Implementación de un sistema de control y seguridad Informático ENDIAN FIREWALL

Implementación de un sistema de control y seguridad Informático ENDIAN FIREWALL

Daniel Eduardo Zapata Escobar[1]
Ignacio León Gómez Tangarife[2]
Jhon Darwin Acevedo Munera[3]
Christian Hernán Obando Ibarra[4]
David Alberto García Arango[5]

DOI: https://doi.org/10.26495/icti.v10i1.2401

Resumen

La tecnología avanza aceleradamente siendo primordial éste mismo ritmo para la seguridad informática, adaptándose fácilmente a las necesidades de las empresas, incluso a las que no poseen sistemas de seguridad que ejecutan planes de mejoras. De lo anterior, es clave la implementación de un firewall que prevenga posibles ataques incrementando eficiencia y eficacia de todo el personal en sus labores diarias; permitiéndoles interactuar con el sistema de forma sencilla y segura. Reducir riesgos y vulnerabilidades en una empresa conlleva cambios importantes orientando los procesos internos y creando mecanismos de seguridad únicos centralizados estableciendo niveles óptimos de confianza, por ello en este artículo se presenta la forma en que se llevó a cabo el mejoramiento de control, protección de la navegación y la activación de características en la plataforma de Seguridad de una empresa, permitiendo generar medidas de defensa frente a HTTP/FTP, Filtro de Contenido web, Antimalware, VPN SSL, IDS. La herramienta de seguridad y control es un sistema único open source, específicamente estructurado y capaz de brindar soluciones óptimas a la red de datos, creando un vínculo estrecho entre los empleados y la seguridad informática, siendo responsabilidad de todos. Finalmente, se validaron los beneficios para la instalación del dispositivo de seguridad perimetral en donde confluyen diferentes servicios informáticos, estableciendo políticas de contenido para navegación interna de usuarios y personal externo, cumpliendo estándares de buenas prácticas, fortaleciendo la seguridad en su red, evitando la pérdida de información y el mal uso de las herramientas por parte de los usuarios.

Palabras clave: Seguridad Informática, Firewall, Seguridad Perimetral, Endian Firewall, Buenas prácticas.

[1] *Corporación Universitaria Americana, Medellín, Colombia, zapatadaniel1016@americana.edu.co,* https://orcid.org/0009-0004-4126-3576
[2] *Corporación Universitaria Americana, Medellín, Colombia, gomezignacio2539@americana.edu.co,* https://orcid.org/0009-0003-8837-5607
[3] *Corporación Universitaria Americana, Medellín, Colombia, acevedojhon6089@americana.edu.co,* https://orcid.org/0009-0008-6186-0780
[4] *Corporación Universitaria Americana, Medellín, Colombia, cobando@americana.edu.co,* https://orcid.org/0000-0003-2326-8934
[5] *Corporación Universitaria Americana, Medellín, Colombia, dagarcia@coruniamericana.edu.co,* https://orcid.org/0000-0002-0031-4275

Abstract

Technology advances rapidly, being essential to maintain the same pace for cybersecurity, easily adapting to the needs of companies, even those that do not have security systems that execute improvement plans. From the above, the implementation of a firewall that prevents possible attacks is key, increasing efficiency and effectiveness of all personnel in their daily work; allowing them to interact with the system in a simple and secure way. Reducing risks and vulnerabilities in a company involves important changes that orient internal processes and create unique centralized security mechanisms establishing optimal levels of trust. Therefore, this article presents the way in which the improvement of control, navigation protection and activation of features in the Security platform of a company was carried out, allowing the generation of defense measures against HTTP/FTP, Web Content Filter, Antimalware, SSL VPN, IDS. The security and control tool is a unique open-source system, specifically structured and capable of providing optimal solutions to the data network, creating a close link between employees and cybersecurity, being everyone's responsibility. Finally, the benefits for the installation of the perimeter security device were validated where different IT services converge, establishing content policies for internal user navigation and external personnel, complying with good practice standards, strengthening security in their network, avoiding information loss and misuse of tools by users.

Keywords: Computer Security, Firewall, Perimeter Security, Endian Firewall, Good practices.

1. INTRODUCCIÓN

De acuerdo con las investigaciones en temas de seguridad de la información, hoy en día se han hecho diferentes dispositivos y componentes que ayudan a implementar controles para empresas, el cual hacen posible crear un marco donde se involucran herramientas como control de acceso, detección de intrusos, reglas de acceso, Antimalware entre otros; para empezar es necesario tener claro que una Red de Computadoras, también llamada red de ordenadores o red informática es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.), servicios (acceso a internet, e-mail, chat, juegos), etc. (Ed, 2004), así pues todos los servicios de una empresa van a través de la Internet y ésta no es una red de ordenadores, es una red de redes, un concepto bastante diferente.

Lo que caracteriza a todas estas redes es que utilizan un conjunto de protocolos denominado TCP/IP para comunicarse entre sí y que, libremente, deciden conectarse entre ellas y compartir recursos y, sobre todo, información (Adell, 1994), es conveniente destacar las 5 características de un sistema seguro pero antes mencionar que la Seguridad Informática es una disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable (López, 2010); en primer lugar la Disponibilidad el cual indica que en todo momento se tenga acceso a la información cuando se requiere, teniendo en cuenta la privacidad así evitar "caídas" del sistema que permitan accesos ilegítimos (Pablo Freire, 2016), en segundo Confidencialidad en la cual la información accesible es solo para personal autentico dado que la información no debe llegar a personas o entidades que no estén autorizadas (Pablo Freire, 2016).

Integridad trata sobre la información correcta sin modificaciones no autorizadas ni errores, ésta se protege frente a vulnerabilidades externas o posibles errores humanos (Pablo Freire, 2016), en cuarto Autenticación en ella la información procedente de un usuario que es quien dice ser al ser verificada y se debe garantizar que el origen de los datos es correcto (Pablo Freire, 2016), en quinto

Irrefutabilidad (No-Rechazo o No Repudio) el uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción (Pablo Freire, 2016), todos con la finalidad de proteger la información así mismo como la Seguridad Perimetral informática no deja de tener el mismo significado que la Seguridad Informática de hecho, también son todos los sistemas destinados a proteger de intrusos el perímetro.

La única diferencia es que, en lugar de un espacio físico, se protegen las redes privadas del sistema informático haciendo un enfoque a profundidad en Seguridad Perimetral, por ejemplo, la seguridad en el exterior de un recinto donde se va a situar el sistema de seguridad. Esta misma intenta detectar algún tipo de actividad sospechosa en una zona delimitada del exterior de un recinto, y proponen el desarrollo de un Sistema de seguridad perimetral inteligente (Morales, 2020), por el contrario a ésta los Virus informáticos son pequeños programas diseñados para instalarse y ejecutarse en un ordenador sin permiso del usuario y habitualmente, con "mala intención" con las funciones de propagarse, defenderse y realizar alguna acción (inocua/dañina), suelen permanecer inactivos algún tiempo para propagarse sin ser detectados (Prieto, 2002), sin embargo, existe Antimalware que es una herramienta fundamental para proteger nuestros sistemas y equipos de cómputo.

El Antimalware realiza un escaneo de archivos que tiene como objetivo la detección, identificación y eliminación de aplicaciones maliciosas o malware (Padilla Espinosa, 2010)**,** por el nombre de Código Maliciosos (Malware) son programas que causan algún tipo de daño o anomalía en el sistema informático, dentro de esta categoría se incluyen los programas troyanos, gusanos, virus informáticos, spyware, backdoors, rootkits, keyloggers, entre otros (Mieres, 2009); ahora bien, en pro de la seguridad informática dos puntos vitales se mencionarán a continuación el termino de VPN el cual permite extenderse a la red local sobre una red pública o una red no controlada, entre los aspectos fundamentales que toda VPN debe tener presente la seguridad, integridad y confidencialidad de la información además del valor agregado que representan al ser fáciles de usar (Jiménez Cely, 2014) y el termino de Firewall que es una herramienta o sistema de información que controla el acceso y el flujo de tráfico de red, que además impide el acceso no autorizado a un computador o a una red de computadores desde otra red que pretende realizar una intrusión, esta herramienta niega o permite que desde otra red se establezca una conexión o no se logre, la importancia de esta radica en que a través de su uso se autorice, detecte o se re-direccione una conexión sin informar al emisor (Forero Gandur, 2015).

En función de lo planteado ENDIAN – FIREWALL es una herramienta de distribución OpenSource de Linux, desarrollada para actuar no solamente como cortafuegos sino como solución integral para proteger su red de amenazas externas ofreciendo la mayoría de servicios que brinda un UTM (Gestión Unificada de Amenazas) fácil de usar e instalar, también cuenta con características especiales permitiendo configurar proxys, canales VPN, enrutadores, filtrado de datos, herramientas Antimalware y anti spam (Quasar Software, 2014 -2015), así brinda gran cantidad de soluciones que ayuda a implementar los respectivos controles en una red de datos por tal motivo se realizará montaje y configuración del ENDIAN FIREWALL para la empresa AM MENSAJES S.A.S., en ultima instancia al personal de la empresa contará con capacitaciones y Buenas prácticas las cuales hacen referencia a una colección de recomendaciones que vienen del mundo profesional y que suscitan un consenso en un dominio dado y están encaminadas al mejor rendimiento y efectividad. (Jean-Luc, 2016)

2. METODOLOGIA

El proyecto se desarrolló utilizando tecnologías existentes en el mercado como los es Firewall con IPS, Antimalware, Conexiones VPN, y otros componentes de seguridad que se pueda brindar en la misma solución. En donde se evaluaron las diferentes opciones que permiten cubrir la mayoría de posibles puntos de ataque, a los cuales la mayoría de las empresas se ven expuestas, de esta forma se podrán basar para un análisis, costos, escalabilidad de la solución para futuras implementaciones.

Es posible basarse en metodologías que incorporen modelos investigativos que nos puedan llevar a mitigar problemas al momento de implementar soluciones y/o políticas de seguridad en una empresa, sirviendo como ejemplo real al ser implementado en la empresa AM MENSAJES S.A.S., de la misma forma para futuras investigaciones se acude al instrumento de la observación, el cual aportará conocimientos al área de seguridad informática en la protección de datos y el uso y mejores prácticas para dicho tema.

Validando otros trabajo e implementaciones de sistemas de seguridad, se Indica "Actualmente, las empresas cada vez son más dependientes de sus propias redes informáticas y por un problema, por pequeño que sea y les afecte puede llegar a interrumpir las operaciones que se realicen en dicha organización" (García Parada et al., 2015).

Es por ello, que es de mucha importancia abordar el tema de seguridad en las redes ya que un fallo en ellas puede resultar muy costoso en productividad, eficiencia, pérdida de datos confidenciales e información valiosa y para proteger tal información de dichas organizaciones es recomendable el uso de dispositivos de Hardware o software que ayuden a detectar vulnerabilidades y riesgos que puedan surgir en dicha red y también de esta manera poder minimizar los mismos. (Cruz y Molina, 2010).

En su totalidad las empresas de seguridad informática sugieren que toda red necesita para su correcto funcionamiento uno o varios equipos que hagan las veces de firewall y router, y así para poder cubrir este aspecto existen soluciones robustas y de gran envergadura donde sus costos de licenciamiento son muy altos para empresas como AM MENSAJES S.A.S. que es una pyme, "además que la función a instalar es limitada y se compra modulo por modulo, en donde entrar a recomendar así pfsense, ENDIAN FIREWALL y FreeBSD; lo considera el sistema operativo más seguro del mundo, además es open source (Código Abierto). SOPHOS ofrece la gestión y supervisión de forma centralizada de sus dispositivos, en el cual encuentras supervisión en tiempo real, configuración centralizada, gestión, informes y se puede probar la herramienta por 30 días con licencia gratuita". (Obando y Torres, 2017) .

Otra de las investigaciones realizadas en la universidad de San Buenaventura Medellín en su artículo Solución Integral de Seguridad para las PYMES mediante un UTM (Caselles, 2017), se enfoca en una solución modular que integre las funciones más comunes requeridas en una política de seguridad informática, la cual incluya firewall, Antimalware, control de contenido, que contrarreste los diferentes tipos de amenazas y ataques a los que se ven expuestas las pequeñas y medianas empresas.

Durante la marcha de la investigación se encontró las diferentes posibilidades de hacer la implementación del Firewall tanto físico (Hardware) como lógico (Software) (Ortiz, 2020) se realiza revisión y en cuanto los Firewall Físico (Pagos) se descubre un ranking de los mejores 5 Firewall para pequeñas empresas (Totalplay Empresas, 2019):

1) Cortafuegos de seguridad SonicWall TZ400
2) FortiGate 30E
3) Cisco Meraki MX64W
4) Dispositivo Protectli Firewall con 4 puertos Intel Gigabit
5) WatchGuard Firebox T15

En Firewall Lógicos (Gratuitos) se detectan 3 para pequeñas empresas (Root Solutions, 2017):

1. Endian Firewall
2. Pfsense
3. Opnsense

Luego de revisar costo - beneficio y ajustándose al presupuesto de la empresa se determinó que el ENDIAN FIREWALL es el mejor instrumento para utilizar en el mejoramiento de la seguridad en la empresa AM MENSAJES S.A.S cumpliendo con las expectativas del cliente no solamente como cortafuegos sino como solución integral para proteger su red de datos ante amenazas externas, ofreciendo todos los servicios (Ver 13.1 MENU ESTADO. pág. 72) que brindará la plataforma de Gestión Unificada contra Amenazas (Netnovation, 2019).

La investigación, de enfoque mixto se tuvo su enfoque en aumentar la seguridad en un 70% en la empresa AM MENSAJES S.A.S. de tal manera que los niveles de protección aumentaron al implementar ENDIAN FIREWALL y al ampliar los conocimientos de los empleados con capacitaciones, buenas prácticas en el uso adecuado de internet se logró maximizar la efectividad en el sistema de seguridad con tranquilidad, teniendo como resultado la reducción de debilidades que presenta la empresa; basándonos en dicha herramienta configurando el sistema HTTP/FTP, Filtro de Contenido web, Antimalware, VPN SSL, IDS.

En términos operativos del método se destacan los fundamentos de Concebir, Diseñar, Implementar y Operar productos, procesos y sistemas, el cual requiere de un aprendizaje activo que resulta muy beneficioso en el área de Seguridad Informática ya que esta área permite analizar, diseñar, programar e implementar un sistema de seguridad perimetral con software de calidad libre para minimizar los costos en forma adecuada cumpliendo con los requisitos del cliente y usuario final.

Etapas

En términos generales el proyecto constara en 4 fases:

Fase 1

Fase exploratoria de la implementación conformada en la teoría, contextualización, mediante la búsqueda y recopilación de la información importante llevando a cabo el análisis, interpretación y clasificación de esta.

Fase 2

Seguridad entrante y saliente de la información mediante un sistema de seguridad.

Levantamiento de la información, identificando los riesgos que la empresa está expuesta con los activos de la información, los procesos y operación, factores críticos de éxito.

Fase 3

Modelo de administración mediante, control y organización de los datos en la red, basados en subprocesos (sistema, estado, red y registros del ENDIAN FIREWALL) de toda la información que pasa a través de la red.

Documentar todo el sistema de manejo de las redes mediante el ENDIAN FIREWALL que permita tener un nivel de control y organización para la administración de la red.

Fase 4

Mejorar el rendimiento de los equipos y de la red, mediante el acceso y no acceso a internet a los usuarios de la empresa, según el área en que se desempeñan.

3. RESULTADOS

Características

"Las características incluyen un firewall de inspección de paquetes, proxys a nivel de aplicación para los distintos protocolos (HTTP, FTP, POP3, SMTP) con el apoyo de Antimalware, virus y spamfiltering para el tráfico de correo electrónico (POP y SMTP), filtrado de contenido de tráfico Web y una molestia" libre "solución VPN (basada en OpenVPN). La principal ventaja de ENDIAN FIREWALL es que es "Open Source" solución que está patrocinado por Endian.

Plataforma de seguridad Integral

ENDIAN FIREWALL es un Appliancie de Seguridad Integral que protege su red y mejora la conectividad, ofreciendo todos los servicios que necesita y más, seguros y fácil de configurar.

ENDIAN FIREWALL es 100% open source e incluye, entre sus funciones principales, una variedad de características:

- Firewall con inspección de estados.
- HTTP/FTP.
- Filtro de Contenido Web, Antimalware POP3/SMTP y Antispam.
- VPN SSL.
- IDS.

Seguridad Web

El filtro de contenidos de ENDIAN FIREWALL mantiene una experiencia de navegación web de forma segura, protegiendo contra virus y contenidos no deseados como violencia, pornografía o software pirata. Permite al administrador de la red monitorizar accesos, mejorando así la productividad. También es útil en aquellas compañías que buscan que sus empleados naveguen solo por sitios bien definidos, asegurando así la integridad de los negocios y un uso adecuado de los recursos. (ITM, 2016)

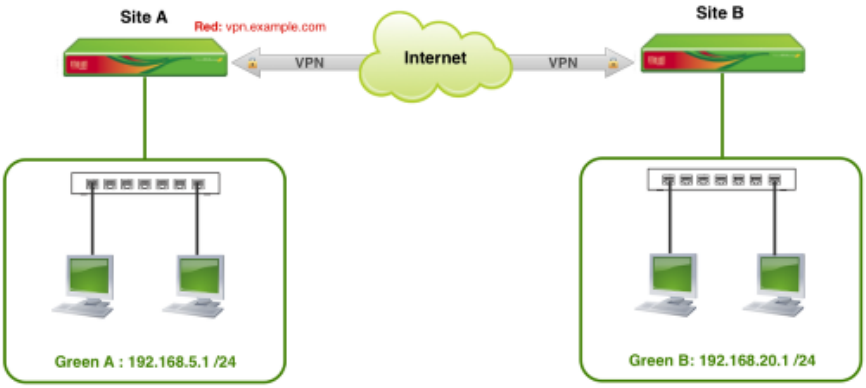

Figura 1. Filtro de contenidos.
Fuente: ITM (2016)

VPNs fáciles y rápidas

Gracias a OpenVPN, se puede rápidamente y sin complicaciones levantar un túnel seguro encriptado con SSL entre sucursales de tu compañía o entre agentes remotos hacia la red corporativa de la Empresa. Los clientes soportados abarcan una gran cantidad de Sistemas Operativos como lo son Linux, Mac OSX o Windows.

Como proyección de minimizar el problema que se tiene de acceso, se procederá con:

- Definir roles y políticas a empleados como también para los usuarios externos o invitados que dentro de la organización requiera acceso de internet como para entrada y/o salida de red.
- Se brindarán las respectivas capacitaciones al personal administrativo, operativo y gerencial de la empresa para socializar las políticas de implementación y sus riesgos que mitigamos con ello.

Instalación FIREWALL ENDIAN

Se realiza la instalación del ENDIAN FIREWALL en la infraestructura propia del cliente AM MENSAJES S.A.S el equipo para la instalación fue aprovisionado por el cliente de unos equipos que se tenían si utilizar en bodega.

La instalación del sistema lo podemos ver en anexos desde pagina 76 a página 126 con figuración inicial y adecuación del sistema a las necesidades propias del cliente

Mejoramiento red de datos

Luego de la implementación del sistema ENDIAN FIREWALL, se puede evidenciar en el siguiente esquema de red como se configuro dicho dispositivo en la empresa AM MENSAJES S.A.S., el filtrado de contenido en la entrada y salida de tráfico desde y hacia internet.

Se seguirá manejando el direccionamiento de red que se tiene ya instalado en la empresa (192.168.1.0 / 24) para un total de 254 equipos más que suficiente para la cantidad de equipos que tiene la empresa, ver figura 5.

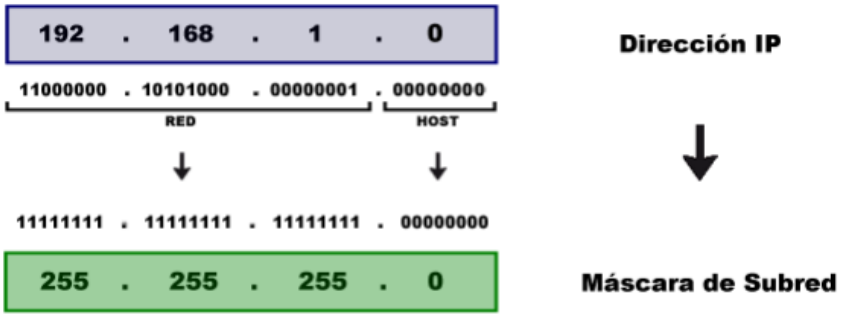

Figura 2. **Relación de mascara de subred con dirección IP.**
Fuente: Morató (2013)

El ENDIAN FIREWALL se le asignado la dirección IP 192.168.1.254 como Gateway por defecto para toda la red de AM MENSAJES S.A. Ver Anexo "12.16 Configuración de Zonas", adicionalmente se realiza un cambio en el directorio activo de la empresa puesto que en el DNS del dominio ammensajes.com se tenía como Gateway 192.168.1.1 y se cambió por el 192.168.1.254.

Adicionalmente se realizó una mejora en el servicio DHCP del dominio ammensajes.com que está instalado en un Windows server 2016, se realiza mejora para que el servicio asigne direccionamiento automático el rango de direcciones IP son desde la 192.168.1.1 a la 192.168.1.50 reservadas para impresoras, Access Point, etc. Entre la dirección 192.168.1.51 a la 192.168.1.200 son direcciones que se asignan para estaciones de trabajo y equipos a utilizar la red de la empresa, la dirección 192.168.1.254 se reserva para que no sea asignada.

El ENDIAN FIREWALL se instaló un equipo DELL Core i5 5ta generación con 8 Gigas de ram, disco duro de 500 Gigas Sata, se instalaron 4 tarjetas de red, una tarjeta para la LAN interna, otra tarjeta para la WAN de internet y la 3 y 4 para contingencia de LAN y WAN, ver figura 6.

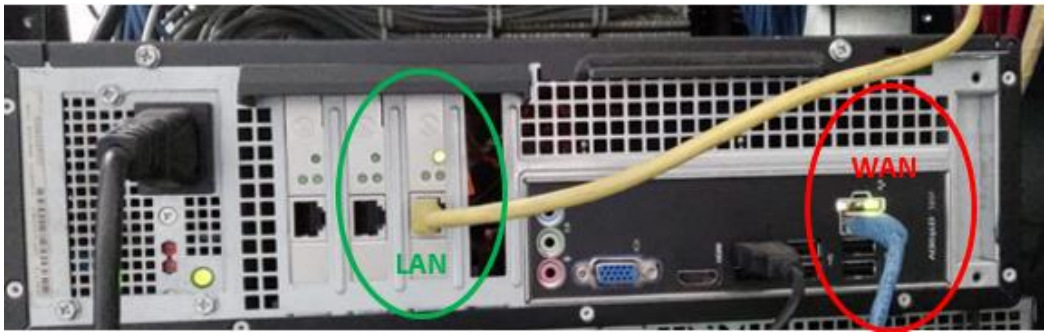

Figura 3. Infraestructura física.
Fuente: Elaboración propia**.**

El cable de red que sale del puerto LAN del ENDIAN FIREWALL va conectado al Switch principal en el puerto 44.

Conexión a internet desde el SW de TIGO UNE que es el proveedor del servicio con un canal de 60 Megas Puerto 1 del Switch de TIGO UNE, Ver figura 4.

Figura 4. Conexión a internet.
Fuente: elaboración propia**.**

Se debió hablar con el proveedor TIGO UNE para que realizara un cambio en el modo de conexión el cual es Bridge puesto que nosotros con el ENDIAN FIREWALL vamos a manejar la conexión y asegurarla por medio de este dispositivo.

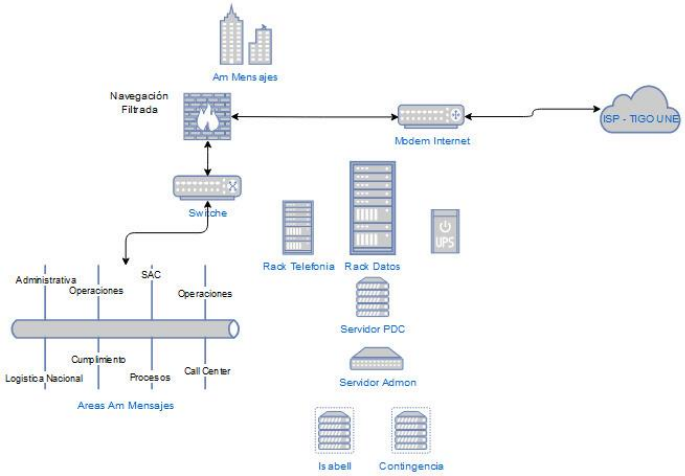

Figura 5. Arquitectura de la conexión.
Fuente: elaboración propia.

Esta distribución de ENDIAN FIREWALL 3.2.4 usa Squid (Es un software de servidor proxy y soporta protocolo HTTPS para establecer conexiones SSL seguras) para el filtrado de contenido de sitios web, cuenta además con un proxy HTTPS que permite filtrar sitios https no deseados, en donde por ejemplo se puede filtrar sitios como facebook.com, youtube.com y todos los sitios que sean catalogados como inseguros y/o de ocio de una manera muy eficiente.

A partir del año 2017 los certificados que utilizan el algoritmo de cifrado SHA-1 serán rechazados por Google como inseguros. Es necesario entonces modificar el certificado del proxy HTTPS a un certificado más seguro como SHA-256 o SHA-512. Este certificado es que se debe importar en los terminales para evitar el mensaje de alerta de certificado no válido, ver figura 6.

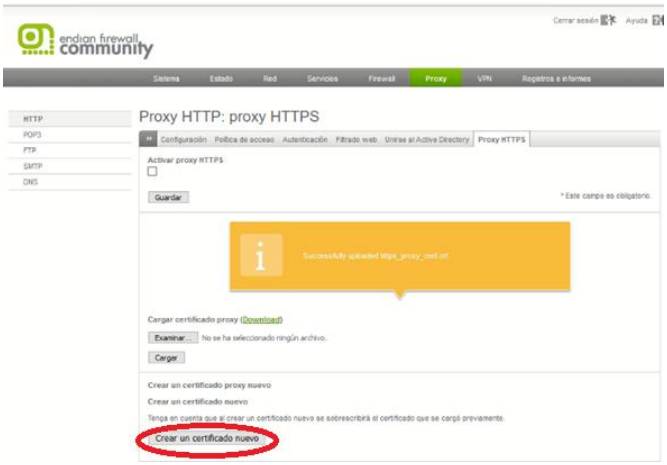

Figura 6. Modificación del certificado del proxy HTTPS.
Fuente: elaboración propia.

Dando clic en este icono da la posibilidad de crear dicho certificado propio de ENDIAN FIREWALL, Se adjunta imágenes de Información de certificado emitido, ver figura 7.

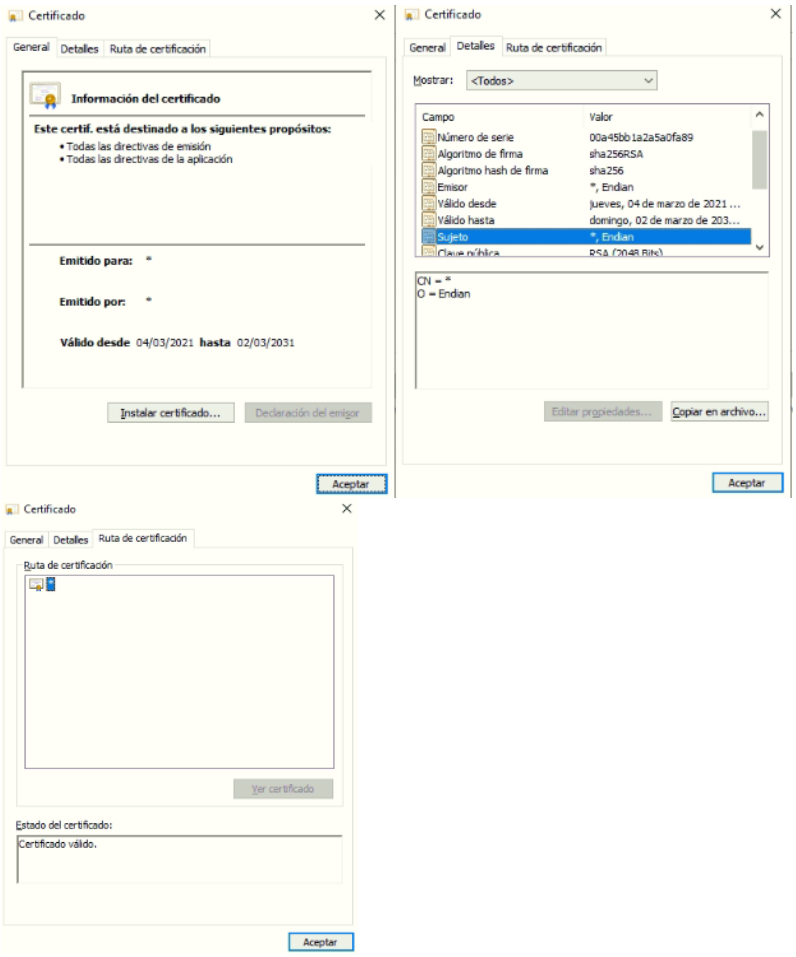

Figura 7. Certificado de ENDIAN FIREWALL.
Fuente: elaboración propia

Una vez realizado la creación del certificado debemos realizar la importación en el mismo ENDIAN FIREWALL, ver figura 8.

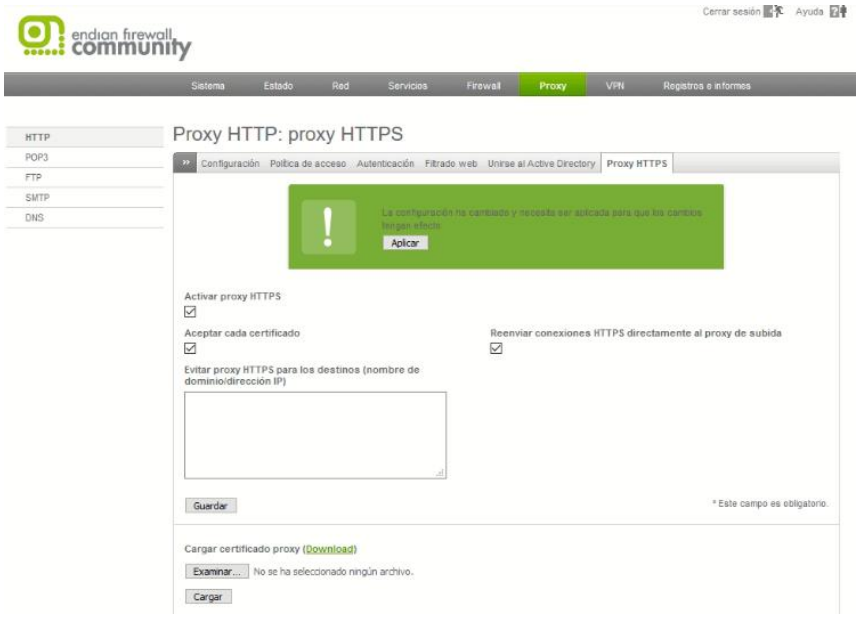

Figura 8. Importación.
Fuente: elaboración propia.

Se debe realiza el proceso de des habilitación de la navegación por el puerto 80, como se muestra a continuación, para que toda la navegación sea filtrada y monitoreada por el servicio de PROXY HTTPS, ver figura 9.

Figura 9. Deshabilitación de la navegación por el puerto 80.
Fuente: elaboración propia.

Se habilita en el Firewall => tráfico de Salida => Navegación por puertos seguros como se muestra a continuación, ver figura 10.

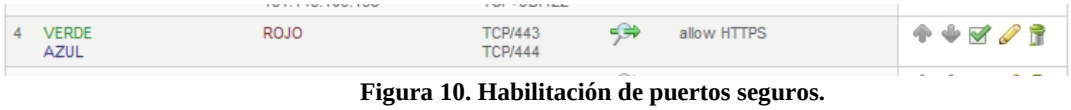

Figura 10. Habilitación de puertos seguros.
Fuente: elaboración propia.

Adicionalmente se debe validar que solo se tenga una salida para toda la navegación de la red y no se presenten navegación por otras puertas de navegación, en donde se realiza que el único servidor que puede consultar registros DNS sería el servidor 192.168.1.31 que este servidor es el servidor de dominio de AmMensajes.com, ver figura 11.

Figura 11. Tráfico de consulta de registros.
Fuente: elaboración propia**.**

En el servicio de Proxy => DNS => Anti-spyware => Debemos colocar en cada línea los dominios que deseamos bloquear, como se muestra en la imagen, ver figura 12.

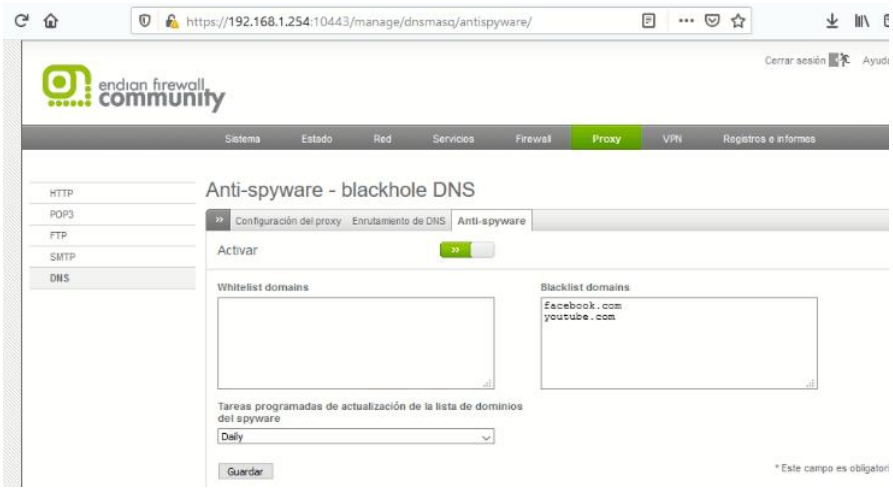

Figura 12. Bloqueo de dominios.
Fuente: elaboración propia.

Dominios propuestos para bloqueo

www.disneyplus.com
www.netflix.com
www.youtube.com
youtube.com
www.facebook.com
facebook.com
es-la.facebook.com
caracol.com.co
www.caracol.com.co
www.caracoltv.com
caracoltv.com
www.canalrcn.com
canalrcn.com
whatsapp.com

Filtrado de Contenido desde ENDIAN FIREWALL mantiene una vivencia de navegación web de forma Rsegura, controlando y protegiendo nuestra navegación de virus y contenidos NO deseados como lo son sitios de violencia, pornografía o software pirata. Permitiendo al administrador del firewall monitorear accesos, NO autorizados y mejorando así la productividad de todos y cada uno de los empleados. Buscando también que AM MENSAJES S.A.S. navegue solo por sitios definidos como seguros, asegurando con esto integridad de los recursos, ver figura 13.

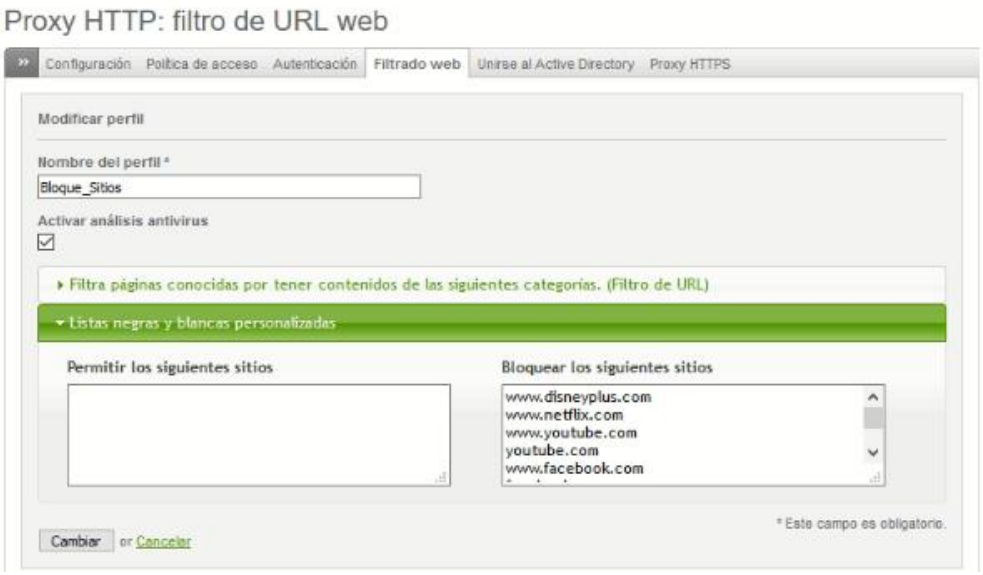

Figura 13. Permisos de sitios.
Fuente: elaboración propia.

Adicionalmente al bloqueo de los dominios indicados con anterioridad, se puede realizar bloqueo por categoría como se muestra a continuación

Categoría bloqueados desde el proxy, ver figura 14.

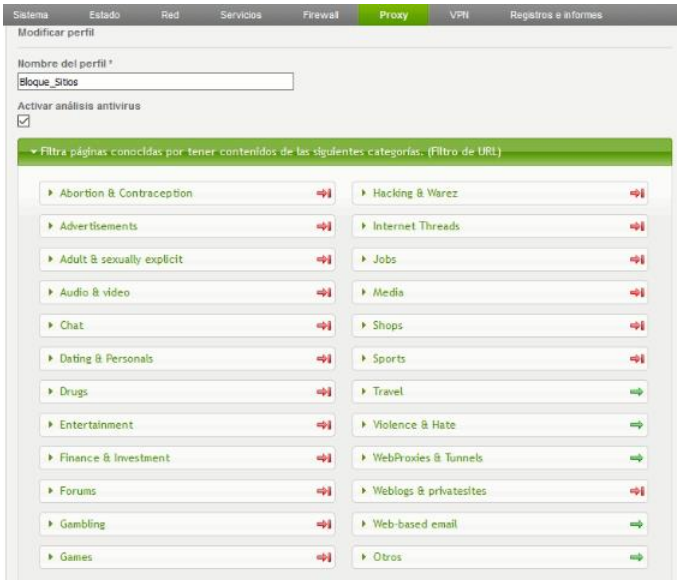

Figura 14. Categoría de bloqueos desde proxy.

Fuente: elaboración propia.

Filtrado de contenido como Política con dominio específico, también podemos realizar bloqueos por MIME types (Los MIME Types (Multipurpose Internet Mail Extensions) son la manera standard de mandar contenido a través de la red. Los tipos MIME especifican tipos de datos, como por ejemplo texto, imagen, audio, etc. que los archivos contienen. Recuerde que debe utilizar el sufijo correcto para este tipo de archivo), ver figura 14.

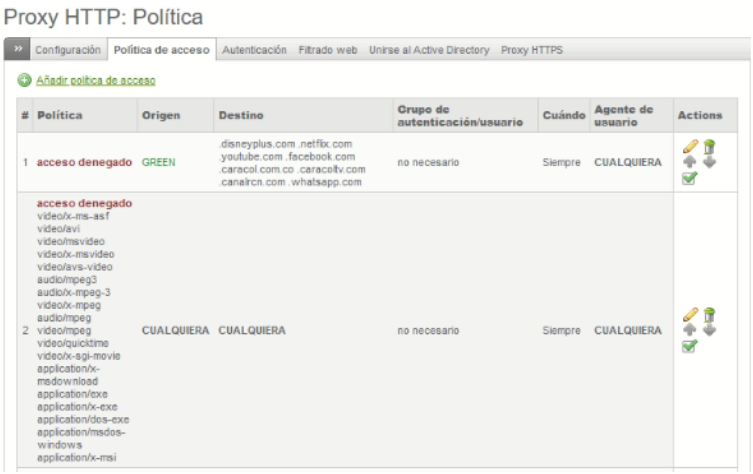

Figura 14. Política de Proxy.
Fuente: elaboración propia.

Filtrado de contenido con URL o por dominio, desde la maquina llamada Remoto1 con IP 192.168.1.137, ver figura 15.

Figura 15. Filtrado de contenido con URL.
Fuente: elaboración propia.

Navegación sin bloqueo al dominio de youtube.com, ver figura 16.

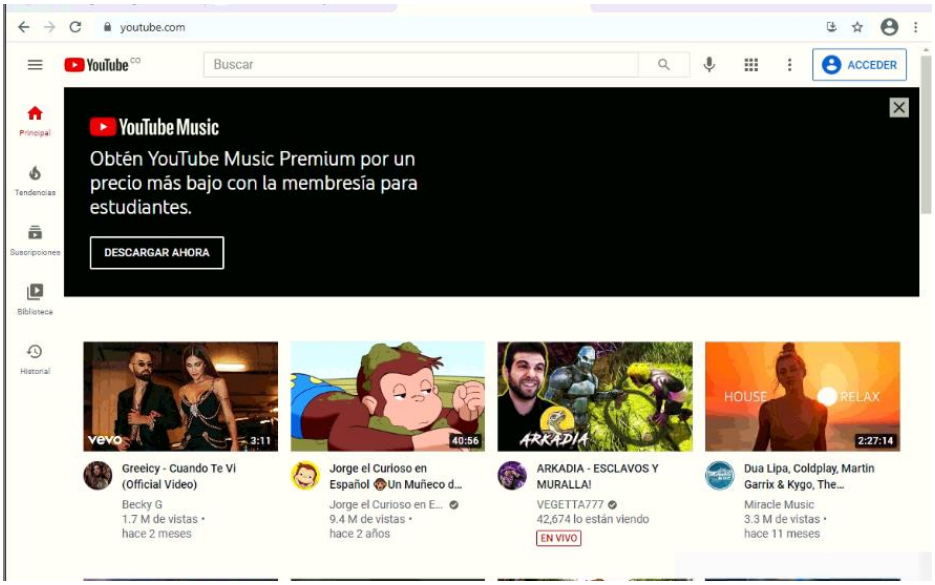

Figura 16. Navegación por Youtube.com sin bloqueo.
Fuente: elaboración propia.

Después de realizar el proceso de bloqueo del dominio de Youtube.com se obtiene la figura 17.

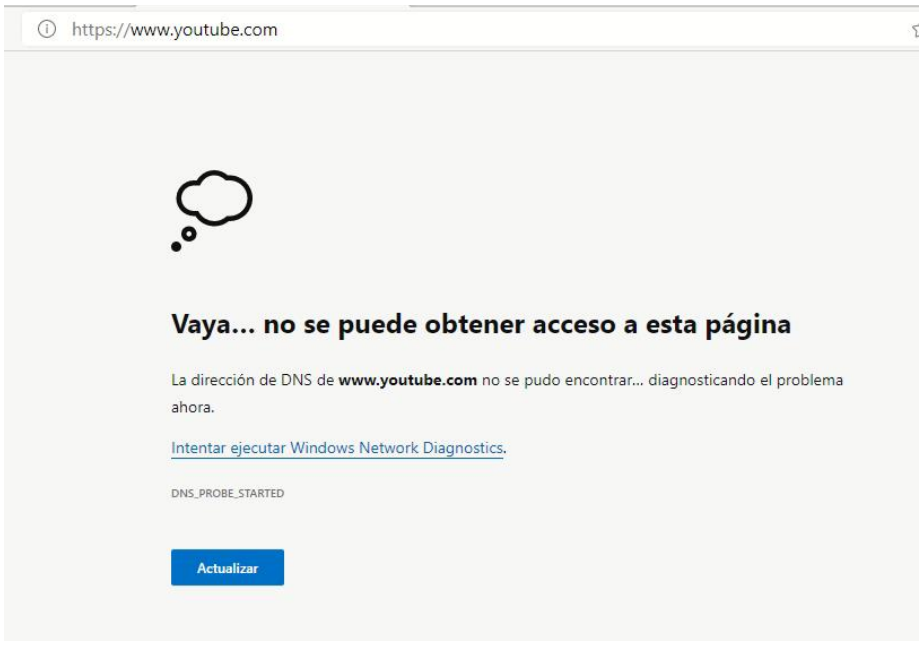

Figura 17. Bloqueo del dominio de Youtube.como.
Fuente: Diseño propio.

CONCLUSIONES

Este trabajo consistió en la implementación de una arquitectura empresarial de seguridad perimetral, en donde se establecieron políticas de seguridad documentadas con el fin de gestionar un plan de capacitaciones para el personal actual y para personal nuevo. Estas políticas son basadas en temas básicos y avanzados para ser utilizados en la empresa AM MENSAJES S.A.S, permitirán definir los comportamientos aceptables, la selección de las herramientas y procedimientos acordes a las necesidades de la empresa.

Al rediseñar una infraestructura creada hace más de 15 años por la empresa AM MENSAJES S.A. en donde el tema de seguridad perimetral no era importante para su operación diaria, el objetivo fundamental de este proyecto fue dar a conocer los conceptos básicos de seguridad perimetral, primero sentando unas bases teóricas, para posteriormente exponer las fases necesarias para la implantación adaptándonos a las necesidades de la empresa AM MENSAJES S.A., con el objetivo final de instalar un ENDIAN FIREWALL como sistema de seguridad perimetral, estableciendo niveles óptimos de seguridad.

En su trabajo diario los usuarios acceden a todo tipo de aplicaciones utilizando una amplia gama de dispositivos. Mientras tanto el crecimiento de los centros de datos en sitio y la virtualización, lleva a que la movilidad y las iniciativas basadas en la nube, están obligando a rediseñar los permisos de acceso de las aplicaciones sin afectar a la protección de la red.

Para cumplir con lo anterior se han identificado y se ha propuesto una arquitectura adaptable a la empresa a dichos requisitos y cumpliendo todo a nivel de seguridad perimetral.

La situación actual en temas de seguridad informática ha evolucionado a ritmos acelerados en la última década y el número de amenazas han crecido de una manera exponencial por ende el ENDIAN FIREWALL se convierte en algo imprescindible actualmente y a muy bajo costo.

REFERENCIAS

Adell, J. (1 de 12 de 1994). *La Internet: posibilidades y limitaciones. Jornada: La Comunidad Valenciana ante la Nueva Sociedad de la Información: Ciencia, tecnología y empresas. Valencia*. Obtenido de https://www.um.es/innova/OCW/diseno_y_evaluacion_materiales_didacticos/mpaz/utilidades/pdf/16.pdf

Alvarado Jaramillo, J. V. (2018). *mplementación de políticas de seguridad y control de navegación a través de un firewall basado en Linux para la Empresa Tributax Services SA.*http://repositorio.ug.edu.ec/handle/redug/36384

Arifin, F. M. (14 de 08 de 2017). *Implementation of Management and Network Security Using Endian UTM Firewall. IJAIT.* https://journals.telkomuniversity.ac.id/ijait/article/view/874

Bueno Rosales, J. J. (2013). *Sistema de control y seguridad endian Firewall para la empresa Frada Sport.* http://repositorio.uisrael.edu.ec/handle/47000/493

CASELLES, W. P. (29 de 06 de 2017). *DIFERENCIAS ENTRE UN FIREWALL UTM Y UN FIREWALL NGFW.* http://www.sugeek.co/firewall-utm-vs-ngfw

CRUZ, Y. R., y MOLINA, M. P. (2010). *Evolución, particularidades y carácter informacional de la toma de decisiones organizacionales.* http://www.acimed.sld.cu/index.php/acimed/article/view/6

Ed, T. (2004). *Redes de Computadoras.* Obtenido de http://files.compuaprendo.webnode.com.ar/200000031-1a6261b5cb/REDES%20DE%20COMPUTADORAS.doc

Elejalde, L. L. (25 de 02 de 2020). *Las nuevas modalidades de vishing, smishing y fishing con las que hacen fraude bancario*. Obtenido de https://www.larepublica.co/finanzas-personales/las-nuevas-modalidades-de-vishing-smishing-y-fishing-con-las-que-hacen-fraude-bancario-2969016

Forero Gandur, J. W. (17 de 07 de 2015). *Firewalls a la vanguardia* . http://repository.unipiloto.edu.co/handle/20.500.12277/2875

GARCÍA PARADA, N. R., INTERIANO RODRÍGUEZ, J. E., & RIVAS ELÍAS, J. I. (09 de 2015). *FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS.* TÉCNICO EN INGENIERÍA EN HARDWARE: http://biblioteca.utec.edu.sv/siab/virtual/tesis/88730.pdf

Guijarro Rodríguez, A. T. (Enero de 2018). *GUÍA DE PRÁCTICAS EN ENDIAN.* http://142.93.18.15:8080/jspui/handle/123456789/55

ITM. (2016). *Endian Firewall*. Obtenido de https://www.i-t-m.com/productos-servicios/seguridad/endian-firewall

Jean-Luc, B. (05 de 2016). *ITIL® V3: Entender el enfoque y adoptar las buenas prácticas. Ediciones ENI.* https://books.google.es/books?hl=es&lr=&id=5xmsQeWfQqoC&oi=fnd&pg=PA15&dq=que+son+buenas+practicas+informaticas&ots=nmr1Kp7jvt&sig=m_AWyDHOzkzYmr0e-iLv_paGEtc#v=onepage&q=que%20son%20buenas%20practicas%20informaticas&f=false

Jiménez Cely, R. (14 de 10 de 2014). *Seguridad en redes VPN.* http://repository.unipiloto.edu.co/handle/20.500.12277/2876

LESCANO DELGADO, M. L. (2015). *ESTUDIO DE FACTIBILIDAD PARA LA PROPUESTA "FRAMEWORK DE TRABAJO PARA PROYECTOSDE TITULACIÓN APLICANDO LA METODOLOGÍA SCRUM EN LA INGENIERÍA DESOFTWARE" ENFOCADO A INFRAESTUCTURA.* Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/11717/1/PTG-B-CISC%20916%20LESCANO%20DELGADO%20MARCOS%20LEONEL.pdf

López, P. A. (2010). *Seguridad informática.* Obtenido de https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=que+es+confidencialidad+informatica&ots=PrknXFEJW1&sig=mSstEzhnKpTjh2_Pz-UL0aV9SOQ#v=onepage&q=que%20es%20confidencialidad%20informatica&f=false

MATIAS, D. E. (2011). *PROPUESTA E IMPLEMENTACIÓN DE UN APPLIANCE DE SEGURIDAD A PARTIR DEL RE-USO TECNOLÓGICO.* https://repositorio.ucp.edu.co/bitstream/10785/929/1/CDMIST43.pdf

Mieres, J. (Enero de 2009). *Ataques informáticos. Debilidades de seguridad comúnmente explotadas.* https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

Molina, K. J. (02 de 12 de 2009). *Firewall–linux: Una solución de seguridad informática para pymes (pequeñas Y medianas empresas).* https://www.redalyc.org/pdf/5537/553756879003.pdf

Morales, F. T. (12 de 11 de 2020). *Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información.* https://www.researchgate.net/profile/Renato-Toasa/publication/339956501_Implementacion_de_un_sistema_de_seguridad_perimetral_como_estrategia_de_seguridad_de_la_informacion/links/5e95ffa5a6fdcca78915c13f/Implementacion-de-un-sistema-de-seguridad-perimetral

Morató, D. (2013). *Direccionamiento IP*. . Obtenido de Morató, D., & de Redes, L. D. P.

Netnovation. (10 de 04 de 2019). *Endian es una de las mejores soluciones y protección en red de amenazas*. Obtenido de https://www.netnovation.com/productos-y-servicios/endia-es-una-de-las-mejores-soluciones-y-proteccion-en-red-de-amenazas/

OBANDO, F. J., y TORRES, C. E. (2017). *IMPLANTACIÓN UN UTM BASADO EN SOFTWARE LIBRE PARA GESTIÓN DE.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/14344/94269897.pdf?sequence=1&isAllowed=y

Ortiz, A. E. (17 de 07 de 2020). *¿Cuales son los tipos de firewalls o cortafuegos que existen?* Obtenido de https://blog.hostdime.com.co/cuales-son-los-tipos-de-firewalls-o-cortafuegos-que-existen/

Padilla Espinosa, M. J. (04 de 01 de 2010). *Antivirus: Una herramienta indispensable para nuestra seguridad.* http://www.ru.tic.unam.mx:8080/handle/123456789/1719

Policia Nacional, Cisco, Fortniet, McAfee, Microsoft. (2019 -2020). *INFORME TENDENCIAS CIBERCRIMEN.* https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Prieto, A. L. (2002). *Introducción a la Informática.* http://elvex.ugr.es/decsai/JAVA/pdf/1A-intro.pdf

Quasar Software. (2014 -2015). *¿QUÉ ES ENDIAN?* https://quasarbi.com/endian.html

Root Solutions. (20 de 06 de 2017). *Tres Firewalls UTM (OpenSource) para tener encuenta*. https://www.rootsolutions.com.ar/tres-firewalls-utm-opensource-encuenta/

Totalplay Empresas. (14 de 11 de 2019). *Los 10 mejores firewalls de hardware para redes domésticas y de pequeñas empresas*. Obtenido de https://tpempresas.com/los-10-mejores-firewalls-de-hardware-para-redes-domesticas-y-de-pequenas-empresas-2019

Urbina, G. B. (2016). *Introducción a la seguridad informática.* https://books.google.es/books?hl=es&lr=lang_es&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=que+es+autenticacion+informatica&ots=0XLyaFAiLr&sig=bX2PLvMrYdxoexHgQ0I4nOjFLtk#v=onepage&q&f=false

Vieites, Á. G. (2011). *Enciclopedia de la seguridad informática.* Grupo Editorial RA-MA (Vol 6).

Zambrano, S. M. (30 de 01 de 2017). *Seguridad en informática: consideraciones.* https://dialnet.unirioja.es/servlet/articulo?codigo=6137824