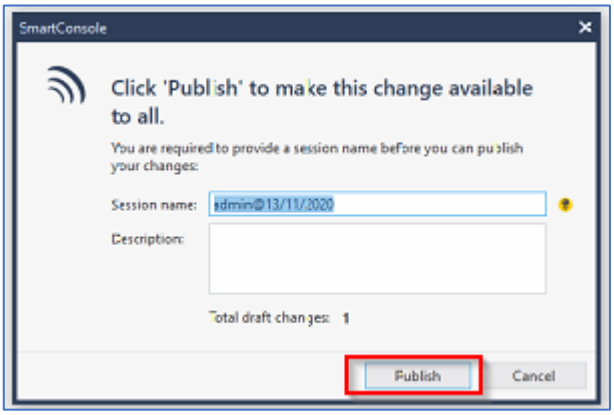

Figura 4-7. Publicación de cambios de CPG-R81 (Salazar Gualoto, 2020)

4.3.2 POLÍTICAS THREAT PREVENTION

El equipo Check Point Gaia R81 en el que se encuentra emulado 6000 appliances contiene dos políticas prevención de prevención de amenazas y una opción para protección de archivos para este estudio se ha configurado las tres como se muestra en los siguientes numerales.

4.3.2.1 *Políticas Threat Prevention*

En las políticas de prevención de amenazas (Threat Prevention) se creó dos, una para prevenir las amenazas en la Red del LTIC como se muestra la Figura 4-8 y la otra para el ingreso de internet como se muestra en la Figura 4-9.

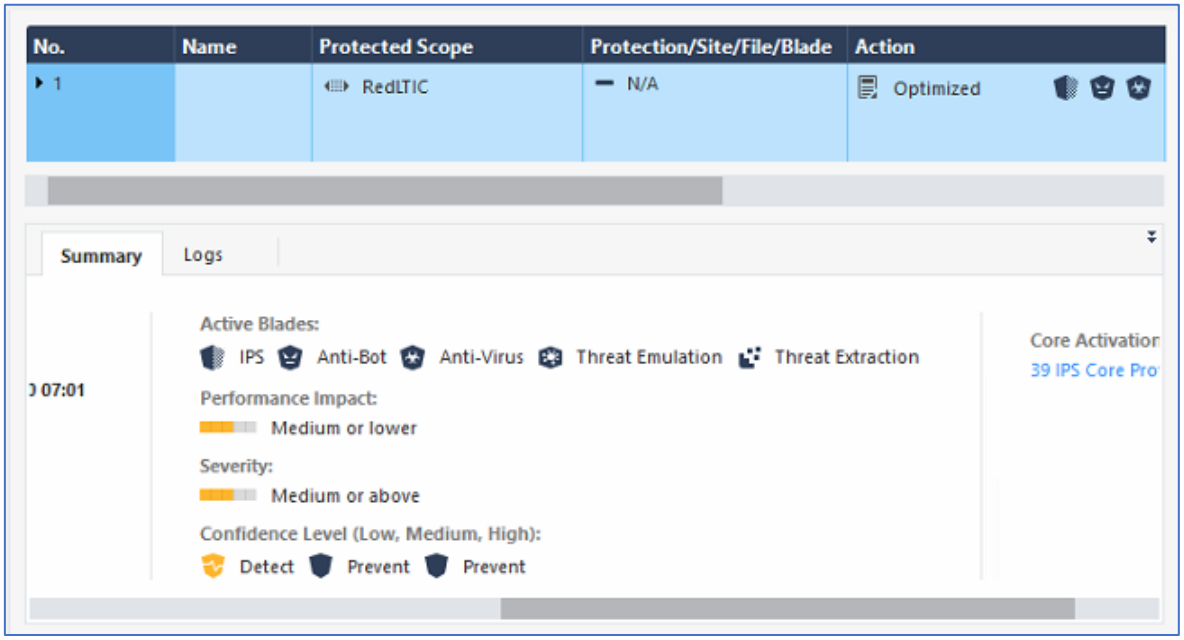

Figura 4-8. Políticas Red LTIC Threat Prevention de CPG-R81 (Salazar Gualoto, 2020)

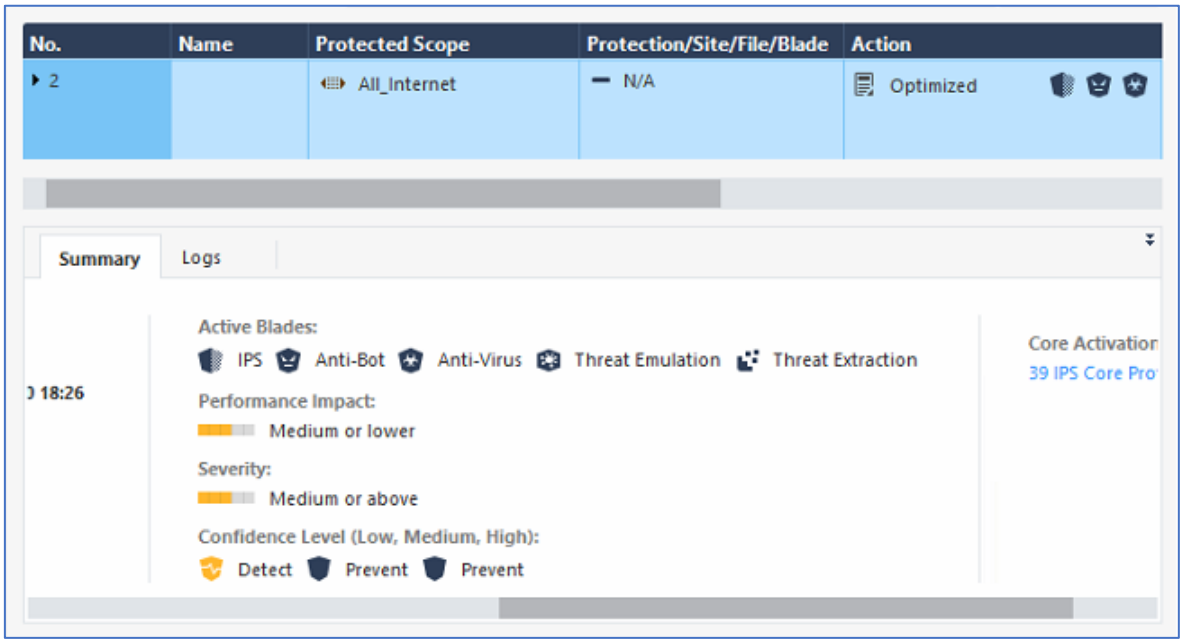

Figura 4-9. Políticas All Internet Threat Prevention de CPG-R81 (Salazar Gualoto, 2020)

4.3.2.2 *Políticas Infinity Threat Prevention*

En la creación de políticas de prevención de amenazas infinitas (Infinity Threat Prevention) con los perfiles de tecnología que brinda Check Point Gaia como se muestra en la Figura 4-10 se agregó la

detección para la Red del LTIC y a todo el Internet acorde los perfiles de toda la tecnología como se muestra en la Figura 4-11

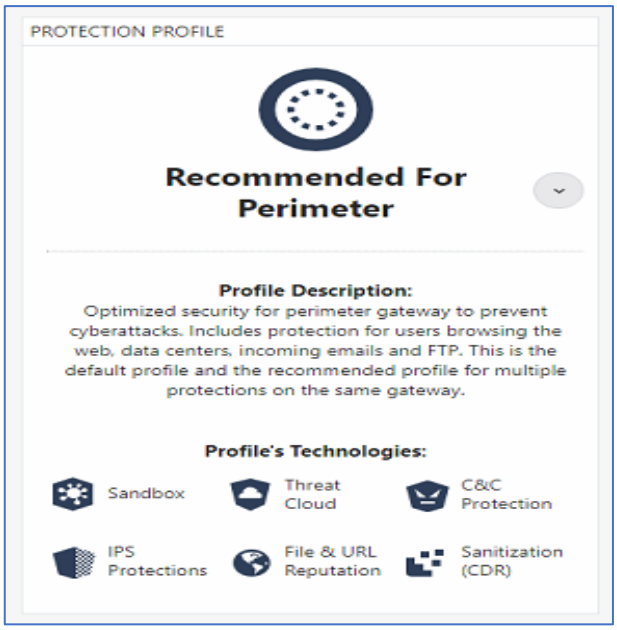

Figura 4-10. Perfiles Tecnológicos de Infinity Threat Prevention de CPG-R81 (Salazar Gualoto, 2020)

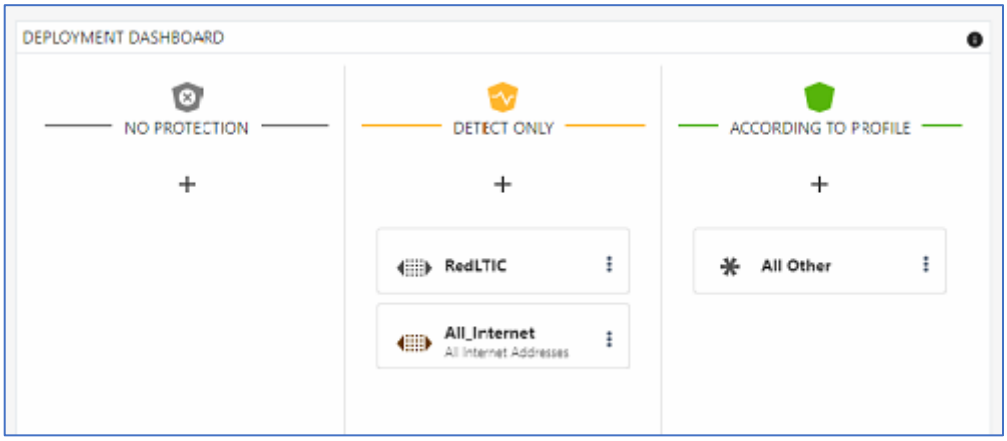

Figura 4-11. Política de Infinity Threat Prevention de CPG-R81 (Salazar Gualoto, 2020)

4.3.2.3 *Protección de Archivos*

La prevención de amenazas consta de una sub opción donde se realiza la protección de archivos (file protections), en este estudio se ha activado la protección a los archivos más conocidos (suite de Microsoft Office) como se muestra en la Figura 4-12

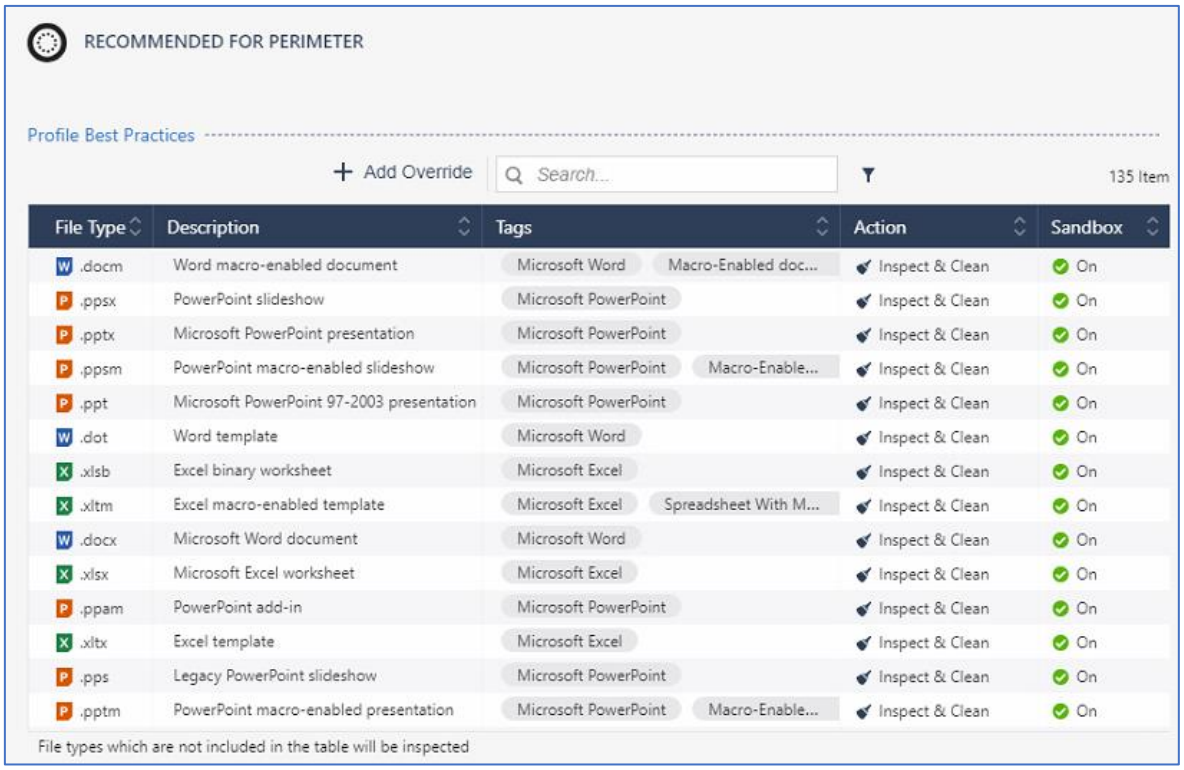

Figura 4-12.Proteccion de archivos de CPG-R81 (Salazar Gualoto, 2020)

4.3.3 POLÍTICA HTTPS INSPECTION

El equipo Check Point Gaia R81 posee la opción de política para inspección https (https inspection) en este caso se agregó tres políticas para la inspección de la red LTIC a Internet, Internet a Red LTIC y para inspección de pornografía como se muestra en la Figura 4-13.

No.	Name	Source	Destination	Services	Category/Custom A.	Action	Track	Blade	Install On	Certificate	Comm...
1	RED LTIC INTERNET	RedLTIC	Internet	HTTPS default s...	Any	Inspect	None	All	Policy H...	Outbound Certi...	
2	INTERNET RED LTIC	Internet	RedLTIC	HTTPS default s...	Any	Inspect	None	All	Policy H...	Outbound Certi...	
3	Pornografia	RedLTIC	Internet	HTTPS default s...	Pornography	Inspect	Alert	IPS Anti-Bot Applicati... URL Filte...	Policy H...	Outbound Certi...	

Figura 4-13. Política Https Inspection de CPG-R81 (Salazar Gualoto, 2020)

4.4. ANÁLISIS FINAL DE VULNERABILIDADES DE LA RED DEL LTIC POST IMPLEMENTACIÓN DE CHECK POINT GAIA R8

El análisis final de las vulnerabilidades de la red del LTIC post implementación de Check Point Gaia emulando Appliances 6000 se realizó mediante hacking ético basado en la metodología caja gris con

la herramienta Nessus profesional, los informes completos para mayor detalle se encuentran en el Anexo 7 y 8. A continuación se presenta un resumen procesado de los resultados.

4.4.1 ANÁLISIS CON NESSUS PROFESIONAL

Se realizó un escaneo de la red del LTIC mediante el uso del software Nessus Profesional post implementación de Check Point Gaia R81 y se obtuvo los resultados que se exponen a continuación.

4.4.1.1 *Análisis de la Red Externa puceing.edu.ec*

Nessus Profesional luego de la implementación de Check Point Gaia R81 determinó los siguientes resultados por gravedad de acuerdo a la Figura 4-14 de la red externa puceing.edu.ec y que se describen en el resumen de análisis por gravedad

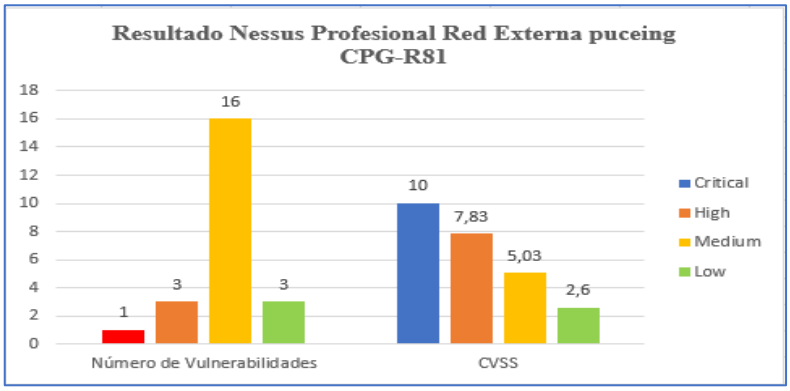

Figura 4-14. Resultado de Vulnerabilidades CPG-R81 - Puceing, Nessus (Salazar Gualoto, 2020)

RESUMEN DE ANÁLISIS POR GRAVEDAD

Vulnerabilidades de Seguridad por Gravedad Critical

CVSS	Plugin	Origen y Vulnerabilidad
10.0	58987	PHP Unsupported Version Detection

Tabla 4-2. Resumen Vulnerabilidades Gravedad Critical CPG-R81- Puceing Nessus (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad High

CVSS	Plugin	Origen y Vulnerabilidad
8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
7.5	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.

Tabla 4-3. Resumen Vulnerabilidades Gravedad High CPG-R81 - Puceing, Nessus (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Medium

CVSS	Plugin	Origen y Vulnerabilidad
6.4	51192	SSL Certificate Cannot Be Trusted
6.4	57582	SSL Self-Signed Certificate
6.1	104743	TLS Version 1.0 Protocol Detection
5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
5.0	10539	DNS Server Recursive Query Cache Poisoning Weakness
5.0	35450	DNS Server Spoofed Request Amplification DDoS
5.0	11213	HTTP TRACE / TRACK Methods Allowed
5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
5.0	142591	PHP < 7.3.24 Multiple Vulnerabilities
5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
4.3	136929	JQuery 1.2 < 3.5.0 Multiple XSS
4.3	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability
4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
4.3	57690	Terminal Services Encryption Level is Medium or Low

Tabla 4-4. Resumen Vulnerabilidades Gravedad Medium CPG-R81 - Puceing, Nessus (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Low

CVSS	Plugin	Origen y Vulnerabilidad
2.6	70658	SSH Server CBC Mode Ciphers Enabled
2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant

Tabla 4-5. Resumen Vulnerabilidades Gravedad Low CPG-R81 - Puceing, Nessus (Salazar Gualoto, 2020)

4.4.1.2 *Análisis de la Red Interna del LTIC*

Nessus Profesional luego de la implementación de Check Point Gaia R81 emulando appliances 6000 encontró las siguientes vulnerabilidades por gravedad como se observa en la Figura 4-15 en la red interna del LTIC y que se describen en el resumen de análisis por gravedad.

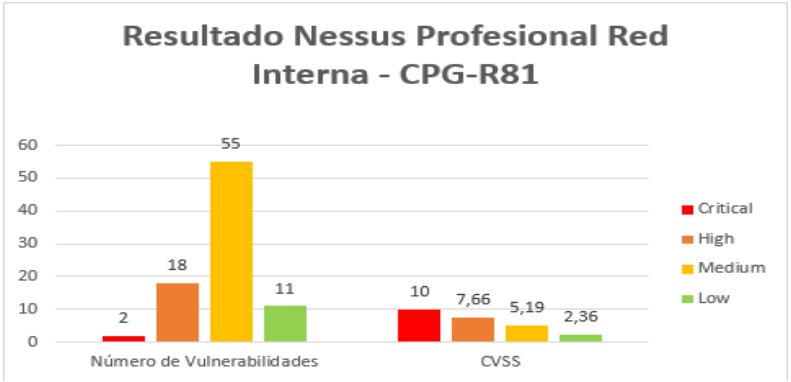

Figura 4-15. Resultado de Vulnerabilidades CPG-R81 - Red Interna, Nessus (Salazar Gualoto, 2020)

RESUMEN DE ANÁLISIS POR GRAVEDAD

Vulnerabilidades de Seguridad por Gravedad Critical

CVSS	Plugin	Origen y Vulnerabilidad	IP
10.0	58987	PHP Unsupported Version Detection	172.16.0.7, 172.16.0.18, 172.16.0.92
10.0	136890	Telnetd - Remote Code Execution (CVE-2020-10188)	172.16.0.58

Tabla 4-6. Resumen Vulnerabilidades por Gravedad Critical CPG-R81 - Red Interna, Nessus (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad High

CVSS	Plugin	Origen y Vulnerabilidad	IP
8.5	122821	PHP 7.0.x < 7.0.33 Multiple vulnerabilities	172.16.0.7
8.5	119766	PHP 7.2.x < 7.2.13 Multiple vulnerabilities	172.16.0.7
8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities	172.16.0.18, 172.16.0.92
7.8	80101	IPMI v2.0 Password Hash Disclosure	172.16.1.52
7.8	122257	iLO 2 <= 2.23 Denial of Service Vulnerability	172.16.1.52
7.5	128148	Flexera FlexNet Publisher < 11.16.2 Multiple Vulnerabilities	172.16.0.6, 172.16.0.8
7.5	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	172.16.0.7
7.5	139574	Apache 2.4.x < 2.4.46 Multiple Vulnerabilities	172.16.0.7, 172.16.0.18, 172.16.0.92
7.5	121353	PHP 7.2.x < 7.2.14 Multiple vulnerabilities.	172.16.0.7
7.5	123828	PHP 7.2.x < 7.2.16 Multiple vulnerabilities.	172.16.0.7
7.5	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.	172.16.0.7, 172.16.0.18, 172.16.0.92
7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.	172.16.0.18, 172.16.0.92
7.5	10882	SSH Protocol Version 1 Session Key Retrieval	172.16.0.54
7.5	41028	SNMP Agent Default Community Name (public)	172.16.0.58, 172.16.0.93, 172.16.0.95
7.5	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities	172.16.0.92
7.5	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow	172.16.0.92
7.2	123642	Apache 2.4.x < 2.4.39 Multiple Vulnerabilities	172.16.0.7, 172.16.0.18, 172.16.0.92
7.1	20007	SSL Version 2 and 3 Protocol Detection	172.16.0.6, 172.16.0.54

Tabla 4-7. Resumen Vulnerabilidades por Gravedad High CPG-R81 - Red Interna, Nessus (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Medium

CVSS	Plugin	Origen y Vulnerabilidad	IP
6.8	122060	Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	172.16.0.7, 172.16.0.92
6.8	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities	172.16.0.92
6.4	51192	SSL Certificate Cannot Be Trusted	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.41, 172.16.0.42, 172.16.0.43, 172.16.0.44, 172.16.0.54, 172.16.0.92, 172.16.0.181
6.4	57582	SSL Self-Signed Certificate	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.41, 172.16.0.42, 172.16.0.43, 172.16.0.44, 172.16.0.54, 172.16.0.92, 172.16.0.181
6.4	101788	Apache 2.4.x < 2.4.27 Multiple Vulnerabilities	172.16.0.7, 172.16.0.92
6.4	128033	Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	172.16.0.7, 172.16.0.18, 172.16.0.92
6.4	141355	PHP 7.2 < 7.2.34 / 7.3.x < 7.3.23 / 7.4.x < 7.4.11 Mulitiple Vulnerabilities	172.16.0.7
6.4	123754	PHP 7.2.x < 7.2.17 Multiple vulnerabilities.	172.16.0.7
6.4	124763	PHP 7.2.x < 7.2.18 Heap-based Buffer Overflow Vulnerability.	172.16.0.7
6.4	125639	PHP 7.2.x < 7.2.19 Multiple Vulnerabilities.	172.16.0.7
6.4	134162	PHP 7.2.x < 7.2.28 / PHP 7.3.x < 7.3.15 / 7.4.x < 7.4.3 Multiple Vulnerabilities	172.16.0.7
6.1	104743	TLS Version 1.0 Protocol Detection	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.92, 172.16.0.181
5.8	50686	IP Forwarding Enabled	172.16.0.1, 172.16.0.44, 172.16.0.58, 172.16.0.93, 172.16.0.95

Tabla 4-8. (a) Resumen Vulnerabilidades por Gravedad Medium CPG-R81 Red Interna, Nessus (Salazar Gualoto, 2020)

CVSS	Plugin	Origen y Vulnerabilidad	IP
5.8	135290	Apache 2.4.x < 2.4.42 Multiple Vulnerabilities	172.16.0.7, 172.16.0.18, 172.16.0.92
5.8	125642	OpenSSL 1.1.0 < 1.1.0k Vulnerability	172.16.0.7
5.8	127131	PHP 7.2.x < 7.2.21 Multiple Vulnerabilities.	172.16.0.7
5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	172.16.0.12
5.8	42263	Unencrypted Telnet Server	172.16.0.54, 172.16.0.58, 172.16.0.93, 172.16.0.95
5.1	18405	Microsoft Windows Remote Desktop Protocol Server MitM Weakness	172.16.0.1, 172.16.0.5, 172.16.0.8, 172.16.0.12
5.0	11213	HTTP TRACE / TRACK Methods Allowed	172.16.0.1, 172.16.0.7, 172.16.0.18, 172.16.0.92
5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm	172.16.0.1, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.12, 172.16.0.18, 172.16.0.41, 172.16.0.43, 172.16.0.44, 172.16.0.54, 172.16.0.92
5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.54, 172.16.0.92, 172.16.0.181
5.0	10061	Echo Service Detection	172.16.0.6, 172.16.0.10
5.0	10198	Quote of the Day (QOTD) Service Detection	172.16.0.6, 172.16.0.10
5.0	57608	SMB Signing not required	172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18
5.0	45411	SSL Certificate with Wrong Hostname	172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18
5.0	103838	Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)	172.16.0.7, 172.16.0.92
5.0	111788	Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	172.16.0.7, 172.16.0.18, 172.16.0.92
5.0	121355	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	172.16.0.7, 172.16.0.18, 172.16.0.92
5.0	140532	PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability	172.16.0.7
5.0	135926	PHP 7.2.x < 7.2.30 Multiple Vulnerabilities	172.16.0.7
5.0	136741	PHP 7.2.x < 7.2.31 / 7.3.x < 7.3.18, 7.4.x < 7.4.6 DoS	172.16.0.7
5.0	142591	PHP < 7.3.24 Multiple Vulnerabilities	172.16.0.7, 172.16.0.18, 172.16.0.92
5.0	15901	SSL Certificate Expiry	172.16.0.7, 172.16.0.12, 172.16.0.18, 172.16.0.41, 172.16.0.42, 172.16.0.43, 172.16.0.44, 172.16.0.54, 172.16.0.92
5.0	132726	OpenSSL 1.0.2 < 1.0.2u Procedure Overflow Vulnerability	172.16.0.18, 172.16.0.92
5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS	172.16.0.18, 172.16.0.92
5.0	76474	SNMP 'GETBULK' Reflection DDoS	172.16.0.58, 172.16.0.93, 172.16.0.95
5.0	104408	OpenSSL 1.0.x < 1.0.2m RSA/DSA Unspecified Carry Issue	172.16.0.92
4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.54
4.3	57690	Terminal Services Encryption Level is Medium or Low	172.16.0.1, 172.16.0.5, 172.16.0.8, 172.16.0.12
4.3	136929	JQuery 1.2 < 3.5.0 Multiple XSS	172.16.0.20, 172.16.0.6, 172.16.0.7
4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	172.16.0.5, 172.16.0.8, 172.16.0.12, 172.16.0.92, 172.16.0.181
4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	172.16.0.6, 172.16.0.54
4.3	117807	Apache 2.4.x < 2.4.35 DoS	172.16.0.7, 172.16.0.18, 172.16.0.92
4.3	121384	OpenSSL 1.1.0 < 1.1.0j Multiple Vulnerabilities	172.16.0.7
4.3	117500	PHP 7.2.x < 7.2.10 Transfer-Encoding Parameter XSS Vulnerability	172.16.0.7
4.3	138593	PHP 7.2.x < 7.2.32 / 7.3.x < 7.3.20 / 7.4.x < 7.4.8 Information Disclosure	172.16.0.7
4.3	112119	OpenSSL 1.0.x < 1.0.2p Multiple Vulnerabilities	172.16.0.18, 172.16.0.92
4.3	121383	OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities	172.16.0.18, 172.16.0.92
4.3	122504	OpenSSL 1.0.x < 1.0.2r Information Disclosure Vulnerability	172.16.0.18, 172.16.0.92
4.3	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability	172.16.0.18, 172.16.0.92
4.3	26928	SSL Weak Cipher Suites Supported	172.16.0.54
4.3	105291	OpenSSL 1.0.2 < 1.0.2n Multiple Vulnerabilities	172.16.0.92
4.3	109945	OpenSSL 1.0.x < 1.0.2o Multiple Vulnerabilities	172.16.0.92
4.3	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities	172.16.0.92

Tabla 4-9.(b) Resumen Vulnerabilidades por Gravedad Medium CPG-R81 Red Interna, Nessus (Salazar Gualoto, 2020)

Vulnerabilidades de Seguridad por Gravedad Low

CVSS	Plugin	Origen y Vulnerabilidad	IP
3.3	10663	DHCP Server Detection	172.16.0.5
3.3	139571	PHP 7.2.x < 7.2.33 Use-After-Free Vulnerability	172.16.0.7
3.3	11197	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)	172.16.0.58, 172.16.0.95
2.6	70658	SSH Server CBC Mode Ciphers Enabled	172.16.0.1, 172.16.0.2, 172.16.0.4, 172.16.0.17, 172.16.0.54, 172.16.0.58, 172.16.0.93, 172.16.0.95, 172.16.1.52, 172.16.1.76
2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	172.16.0.1, 172.16.0.5, 172.16.0.6, 172.16.0.7, 172.16.0.8, 172.16.0.10, 172.16.0.12, 172.16.0.18, 172.16.0.92
2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant	172.16.0.1, 172.16.0.5, 172.16.0.8, 172.16.0.12
2.6	71049	SSH Weak MAC Algorithms Enabled	172.16.0.54, 172.16.0.58, 172.16.0.93, 172.16.0.95, 172.16.1.52
1.9	128117	OpenSSL 1.1.0 < 1.1.0l Multiple Vulnerabilities	172.16.0.7
1.9	128115	OpenSSL 1.0.2 < 1.0.2t Multiple Vulnerabilities	172.16.0.18, 172.16.0.92
1.9	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability	172.16.0.92
N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	172.16.0.6, 172.16.0.41, 172.16.0.43, 172.16.0.44

Tabla 4-10. Resumen Vulnerabilidades por Gravedad Low CPG-R81 Red Interna, Nessus (Salazar Gualoto, 2020)

4.4.2 RESUMEN DE VULNERABILIDADES

Al procesar los resultados del escaneo de las vulnerabilidades con Nessus Profesional luego de implementar Check Point Gaia R81 emulando appliances 6000 se determinó lo siguiente:

4.4.2.1 *Red Externa puceing.edu.ec*

En la red externa según la Figura 4-16 Nessus Profesional determino 23 vulnerabilidades con un promedio de CVSS de 5,30

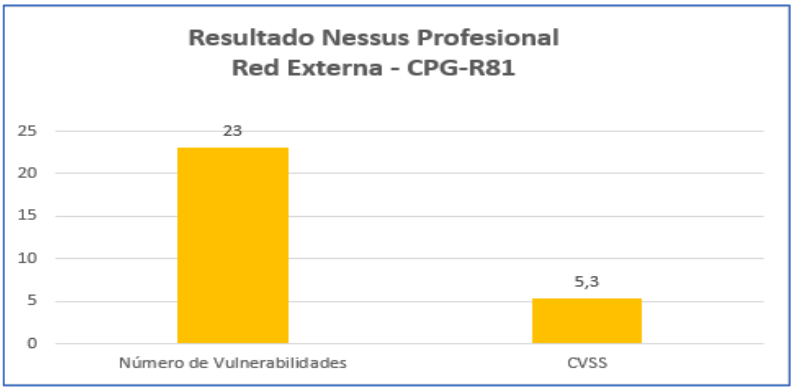

Figura 4-16. Resumen Final de VulnerabilidadesCPG-R81 - Red Externa LTIC (Salazar Gualoto, 2020)

4.4.2.2 *Red Interna del LTIC*

En la red interna del LTIC según la Figura 4-17 se encontró que Nessus Profesional determinó 86 vulnerabilidades con un promedio de CVSS de 5,46.

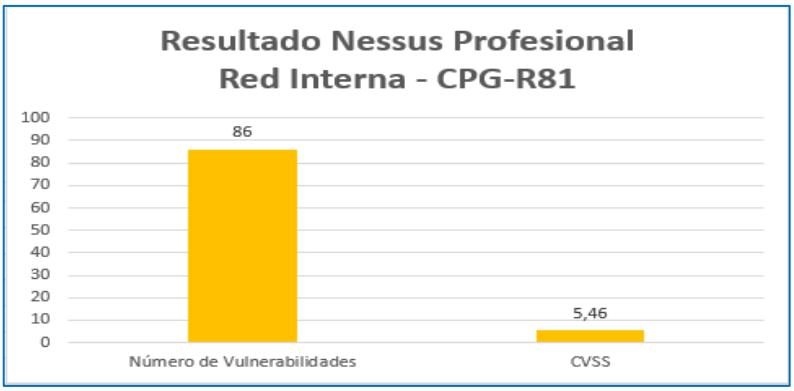

Figura 4-17. Resumen Final de Vulnerabilidades CPG-R81 - Red Interna LTIC (Salazar Gualoto, 2020)

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- ✓ Se identificó una variedad de vulnerabilidades en el análisis inicial, mediante el uso de las herramientas Nessus profesional, OpenVAS, Legion y GFI LandGuard en la infraestructura tecnológica del LTIC, las cuales denotan un promedio de CVSS de 5,14 en la red externa puceing.edu.ec y 5,64 en la red interna que nos determina un vector de ataque superior a 5,00.

- ✓ Mediante la inteligencia de amenazas se logró identificar que la red del LTIC se encuentra en gran medida expuesto a varios ataques, entre ellos tenemos ataques leves como MitM, Clickjacking, inyección de código malicioso y los más graves DoS, DDoS entre otros.

- ✓ Se encontró que los mecanismos de seguridad que el LTIC posee son un software de antivirus McAfee y UTM Untangle, herramientas que le proveen protección a la red, pero no permiten inspección de amenazas con baja latencia y rendimiento optimizado, gestión unificada y eficiente de los dispositivos y usuarios, aplicabilidad de políticas de seguridad y rendimiento de IPS mejorado.

- ✓ Se concluye de acuerdo al análisis de Gartner que los firewalls de nueva generación son tecnologías que incluyen características claves muy ponderadas como la integración con productos de seguridad, interfaz de administración, baja latencia y nuevos mecanismos para lograr un alto rendimiento.

- ✓ Se determinó luego del análisis de tecnologías de seguridad perimetral que es necesario la implementación de un firewall de nueva generación como sistema de seguridad perimetral informático debido que esta tecnología permite una protección unificada y de alto calibre a la red del LTIC, ayudando así a la seguridad de la infraestructura tecnológica y a los equipos informáticos del LTIC.

- ✓ Se estableció la necesidad de incluir en el diseño del sistema de seguridad perimetral la creación de una red privada virtual VPN para poder establecer comunicaciones privadas seguras sobre Internet y tener acceso desde el hogar a la red del LTIC para el personal técnico y para uso de personal docente de la Facultad de Ingeniería.

- ✓ La propuesta de política de seguridad informática presentada en este estudio permitirá mejorar procesos de seguridad y dotar de buenas prácticas para los usuarios del LTIC.

- ✓ En la evaluación del desempeño del prototipo de seguridad perimetral implementado mediante plataforma de seguridad cibernética Check Point Gia R81 emulando appliances 6000 se requirió 8GB de memoria, encontrando en este estudio el limitante del equipo físico que solo permitió usar 4,5 GB de memoria.

- ✓ En el análisis final de vulnerabilidades post implementación de CPG-R81 mediante la herramienta Nessus Profesional identificó un promedio de CVSS de 5,3 en la red externa puceing.edu.ec y 5,46 en la red interna que nos determina un vector de ataque superior a 5,00.

- ✓ El presente trabajo de titulación provee una base para la implementación de un sistema de seguridad perimetral informático en el LTIC basado en la tecnología de firewall de nueva generación.

- ✓ La formación cognitiva que proporciona la Maestría en Tecnologías de la Información mención Redes de Comunicaciones permitió el dominio en el desarrollo del presente estudio con visión integral para solucionar la problemática actual de la seguridad perimetral del LTIC y generar un alto nivel en el trabajo de titulación que de seguro influirá significativamente en la administración de la red del LTIC.

- ✓ La Maestría en Tecnologías de la Información mención Redes de Comunicaciones ha dotado de los conocimientos necesarios y el enfoque teórico - practico para el manejo y protección digital ampliando el perfil profesional del maestrante en un campo clave del negocio como es la seguridad informática para de esta manera aportar al desarrollo del país generando nuevos emprendimientos o mejorando el desempeño laboral en áreas públicas o privadas.

- ✓ Se concluye que la Pontificia Universidad Católica del Ecuador considerando la alta demanda de conocimientos en ciberseguridad, debe aumentar procesos teóricos – prácticos en sus programas carrera de pregrado y posgrado para fortalecer el perfil profesional de sus estudiantes.

- ✓ El análisis de la seguridad perimetral de las organizaciones públicas o privadas depende principalmente de la ejecución de las tres fases del hacking ético (reconocimiento de la

información, escaneo y explotación) para tener una visión integral de las vulnerabilidades y amenazas presentes en la red y mitigarlas.

5.2. RECOMENDACIONES

- ✓ El escaneo de vulnerabilidades utilizando hacking ético es una de las técnicas de caja gris para identificar las vulnerabilidades presentadas en la Red del LTIC, por lo tanto, se propone la implementación de una solución sea esta pagadas u open source en la Red del LTIC

- ✓ Para prevenir amenazas en la Red del LTIC es necesario la evaluación permanente de vulnerabilidades, esta evaluación preferentemente se plantea realizarla cada tres o seis meses.

- ✓ Las soluciones de escaneo para la evaluación de vulnerabilidades usadas en este estudio pueden ser consideradas como base de un futuro trabajo de titulación para la instalación y uso periódico en la Red del LTIC.

- ✓ Revisada la literatura del análisis inicial y final de las vulnerabilidades de la Red del LTIC se recomienda la implementación de procesos Hardening en servidores, aplicaciones y servicios usados como PHP, Apache, SSL, TLS.

- ✓ Se plantea la elaboración a futuro del trabajo de titulación la mitigación de las vulnerabilidades en la Red del LTIC mediante procesos de Hardening para mejorar la seguridad informática del LTIC

- ✓ Se recomienda la implementación de la tecnología firewall de nueva generación como sistema de seguridad perimetral informático por la protección unificada y de alto calibre que esta tecnología provee para lo cual este estudio realizo el análisis de tres proveedores de NGFW de los cuadrantes líderes y challengers para de esta manera mejorar la seguridad perimetral del LTIC

- ✓ Se aconseja considerar el estudio de tecnologías de seguridad perimetral open source como trabajo de titulación a futuro en función de reducir los costos de adopción de tecnologías firewall de nueva generación pagadas.

- ✓ Gartner en la revisión de firewall de red plantea en el supuesto de planificación estratégica para empresas medianas y grandes por el impacto de la pandemia Covid-19 la adopción de

FWaaS para respaldar el trabajo de los empleados desde casa. Por lo tanto, se sugiere FWaaS como trabajo de investigación a futuro.

- ✓ Se propone establecer buenas prácticas de seguridad a los usuarios del LTIC mediante la implementación y capacitación de la política de seguridad informática propuesta en este estudio.

- ✓ Se plantea realizar evaluaciones periódicas de la propuesta de política de seguridad de este estudio preferentemente cada año.

- ✓ El desarrollo de este estudio en medio de una pandemia determinó la necesidad de contar con una VPN para facilitar el acceso a la red del LTIC del personal técnico y docente de manera segura, por lo que se recomienda realizar la implementación de una VPN.

- ✓ Se sugiere para la implementación de Check Point Gia R81 como plataforma de seguridad cibernética emulando appliances 6000 contar con equipos físicos con memoria superior a los de 12 GB para abstraer un mejor desempeño.

- ✓ Se propone el uso de plataforma de seguridad cibernética Check Point Gaia R81 para la obtención de conocimientos e interacción con equipos de seguridad perimetral al ser un nicho de mercado muy poco explotado y requerido en el país.

- ✓ Si bien la implementación de equipos firewall de nueva generación aumenta la seguridad perimetral significativamente a la red, se recomienda en base al desarrollo del presente estudio que las organizaciones públicas o privadas realicen estudios sectorizados o individualizados para determinar la efectividad de la tecnología NGFW en la seguridad perimetral de la empresa.

- ✓ Se aconseja el uso de Hacking ético mediante caja gris para la evaluación de vulnerabilidades y amenazas en la seguridad perimetral de las organizaciones públicas o privadas.

BIBLIOGRAFÍA

Abad Domingo, A. (2018). *Seguridad y alta disponibilidad. 2ª edición.* España: GARCETA GRUPO EDITORIAL.

Astudillo, K. (2018). *Hacking Ético 3ra Edición.* Guayaquil: RA-MA.

ATEB. (07 de 06 de 2020). *blogateb.files.wordpress.com.* Obtenido de blogateb.files.wordpress.com: https://blogateb.files.wordpress.com/2017/08/politicas-corporativas-de-seguridad-informatica-ver-5-1.pdf

Carisio, E. (07 de 06 de 2020). *blog.mdcloud.es*. Obtenido de blog.mdcloud.es: https://blog.mdcloud.es/politicas-de-seguridad-informatica-y-su-aplicacion-en-la-empresa/

Castellanos Crespo, R. (28 de 05 de 2020). *seguridadasir.files.wordpress.com.* Obtenido de seguridadasir.files.wordpress.com: https://seguridadasir.files.wordpress.com/2012/01/tema_3_sad.pdf

Chakraborty, M., Chakrabarti, S., & Balas, V. (2019). *Advances in Intelligent Systems and Computing 1065.* Singapore: Springer.

Chang, H.-C., & Hawamdeh, S. (2020). *Cybersecurity for Information Profesionals Concepts and Applications.* Boca Raton: Taylor & Francis Group, LLC.

CHECK POINT. (25 de 09 de 2020). *www.checkpoint.com.* Obtenido de www.checkpoint.com: https://www.checkpoint.com/downloads/products/6600-security-gateway-datasheet.pdf

Check Point Gaia. (10 de 11 de 2020). *sc1.checkpoint.com*. Obtenido de sc1.checkpoint.com: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_RN/Topics-RN/Whats-New.htm

Check Point Gaia Realase Notes. (10 de 11 de 2020). *dl3.checkpoint.com.* Obtenido de dl3.checkpoint.com: http://dl3.checkpoint.com/paid/dc/dcae385f243a7c8b3f7f64b4117d1b66/CP_R81_ReleaseNotes.pdf?HashKey=1605057135_20a2d302e70feb96cc6fa4798dba40bb&xtn=.pdf

Chicano Tejada, E. (2014). *Auditoría de Seguridad Informatica.* Málaga: IC Editorial.

Christen, M., Gordijn, B., & Loi, M. (2020). *The Ethics of Cybersecurity.* Suiza: Board.

Cisco. (28 de 05 de 2020). *www.cisco.com*. Obtenido de www.cisco.com: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Cisco. (01 de 20 de 2020). *www.cisco.com*. Obtenido de www.cisco.com: https://www.cisco.com/c/es_ec/products/security/firepower-2100-series/index.html#~modelos

CISCO. (25 de 09 de 2020). *www.cisco.com.* Obtenido de www.cisco.com: https://www.cisco.com/c/en/us/products/collateral/security/firepower-2100-series/datasheet-c78-742473.pdf

Cortes, D. (01 de 09 de 2020). *polux.unipiloto.edu.co:.* Obtenido de polux.unipiloto.edu.co:: http://polux.unipiloto.edu.co:8080/00003329.pdf

Costas Santos, J. (2006). *Seguridad y Alta Disponibilidad.* Madrid, España: RA-MA S. A. Editorial y Publicaciones.

CVS. (20 de 06 de 2020). *cvs.gov.co.* Obtenido de cvs.gov.co: https://cvs.gov.co/jupgrade/images/stories/docs/varios/Politicas_de_Seguridad_Act.pdf

DTIC-ESPOCH. (20 de 06 de 2020). *dtic.espoch.edu.ec.* Obtenido de dtic.espoch.edu.ec: http://dtic.espoch.edu.ec/images/oasis/resolucion.pdf?fbclid=IwAR0V1cQr6LxVtVI9Hlg8xzMFq9U_0QQIr9IdlXkhtppdMgUKQWS5BBfuNlM

EducaAragon. (07 de 06 de 2020). *e-ducativa.catedu.es*. Obtenido de e-ducativa.catedu.es: http://e-ducativa.catedu.es/44700165/aula/archivos/repositorio/1000/1063/html/31_polticas_de_seguridad.html

Escrivá Gascó, G., Romero Serrano, R., Ramada, D. J., & Onrubia Pérez, R. (2013). *Seguridad Informática.* España: MACMILLAN.

Eset. (28 de 05 de 2020). *www.eset.com.* Obtenido de www.eset.com: https://www.eset.com/es/caracteristicas/antivirus-software-que-es/#

Firewalls Hardware. (22 de 06 de 2020). *firewalls-hardware.com*. Obtenido de firewalls-hardware.com: https://firewalls-hardware.com/utm-gestion-unificada-amenazas-unified-threat-management/

FORTINET. (25 de 09 de 2020). *www.fortinet.com.* Obtenido de www.fortinet.com: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_300E.pdf

Gartner. (24 de 11 de 2020). *www.gartner.com*. Obtenido de www.gartner.com: https://www.gartner.com/reviews/market/network-firewalls/compare/product/checkpointsoftwaretechnologies-generation-firewall-vs-firepower-vs-fortigate-next-generation-firewall-ngfw

Gartner. (04 de 10 de 2020). *www.gartner.com*. Obtenido de www.gartner.com: https://www.gartner.com/reviews/market/network-firewalls/compare/check-point-software-tech-vs-cisco-vs-fortinet

GARTNER. (24 de 11 de 2020). *www.gartner.com*. Obtenido de www.gartner.com: https://www.gartner.com/doc/reprints?id=1-24KX0CRD&ct=201111&st=sb

Goujon, A. (21 de 06 de 2020). *www.welivesecurity.com*. Obtenido de www.welivesecurity.com: https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

Guitérrez Salazar, P. (2019). *HACKER'S WHITE BOOK.* Monterrey: Edición White Suit Hacking.

Haber, M., & HIbbert, B. (2018). *Asset Attack Vectors: Building Effective Vulnerability Management Strategies to Protect Organizations.* New York: Apress.

Hackingloops. (30 de 07 de 2020). *www.hackingloops.com*. Obtenido de www.hackingloops.com: https://www.hackingloops.com/legion-framework/

Hertzog, R., O'Gorman, J., & Aharoni, M. (2017). *Kali Linux Revealed Mastering the Penetration Testing Distribution.* USA: Offsec Press.

Infotecs. (21 de 06 de 2020). *infotecs.mx*. Obtenido de infotecs.mx: https://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html

Infotecs. (22 de 06 de 2020). *infotecs.mx*. Obtenido de infotecs.mx: https://infotecs.mx/blog/ips-sistema-de-prevencion-de-intrusos.html

Koret, J., & Bachaalany, E. (2015). *The Antivirus Hacker's Handbook.* Indianapolis: John Wiley & Sons, Inc.

Kou, J. (2019). *Hacking: The Practical Guide to Become a Hacker | Field Manual for Ethical Hacker | Including Ethical Hacking with Kali Linux.*

Maurushat, A. (2019). *Ethical Hacking.* Canada: Gauvin Press.

Messier, R. (2018). *Leraning Kali Linux Security Testing, Penetration Testing, and Ethical Hacking.* Sebastopol: O'Reilly Media.

Misfud, E. (07 de 06 de 2020). *recursostic.educacion.es*. Obtenido de recursostic.educacion.es: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=4

Moes, T. (22 de 06 de 2020). *softwarelab.org*. Obtenido de softwarelab.org: https://softwarelab.org/es/que-es-un-antivirus/

Pandasecurity. (28 de 05 de 2020). *www.pandasecurity.com*. Obtenido de www.pandasecurity.com: https://www.pandasecurity.com/es/enterprise/solutions/security-appliances/ips/

Rahalkar, S. (2019). *Quick Start Guide to Penetration Testing: With NMAP, OpenVAS and Metasploit.* California : Apress.

Redacción APD. (20 de 06 de 2020). *www.apd.es*. Obtenido de www.apd.es: https://www.apd.es/tipos-de-seguridad-informatica/

Rodríguez, A. (22 de 06 de 2020). *es.godaddy.com*. Obtenido de es.godaddy.com: https://es.godaddy.com/blog/que-es-un-honeypot-y-como-usarlo-en-beneficio-de-tu-negocio/

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., . . . Castillo, M. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Alicante: 3ciencias.

Salazar Gualoto, R. C. (29 de 06 de 2020). *ESTUDIO PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL INFORMÁTICA PARA EL LABORATORIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DE LA FACULTAD DE INGENIERÍA DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR.* Quito.

Siemlab. (28 de 05 de 2020). *siemlab.com*. Obtenido de siemlab.com: https://siemlab.com/que-es-un-ids-intrusion-detection-system/

Singh, G. (2019). *Learn Kali Linux 2019: Perform Powerful Penetration Testing Using Kali Linux, Metasploit, Nessus, Nmap, And Wireshark.* Birmingham: Packt Publishing.

Softwarelab. (28 de 05 de 2020). *softwarelab.org.* Obtenido de softwarelab.org: https://softwarelab.org/es/que-es-un-antivirus/

Triviño Mosquera, I. (2019). *Seguridad y Alta Disponibilidad.* Madrid, España: Sintesis.

T-Systems. (28 de 05 de 2020). *www.t-systemsblog.es*. Obtenido de www.t-systemsblog.es: https://www.t-systemsblog.es/que-es-un-honeypot/

Welivesecurity. (28 de 05 de 2020). *www.welivesecurity.com*. Obtenido de www.welivesecurity.com: https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

GLOSARIO

Criptografía es la práctica y estudio de las técnicas que se utilizan para establecer una comunicación segura. (Guitérrez Salazar, 2019, pág. 93)

Hacker se refiere al termino usado para definir a un experto en ciberseguridad capaz de resolver problemas de tecnología y seguridad en diferentes contextos (Guitérrez Salazar, 2019, pág. 54)

Gartner es una empresa consultora que realiza investigación de productos y proveedores de tecnologías de la información

Host Bastion es una aplicación que se localiza en un servidor con el fin de ofrecer seguridad a la red interna

Ingeniería Social este término se refiere a la metodología no – técnica de manipular a las personas para llegar a un objetivo. (Guitérrez Salazar, 2019, pág. 71)

IP de las siglas en ingles Internet Protocol es una etiqueta numérica que se le asigna a todo sistema para comunicarse por este protocolo de internet y además sirve para identificar la red (Guitérrez Salazar, 2019, pág. 44)

ISP del inglés Internet Service Provider es el término que se refiere a las empresas que brindan el servicio de internet a los clientes

Malware o software malicioso comúnmente conocido como virus, se refiere a cualquier software no deseado o no autorizado que fue diseñado para tener intención maliciosa en un recurso. (Haber & HIbbert, 2018, pág. 13)

NEBS Network Equipment Building Standards es el conjunto más común de pautas de diseño ambiental, espacial y de seguridad aplicadas a los equipos de telecomunicaciones en los Estados Unidos (CISCO, 2020)

NGFW siglas en ingles que significa firewall de nueva generación son una herramienta fundamental para proteger a cualquier organización frente a las amenazas procedentes de internet. (Cortes, 2020, pág. 4).

NVT de las siglas en ingles Network Vulnerability Tests que significa pruebas de vulnerabilidades de la red son rutinas que comprueban la presencia de un problema de seguridad especifico o potencial en los sistemas. (Rahalkar, 2019)

Perímetro es la frontera fortificada de la red (Abad Domingo, 2018, pág. 139)

ROI siglas del término retorno de la inversión es una métrica para determinar la ganancia de una empresa a través de sus inversiones

SSL Secure Socket Layer un protocolo criptográfico que proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía

TLS Transport Layer Security es la evolución de SSL, un protocolo mediante el cual se establece una conexión segura por medio de un canal cifrado entre el cliente y servidor.

VMDK es un formato de archivo para almacenaje de un disco duro virtual (Guitérrez Salazar, 2019, pág. 101)

ANEXOS

Anexo 1

Escaneo inicial de la red externa puceing.edu.ec del LTIC mediante Nessus Profesional

Archivo testouceing_2x94dw.html

Anexo 2

Escaneo inicial de la red interna del LTIC mediante Nessus Profesional

Archivo scan_advanced_test_rwvfky.html

Anexo 3

Datasheet (Ficha Técnica) de Firewall de Nueva Generación Check Point Quantum 6600

Archivo 6600-security-gateway-datasheet.pdf

Anexo 4

Datasheet (Ficha Técnica) de Firewall de Nueva Generación Cisco Firepower 2130

Archivo datasheet-c78-742473.pdf

Anexo 5

Datasheet (Ficha Técnica) de Firewall de Nueva Generación Fortinet Fortigate 300E

Archivo FortiGate_300E.pdf

Anexo 6

Propuesta de Política de seguridad Informática para el LTIC

Archivo POLÍTICA DE SEGURIDAD INFORMÁTICA LTIC.docx

Anexo 7

Escaneo final de la red externa puceing.edu.ec del LTIC – CPH-R81 mediante Nessus Profesional

Archivo RedExternaP__ibwulh.html

Anexo 8

Escaneo final de la red interna del LTIC – CPH-R81 mediante Nessus Profesional

Archivo redinterna_3_4jjjha.html

Anexo 9

Sitio Oficial de descarga de Check Point Gaia R81

https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=109064

Anexo 10

Instalación y Configuración de la Plataforma de Seguridad Cibernética Check Point Gaia R81

Archivo INSTALACIÓN Y CONFIGURACIÓN DE CHECK POINT GAIA R81.docx