PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERIA
MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES DE COMUNICACIONES

DISERTACIÓN PREVIA A LA OBTENCIÓN DE TÍTILO DE MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN REDES DE COMUNICACIONES

TEMA:

“ESTUDIO DE UN MODELO DE SEGURIDAD DE RED Y PROPUESTA DE MEJORAMIENTO DEL SISTEMA DE SEGURIDAD PERIMETRAL CASO DE ESTUDIO EMPRESA AKEA S.A.”

GEOVANNA STEPHANYE HIDALGO MORETA

DIRECTOR: MSc. SUYANA ARCOS

QUITO, abril 2021

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios por su infinito amor y por haberme permitido cumplir este reto con éxito gracias a los dones que Él puso en mí, sin Dios no lo hubiese logrado jamás.

Agradezco también a mis padres, Giovani y María Eugenia, por la confianza que tienen en mis habilidades y por cada palabra de aliento que me brindaron durante todo este proceso. Les agradezco por impulsarme a seguir creciendo cada día.

También quiero agradecer a mi hermano Francisco, con quien empezamos juntos este desafío, en diferentes carreras, pero juntos. Gracias por tu motivación y por tu compañía en esas madrugadas y tardes de investigación que ayudaron inmensamente a cumplir con mi objetivo.

No podía faltar mi agradecimiento a Christian, por su paciencia durante este período ya que tuvimos que sacrificar los momentos que compartíamos juntos, pero sabemos que todo esfuerzo tiene su recompensa.

Agradezco infinitamente a mi compañero de trabajo y amigo, Santiago, por su apoyo incondicional, por compartir conmigo su conocimiento en ciberseguridad y por ayudarme a salir de esa laguna mental cuando toda la información se apoderaba de mí.

También quiero dar gracias a la MSc. Suyana por todo el apoyo y los consejos brindados durante la ejecución de este proyecto, su conocimiento fue de muchísima utilidad para poder culminar con éxito este reto.

Finalmente doy gracias a la Pontificia Universidad Católica del Ecuador, porque a pesar de la difícil situación que se presentó para el país en el 2020, nos permitió continuar con el proceso de aprendizaje e innovación para adquirir mayor conocimiento y así, seguir creciendo como profesionales en una rama tan cotizada como es la tecnología.

Geovanna Stephanye Hidalgo Moreta

DEDICATORIA

Este proyecto lo quiero dedicar a mis abuelitos Lolita y Víctor Hugo, que son una fuente de inspiración muy poderosa; su fuerza, su amor, su cariño y preocupación por sus nietos, a pesar de la distancia, es lo que me ha motivado a seguir creciendo y no desfallecer sin importar cuán difícil se ponga el camino que Dios tiene preparado para mí.

Geovanna Stephanye Hidalgo Moreta

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Los avances agigantados de la tecnología en los últimos 10 años han hecho que las empresas consideren la seguridad de la red como una prioridad en su negocio (Khelf & Ghoualmi-Zine, 2019). La tendencia de los negocios digitales ha tomado fuerza mientras la tecnología y las telecomunicaciones han ido avanzando, sin embargo, los riesgos a ataques cibernéticos que presentan las empresas que usan medios digitales también ha aumentado (Uctu, Alkan, Dogru, & Dorterler, 2019).

Las técnicas de ataques cibernéticos han ido evolucionando con el paso del tiempo y han afectado a empresas tanto financieras, tecnológicas e incluso gubernamentales. Una de las técnicas que más riesgo presenta para las empresas es la denegación de servicios (DoS) mediante la sobrecarga de redes con tráfico inútil o la saturación de recursos del servidor incapacitándolo para responder a peticiones legítimas (Maraj, Jakupi, Rogova, & Grajqevci, 2017).

Estudios realizados han determinado que técnicas como phishing y ransomware, utilizadas para fraude y robo de información, han provocado pérdidas económicas a varias empresas. Estas técnicas, encriptan la información y solicitan un rescate para liberarla, en muchos casos incluso utilizan el chantaje y extorsión amenazando con exponer información crítica de la empresa si no se realiza el pago solicitado (Gómez Vieites, 2019).

Un modelo de seguridad de red está orientado a la definición de políticas de seguridad perimetral, seguridad de red interna, seguridad de dispositivos finales y seguridad de la información lo que permite disminuir los riesgos a ataques cibernéticos (Uctu, Alkan, Dogru, & Dorterler, 2019).

Se han realizado varios estudios (Delgado, 2018; Mero Garcia, 2016; Puga Hermosa, 2017) basados en la implementación de un sistema de gestión de seguridad de la información (SGSI) para determinar la arquitectura, modelo y políticas que debe aplicar una empresa para minimizar los riesgos tecnológicos estos estudios aportarán como referencia al diseño de políticas que se acoplen al caso en cuestión.

Adicionalmente, existen investigaciones anteriores (Aguayo Morales, 2020; Bolaños Botina, 2018; Soewito & Andhika, 2019) que han demostrado que la implementación de un modelo de seguridad de red con el uso de equipos de siguiente generación correctamente configurados y la aplicación de políticas de seguridad basados en un sistema de gestión de seguridad de la información, han mejorado el rendimiento de los sistemas de seguridad perimetral, han reducido las zonas de ataque y vulnerabilidades y han optimizado el uso de los recursos empresariales.

Este proyecto está orientado a determinar el modelo de seguridad de red que se acopla a la infraestructura de la empresa y que represente una mejora en la disponibilidad de sus servicios y seguridad tanto para su red como para sus usuarios.

INTRODUCCIÓN

Justificación

La seguridad de la información y de la infraestructura de una empresa debe ser considerada una prioridad ya que los negocios actuales se manejan con el uso de aplicaciones e Internet, en lo que se conoce como la era digital. El acceso a Internet y la publicación de los servicios de una empresa sin la definición de un modelo de seguridad, representa un riesgo que debe ser mitigado inmediatamente para que tanto los usuarios como los servicios de la empresa no se encuentren vulnerables a posibles ataques cibernéticos.

Es indispensable identificar las vulnerabilidades que presenta la infraestructura de una empresa con el fin de poder corregirlas mediante la aplicación de un modelo de seguridad utilizando las mejores prácticas tanto en arquitectura como en configuración de equipos del perímetro, con el fin de asegurar un correcto funcionamiento de los servicios de la empresa, reduciendo al máximo los riesgos de ataques que pueden afectar al giro del negocio.

Las soluciones de seguridad perimetral están orientadas a defender la infraestructura de ataques externos, sin embargo, hay que considerar que los riesgos pueden estar inmersos también en la red interna de la empresa. Por lo cual, es necesario tener un control de acceso y uso de los recursos empresariales mediante la definición de políticas de seguridad. No cualquier persona así sea funcionario de la empresa debe tener acceso a información crítica como sistemas contables, financieros, y de talento humano. De igual manera, el uso de los recursos como Internet, servicios de impresión, repositorios, bases de datos, almacenamiento entre otros, también deben ser regularizados. Con políticas de seguridad adecuadas se disminuye la superficie de ataque interna, se optimiza el uso de los recursos y se garantiza que estos sean utilizados en pro de la empresa y sus objetivos.

Las empresas que no cuentan con una arquitectura y políticas adecuadas de seguridad están propensas a recibir reportes de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) la cual está encargada de regular el uso de los servicios de telecomunicaciones y garantizar el derecho de acceso a servicios de calidad, convergentes y seguros (ARCOTEL, 2017). Mediante el departamento de EcuCERT, la ARCOTEL envía reportes de riesgos tecnológicos a los Proveedores de Servicios (ISP) respecto a las vulnerabilidades encontradas

en las redes de sus clientes con el fin de que las empresas tomen acción y los corrijan antes de un posible ataque. Estos reportes conllevan una advertencia, ya que, si el problema no es solventado en el tiempo determinado por la ARCOTEL, los ISPs tienen la autorización para tomar las medidas necesarias que eviten que esta vulnerabilidad afecte a sus demás clientes; esto puede ser bloqueo de puertos, aplicaciones e incluso bloqueo total de la IP pública por la cual se publican los servicios de la empresa. Un modelo de seguridad de red evita los reportes de la ARCOTEL para que los servicios de la empresa no se vean afectados en su operación por bloqueos por parte de los ISPs.

Planteamiento del proyecto

La empresa AKEA S.A se dedica a brindar servicios como: almacenamiento, virtualización, optimización de enlaces, networking, comunicaciones unificadas y seguridad de red. Sin embargo, internamente su infraestructura tecnológica no cuenta con un modelo de seguridad de red, lo cual ocasiona que sus usuarios y sus servidores estén vulnerables a diferentes tipos de ataques tanto desde Internet como desde la red interna. Los atacantes aprovechan estas brechas de seguridad para extraer información valiosa de las empresas o a su vez incapacitar los servicios publicados en Internet lo que puede causar pérdidas incluso económicas para las empresas.

La arquitectura actual de la empresa no tiene la capacidad de evitar que exista posibles ataques como malware, ransomware, phishing, comando y control, denegación de servicio y extracción de información, originados desde Internet. Esto puede ocasionar que la información crítica de los usuarios y de la empresa caiga en manos de ciberdelincuentes. Además, puede hacer que los servicios estén inaccesibles y esto representaría pérdidas tanto de la confianza de los clientes finales a quienes se brinda servicio como pérdidas económicas.

La empresa no cuenta con un documento adecuado de políticas de seguridad, lo cual permite que todos los usuarios puedan acceder a cualquier tipo de información y también tengan permisos sin restricciones a la navegación por Internet. Esta falencia representa una brecha de seguridad, una puerta de acceso a ataques e incluso el uso de recursos para fines no corporativos, bajando el tiempo productivo de los funcionarios de la empresa.

Adicionalmente, en los últimos 12 meses, la ARCOTEL, ha reportado que la empresa presenta una mala configuración para los servicios openDNS y openRDP. El reporte respecto al servicio

openDNS informó que la dirección IP pública de la empresa se encontraba respondiendo a consultas recursivas de DNS, realizadas por hosts o direcciones IP que no corresponden al dominio de este servidor. Esta condición podría ser abusada por un posible atacante que realice un gran número de consultas, lo que provocaría una situación de denegación de servicio (DoS), al consumir todos los recursos del servidor intentando responder a estas consultas.

Respecto al reporte sobre el servicio openRDP se informó que se tenía habilitado el protocolo RDP hacia el Internet. Este protocolo es propietario de Microsoft y permite conectarse a otra computadora sobre una conexión de red. La exposición de este servicio al Internet es riesgosa debido a que los atacantes podrían adivinar las credenciales por medio de fuerza bruta y acceder a información sensible alojada en el servidor remoto. Además, los atacantes podrían explotar vulnerabilidades en la implementación del protocolo en sistemas operativos no actualizados.

En caso de que estas vulnerabilidades no sean solventadas en el tiempo determinado por la ARCOTEL, el ISP tiene la facultad de bloquear los puertos por defecto de estos servicios e imposibilitar su uso indefinidamente, lo que causaría que los servicios y aplicaciones de la empresa se encuentren inaccesibles. Debido a la falta de un modelo de seguridad de red esto vulnerabilidades no fueron detectadas para evitar los reportes de la ARCOTEL.

Objetivo general

Realizar el estudio de un modelo de seguridad de red mediante la aplicación de las mejores prácticas de implementación y configuración de equipos del perímetro, así como las normativas de un sistema de gestión de seguridad de información para el mejoramiento del sistema de seguridad perimetral de la empresa AKEA S.A.

Objetivos específicos

- Analizar el modelo de arquitectura y la metodología de seguridad perimetral en base a la aplicación de las mejores prácticas para la implementación y configuración de los equipos del perímetro que permita la disminución de los riesgos tecnológicos que presenta la infraestructura actual.
- Diseñar un modelo de políticas de seguridad que se acoplen a las necesidades de la empresa mediante las normativas y recomendaciones de un sistema de gestión de seguridad de la información para la regularización de los recursos empresariales.

- Diseñar la arquitectura de seguridad perimetral en base a la metodología y políticas de seguridad propuestas para la mitigación de los riesgos de red actuales.
- Evaluar el diseño de la metodología y políticas de seguridad mediante la comparativa de lo propuesto con el manual de mejores prácticas de implementación y configuración y la normativa vigente para un sistema de gestión de seguridad de la información con el fin de determinar si el diseño propuesto mejorará el sistema de seguridad perimetral actual.

Procedimiento marco metodológico

Este proyecto se iniciará con la determinación de las vulnerabilidades de red que presenta la arquitectura actual para lo cual se realizará un estudio no experimental de tipo exploratorio que permitirá recopilar todos los datos mediante levantamiento de información en sitio. A través de un estudio descriptivo se analizará los modelos de arquitectura y metodologías de seguridad de red que mejorarán la seguridad perimetral de la empresa en cuestión en base a trabajos de investigación realizados anteriormente y de documentación de los fabricantes de seguridad.

El siguiente paso será determinar las falencias del documento de las políticas de seguridad que presenta la empresa actualmente, se realizará un estudio no experimental de tipo exploratorio que permitirá recopilar toda la información, mediante la técnica de la entrevista al ingeniero del área de seguridad y al gerente técnico. En base al análisis anterior se realizará un estudio de tipo descriptivo de los modelos de políticas de seguridad basados en la normativa vigente para elaborar una propuesta de las políticas de seguridad que se acoplen a los objetivos de la empresa.

Se realizará la propuesta de diseño de la arquitectura de seguridad mediante un estudio de tipo descriptivo en base a la metodología y políticas de seguridad propuestas. Por medio de un estudio experimental, se simulará la aplicación de las políticas de navegación y en laboratorio con el uso del software de seguridad perimetral virtualizado en un servidor físico.

Finalmente, se realizará la evaluación del modelo de seguridad de red mediante un estudio no experimental de tipo correlacional causal para establecer si la arquitectura, metodología y políticas aplicadas mejorarán la seguridad perimetral, permitirán la regulación de los recursos empresariales y evitará reportes de la ARCOTEL que indispongan el servicio de red.

CAPÍTULO 1: FUNDAMENTOS TEÓRICOS

Entre los aspectos importantes que la seguridad debe resguardar es la confidencialidad, la disponibilidad y la integridad de la información, es por esto que, para poder determinar una solución tecnológica para un sistema de gestión de seguridad de la información a nivel empresarial, es necesario conocer los conceptos teóricos que permiten identificar los posibles riesgos y así seleccionar la mejor opción que disminuya estas brechas de seguridad.

1.1 TIPOS DE ATAQUES DE RED

Existen diferentes tipos de ataques tanto a la red como a la información que se envía a través de la misma. Estos ataques han ido evolucionando con forme pasa el tiempo y a pesar de que las técnicas seguridad también han evolucionado, los atacantes buscan la forma para poner romper esa seguridad e infiltrarse en la red de la empresa para hacer uso de sus recursos y de su información sin tener los permisos necesarios.

En esta sección se detalla los diferentes tipos de ataques cibernéticos más conocidos que una red puede sufrir y las formas en las que estos ciberataques pueden perjudicar a las empresas.

1.1.1 Detección de vulnerabilidades en los sistemas

Este tipo de ataques es pasivo ya que técnicamente no genera una alteración o afectación a la red o a la información que circula en ella. Su principal objetivo es detectar las posibles vulnerabilidades de una red o de un sistema informático en particular, para después desarrollar una herramienta que permita explotarlas fácilmente.

Los ataques de detección de vulnerabilidades hacen uso de herramientas y técnicas de análisis de tráfico para observar lo que se está transmitiendo a través de las redes de la empresa. Entre las herramientas o técnicas que usan estos ataques se puede mencionar las siguientes (Gómez Vieites, 2019):

- *Sniffers:* permiten la interceptación del tráfico que circula por una red sin modificar su contenido.
- *MAC flooding*: esta técnica provoca un desbordamiento de las tablas de memoria de un switch con el fin de que el switch actúe como un simple hub y la información estaría disponible en cualquiera de los puertos en el que se conecte.

1.1.2 Robo de información mediante la intercepción

Este tipo de ataques son considerados activos ya que afectan notablemente a la información que circula en la red. El objetivo principal es interceptar los mensajes de correo o los documentos que se envían a través de red, vulnerando de este modo la confidencialidad del sistema y la privacidad de sus usuarios.

Estos ataques son los que han ido evolucionando con mayor fuerza para fraudes, estafas y extorsiones a través de Internet, muchos de ellos utilizan técnicas de difusión de correos electrónicos fraudulentos que contienen información falsa virus, o *software* malicioso. Entre las técnicas de ataques más utilizados en este tipo de robo de información se puede mencionar los siguientes (Gómez Vieites, 2019):

- *Phishing:* mediante la creación de páginas web falsas imitan y suplantan a las originales, comúnmente orientados a servicios bancarios, el fin de este ataque es obtener los números de cuenta y las claves de acceso para realizar operaciones fraudulentas que perjudiquen a los legítimos propietarios.
- *Pharming:* es una variante del phishing, se basa en un virus que se implanta en los ordenadores de las víctimas, para que las solicitudes a páginas web bancarias sean redireccionadas a páginas web falsas que imitan a las originales, el fin es el mismo, sustraer números de cuenta y claves de acceso.
- *Ransomware*: es un software malicioso que, al ser ejecutado en el ordenador de la víctima, utiliza técnicas de encripción para que la información de la víctima no pueda ser legible. Esta técnica es muy usada para extorsiones y estafas a usuarios de Internet, el fin de este ataque es la solicitud de un rescate a cambio de la liberación de la información encriptada.

1.1.3 Ataques de suplantación de la identidad

Este tipo de ataque activo, intercepta la comunicación entre cliente servidor y modifica algunos parámetros de las cabeceras para suplantar la identidad ya sea del cliente como del servidor, entre las técnicas que se utilizan para suplantación de identidad a nivel de red se pueden mencionar las siguientes (Gómez Vieites, 2019):

- *IP Spoofing*: conocido como enmascaramiento de la dirección IP, el propósito de esta técnica es adquirir la dirección IP autorizada para acceder a los servicios a los cuales se pretende afectar, una vez que el atacante consigue esa información, suplanta sus propias cabeceras por las adquiridas del cliente autorizado, de esta manera puede acceder a la información del servidor suplantando la identidad de un cliente autorizado. Esta técnica puede ser minimizada con el uso de protocolos de acceso en base a usuarios y no únicamente a direcciones IP.
- *Hijacking*: esta técnica no solo enmascara la dirección IP sino también suplanta el número de sesiones ya establecidas entre el cliente y el servidor. De esta manera el atacante conoce la secuencia de los paquetes y podría hacer operaciones fraudulentas en nombre del cliente bajo una sesión ya establecida, como por ejemplo realizar una transferencia sin conocimiento del usuario mientras mantiene la sesión activa con el servidor de la entidad financiera.
- *DNS Spoofing*: el objetivo principal de esta técnica es afectar a los servidores DNS con la inserción de información falsa en su base de datos, con el fin de poder hacer redireccionamientos de las solicitudes de las víctimas a páginas web falsa que han suplantado la identidad de las páginas originales o la intercepción de correos electrónicos. Esta técnica va de la mano con el robo de información y la descarga de *software* malicioso como por ejemplo ataques de phishing o ransomware.
- *SMTP Spoofing*: esta técnica utiliza las debilidades del protocolo SMTP en cuestión de autenticación. Utiliza correos electrónicos falsos que se asemejan a los originales con el fin de engañar al usuario e implantar un virus en el equipo de la víctima al momento de abrir o dar clic en la información enviada. Los atacantes usan esta técnica en conjunto con correo basura o llamado spam el cual envía una gran cantidad de mensajes a diferentes destinatarios esperando que uno o varios de ellos caigan en el engaño y generen una puerta de acceso hacia la organización a través del virus implantado.

1.1.4 Conexión no autorizada a equipos y servidores

Las técnicas de conexión no autorizada afectan principalmente a la confidencialidad e integridad de la información, y puede conllevar a graves consecuencias como el consumo inadecuado de la información, uso de los recursos de la empresa para realizar fraudes, posible desencripción

de claves de servicios de alta sensibilidad. Existen varias maneras de establecer una conexión no autorizada a otros equipos y servidores, entre las cuales se puede destacar las siguientes (Gómez Vieites, 2019):

- *Exploits*: uso de agujeros de seguridad, posterior a una detección de vulnerabilidades de la red.
- *Backdoors*: es el uso de puertas traseras para acceso a la red y a la información de la empresa, utiliza un conjunto de instrucciones no documentadas dentro de un programa o sistema operativo, lo cual permite tomar el control del equipo afectado y así hacer solicitudes a los servidores desde un usuario legítimo.
- *Rootkits*: son programas que se instalan en un equipo sin el consentimiento del usuario, reemplazando a una herramienta o servicio legítimo del sistema operativo. El objetivo principal de esta técnica es realizar funciones ocultas bajo servicios o herramientas legitimas con el fin de tomar el control del dispositivo afectado.

1.1.5 Introducción en el sistema de código malicioso

Los códigos maliciosos conocidos como malware, son programas o documentos que tienen la posibilidad de causar daño a la red o a los servidores. Su principal objetivo, al ser un software malicioso, es interrumpir en las funciones normales de los equipos como servidores o computadores provocando así pérdidas de información e indisponibilidad del servicio. También se enfoca en la sustracción de información susceptible de la empresa o el usuario con el fin de solicitar un intercambio monetario para su liberación (Gómez Vieites, 2019).

La propagación del malware en los últimos años es mucho más rápida con el uso de las aplicaciones de comunicación como correo electrónico, mensajería instantánea y soluciones P2P, sin embargo, donde más se puede encontrar este tipo de ataques es en la navegación en páginas de dudosa procedencia o en la descarga de software ilegal (Gómez Vieites, 2019).

1.1.6 Ataques de denegación del servicio

Los ataques de denegación de servicio (DoS) afectan a uno de los principios básicos de la seguridad, que es la disponibilidad. En sí, su objetivo es evitar que los servidores sean capaces de responder a solicitudes legítimas mediante técnicas que podrían colapsar a los recursos de dichos servidores (Gómez Vieites, 2019). Existen un sin número de técnicas utilizadas por los

atacantes para alcanzar un DoS, entre las cuales se puede mencionar las siguientes (Gómez Vieites, 2019):

- *Mail bombing*: es el envío masivo de miles de correo electrónico que provocan la sobrecarga del servidor de correo y/o de las redes afectadas.
- *Ping de la muerte*: hace uso del comando ping para enviar un excesivo número de solicitudes ICMP, provocando el reinicio o bloqueo del servidor.
- *SYN Flood*: esta técnica se basa en el procedimiento para establecer una conexión TCP, en la cual se utiliza la conexión en tres vías o three-way handshake, el propósito de este ataque es no respetar las normas del intercambio en tres vías, sino llenar de paquetes de inicio de sesión (SYN) al servidor, sin que se envíe un acuse de recibo (ACK), lo que genera que el servidor mantenga varias sesiones semi-abiertas consumiendo recursos de procesamiento del equipo y volviéndolo lento o incluso imposibilitándolo para responder conexiones legítimas.
- *Connection Flood*: esta técnica consiste en intentar establecer miles de conexiones simultáneas contra un determinado servidor, provocando un elevado consumo de recursos y degradando su respuesta ante solicitudes de usuarios legítimos.
- *Net Flood*: esta técnica es similar a la anteriormente descrita, sin embargo, su diferencia radica en el objetivo, ya que esta técnica no se orienta a un servidor en específico, sino más bien a la degradación de la red en general, llenándola de trafico masivo innecesario que evita que trafico legítimo circule con normalidad en la red.

Los ataques de DoS suelen ir de la mano de técnicas de suplantación de identidad como IP Spoofing, los atacantes se ocultan bajo estas técnicas para no ser descubiertos al momento de comprometer sol servicios de una empresa (Gómez Vieites, 2019).

1.1.7 Ataques de denegación de servicio distribuidos

Una vez conocidas las técnicas de denegación de servicio (DoS), con el pasar del tiempo, los atacantes han desarrollado nuevas técnicas para ser más efectivos en sus ataques, entre estas técnicas se encuentra la denegación de servicio distribuido (DDoS). La principal característica de este tipo de ataque es el uso de equipos previamente infectados con algún tipo de virus que permita al atacante el control de los mismos. Comúnmente, los usuarios no suelen tener

conocimiento de que sus dispositivos están comprometidos. Los atacantes al tener acceso remoto a varios equipos autorizados dentro de la empresa realizan ataques coordinados para colapsar la red o el servidor objetivo del ataque (Gómez Vieites, 2019).

1.2 CICLO DE VIDA DE UN ATAQUE

Los diferentes tipos y técnicas de ataque mencionadas anteriormente han permitido que los atacantes puedan infiltrar la red de una empresa de diversas maneras, sin embargo, deben seguir un ciclo para completar un ataque satisfactorio.

El ciclo de vida de un ataque es un modelo propuesto por Lockheed Martin en 2011 que indica la estructura de un ataque de seguridad cibernética e intrusión en una red informática (Khan, Siddiqui, & Ferens, 2017). Este modelo está compuesto por siete etapas como se muestra en la Figura 1-1. El propósito de este modelo es poder analizar las fases de los ataques y determinar la defensa que permite romper la cadena del ataque (Tarun & Rao, 2015).

Figura 1-1 Ciclo de vida de un ataque
Fuente: (Tarun & Rao, 2015)

El modelo de Lockheed está estructurado de forma que el ataque pueda ser bloqueado en cualquiera de sus etapas, si se bloquea en una etapa el ataque no es satisfactorio, sin embargo, mientras más rápido sea bloqueado menos información puede perderse o ser afectada.

1.2.1 Reconocimiento

El clico de un ataque inicia con el reconocimiento de las falencias del objetivo de ataque. En esta etapa se recopila la mayor cantidad de información posible de la víctima, que puede ser un individuo en específico o toda una organización. Toda la información extraída en esta etapa es utilizada en etapas posteriores para afectar al objetivo. Existen dos tipos de reconocimientos (Tarun & Rao, 2015):

- *Reconocimiento Pasivo*: este tipo de reconocimiento recopila información sí que la víctima tenga conocimiento de que su información está siendo extraída.

- *Reconocimiento Activo*: este tipo de reconocimiento es más complejo, ya que utiliza técnicas de perfilamiento que pueden ser detectadas por la víctima y ser bloqueadas en ese momento.

A continuación, se presentan algunas técnicas de reconocimiento que son utilizadas en esta etapa por los atacantes diferenciándolas si son activas o pasivas:

Tabla 1-1 Metodología de reconocimiento

METODOLOGÍA DE RECONOCIMIENTO	TIPO DE RECONOCIMIENTO	TÉCNICA USADA
Identificación y selección de objetivos	Pasiva	Nombres de dominio, registros en APNIC, RIPE, ARIN
Perfil social de objetivos	Pasiva	Redes sociales, documentos públicos, informes y sitios web corporativos
Perfil de sistema de objetivos	Activa	Barrido de ping, huella digital, escaneo de puertos y servicios
Validación de objetivo	Activa	Mensajes de SPAM, Correos con phishing e ingeniería social.

Fuente: (Tarun & Rao, 2015)

1.2.2 Armamento

Esta etapa utiliza la información recopilada anteriormente para definir las herramientas de ataque efectivo que vulneren el sistema. Su objetivo es la creación de puertas traseras que permitan la penetración del atacante en la red y así poder explotar sus vulnerabilidades; esta etapa se enfoca en el diseño y desarrollo de dos componentes principales (Tarun & Rao, 2015):

- *Herramientas de Acceso remoto*: conocidos como RAT (Remote Access Tool), es un software que se ejecuta en el sistema de la víctima de manera anónima, esta herramienta permite tener acceso al control del sistema, como por ejemplo ejecución remota de programas, carga y descarga de archivos, incluso la suspensión completa del sistema y, dependiendo de los mecanismos usados, los RAT pueden obtener privilegios de usuario administrador para realizar captura de data, saturación de red y la instalación de módulos de anti-detección de intrusos.

Las RAT están compuestas de dos partes, la parte del cliente que es en si el sistema de la víctima, donde se ha instalado el software de acceso remoto, la cual se comunica constantemente con su controlador. La segunda parte es la del servidor, la cual suele ser usada por el atacante, es aquella que manda los comandos de control hacia el cliente para ejecutar los ataques, en la etapa de comando y control.

- *Exploits*: actúan como portadores de la RAT y utiliza las vulnerabilidades del sistema para y ejecutar la RAT sin que la víctima lo detecte mientras se establece un acceso de puerta trasera silencioso. Los exploit pueden disfrazarse de archivos legítimos como documentos de Word, PDF, audio/video o también páginas web con software malicioso embebido; una vez que la víctima abre uno de estos archivos el exploit comienza a realizar su función escalando privilegios que permitan la instalación de la RAT.

1.2.3 Entrega

Esta es la etapa más importante para el atacante, ya que de ella depende si el ataque puede ser satisfactorio o no. Muchas veces la etapa de entrega o delivery requiere de la interacción de la víctima como por ejemplo el descargar un archivo con software malicioso o el ingresar a una página web con contenido sospechoso (Tarun & Rao, 2015).

Debido a esta interacción, esta etapa es la más crítica y de mayor riesgo, ya que aquí el atacante puede dejar algún tipo de rastro a pesar de que se utiliza técnicas para estar en el anonimato. Los atacantes suelen utilizar diferentes mecanismos para la entrega porque con un solo mecanismo no se puede garantizar el 100% de éxito en el ataque. Muchas veces los mecanismos fallidos son utilizados para extraer información de la víctima y su sistema, como en un reconocimiento activo (Tarun & Rao, 2015). Entre los mecanismos de entrega o delivery se pueden mencionar los siguientes (Tarun & Rao, 2015):

- Correos electrónicos con adjuntos
- Ataques de phishing
- Conducir a la descarga de archivos maliciosos
- Medios externos infectados
- Envenenamiento de cache de DNS

1.2.4 Explotación

Cuando la etapa de entrega se completa, con la interacción de la víctima, la siguiente etapa es la explotación, la cual consiste en silenciosamente instalar y ejecutar el software necesario para vulnerar el sistema.

En esta etapa se utiliza diversos mecanismos de explotación basados en las vulnerabilidades de los sistemas las cuales fueron descubiertas y analizadas en las etapas anteriores. Estas vulnerabilidades son identificadas como CVE (Common Vulnerabilities and Exposures), son anomalías en el comportamiento del sistema frente a ciertas interacciones del usuario. Los desarrolladores de software están constantemente realizando actualizaciones que permiten corregir estas anomalías o bugs, sin embargo, no todas suelen ser corregidas y es ahí donde los exploits se pueden utilizar (Tarun & Rao, 2015).

Hay que tener en consideración que para que un exploit permita un ataque satisfactorio debe cumplir con tres condiciones esenciales (Tarun & Rao, 2015):

- El exploit se debe usar sobre el software o sistema operativo para el cual fue creado.
- El software o sistema operativo no debe ser actualizado a versiones donde el exploit no pueda funcionar.
- Los sistemas de anti-virus no deben detectar ni de forma estática ni dinámica al exploit durante el proceso de instalación.

Es por esto que se utilizan diferentes tipos de exploits al momento de realizar el ataque, para poder ser más efectivos.

1.2.5 Instalación

Esta etapa afecta a los mecanismos de seguridad del dispositivo donde reside el sistema operativo al cual se realiza el ataque. Su objetivo es la instalación de código malicioso o malware que afecte al comportamiento adecuado del sistema (Tarun & Rao, 2015). El malware puede ser de diferentes tipos y afectar a partes especificas del sistema que se encargan de la seguridad, entre los tipos más conocidos de malware se puede mencionar los siguientes (Tarun & Rao, 2015):

- *Anti-Debugger y Anti-Emulation*: mediante mecanismos de cifrado, motores de inspección y detección, el malware puede asegurar que las técnicas de emulación y depuración de un sistema dejen de funcionar.
- *Anti-Antivirus*: muchos paquetes de malware incluyen herramientas que automáticamente puede deshabilitar los sistemas de protección de un equipo como son los antivirus y los IDS, estas herramientas ejecutan con frecuencia el proceso para deshabilitar estos sistemas evitando que el dispositivo pueda detectar la amenaza.
- *Rootkit y Bootkit*: los rootkit son un tipo de malware que esconde los procesos que están siendo ejecutados. Los bootkit, por otro lado, se enfocan en el kernel del sistema al cual están atacando, obteniendo acceso no permitido a todo el sistema. Su objetivo principal es evitar que el sistema operativo los detecte y ejecute los mecanismos de protección.
- *Targeted Delivery*: las entregas dirigidas son mecanismos que permiten al atacante validar si el dispositivo es real o es algún sistema de análisis, lo que realiza es un inventario del equipo, como por ejemplo memoria, procesador, disco etc., y la información lo envía al sitio central del *malware* para determinar si el ataque puede continuar o no.
- *Host-Based Encrypted Data Exfiltration*: este proceso se lo realiza al momento de la extracción de la información comprometida, los malware generalmente encriptan la información en el nivel de host previo al envío por medio de protocolos sin cifrar como HTTP o SMTP, esto con el fin de no ser detectados por sistemas de detección de anomalías o prevención de fugas.

1.2.6 Comando y control

Una de las etapas principales del ciclo de vida de un ataque es la etapa de comando y control, una vez ejecutado las etapas anteriores, el dispositivo comprometido puede comunicarse sin ser detectado con el centro de comando y control del atacante, donde comúnmente es llevada la información que se va a extraer (Tarun & Rao, 2015).

En la actualidad existen tres estructuras utilizadas para los sistemas de comando y control, las cuales han ido evolucionando en base a la anterior, a continuación se detalla cada estructura (Tarun & Rao, 2015):

- *Estructura centralizada*: es la estructura básica de un sistema de comando y control utilizando un modelo de cliente-servidor, donde el/los clientes son los dispositivos comprometidos y el servidor es único y es quien toma el control de los equipos infectados. El problema que presenta esta arquitectura es que depende netamente del servidor y sus recursos limitando así los ataques masivos. Además, al ser el punto central, si el servidor es neutralizado, la estructura de comando y control total es neutralizada también.
- *Estructura descentralizada*: es la segunda evolución de la estructura de comando y control, su objetivo es superar las limitantes de su antecesor, utilizando técnicas de *peer-to-peer* donde se dividen los dispositivos infectados para ser controlados por diferentes nodos. Esto permite escalabilidad y redundancia, haciendo que sea más complejo detectar exactamente de donde proviene el ataque.
- *Estructura basada en redes sociales*: el uso de redes sociales como Facebook ha ido incrementando con el pasar del tiempo, y es considerado tráfico benigno en la mayoría de organizaciones, es por esto de los atacantes utilizan estas plataformas para tomar control de manera centralizada o descentralizada de los dispositivos infectados.

Lo principal a considerar en esta etapa es que el atacante necesita que la comunicación entre el dispositivo comprometido y su centro de control sea completamente anónima, de manera que no lo puedan rastrear. Utiliza técnicas como TOR (The Onion Router), ICR Chat (Internet Relay Chat), DNS Fast Flux, entre otras para mantener el anonimato el mayor tiempo posible (Tarun & Rao, 2015) .

1.2.7 Acción sobre el objetivo

Como etapa final del ataque, una vez que se tenga el control sobre la víctima, el atacante comienza a ejecutar los comandos correspondientes dependiendo del tipo de ataque que se vaya a realizar. En ataques masivos, el objetivo son varios sistemas en conjunto que tienen como propósito romper mecanismos de seguridad y obtener credenciales de administrador de un sistema, incluso este tipo de ataque es orientado a la denegación de servicios al tener el control de varios dispositivos en la red (Tarun & Rao, 2015).

Otro tipo de ataque es el ataque dirigido, el cual es más sofisticado, este ataque tiene como objetivo la extracción de información sensible o confidencial o a su vez escalar en la red de la empresa hasta llegar a su objetivo principal dentro de una organización (servidor contable, pc gerente, etc.) (Tarun & Rao, 2015).

1.3 TÉCNICAS DE PREVENCIÓN DE AMENAZAS.

Para impedir de manera significativa que un ataque tenga éxito, es necesario contar con una arquitectura de seguridad que incluya técnicas de prevención de amenazas, las cuales permite la detección, prevención, disrupción, degradación y escape para detener el ataque en alguna de las fases del ciclo de vida. Existe hardware y software especializados, como por ejemplos los firewalls, antivirus, IPS, sandboxing etc., orientados a defender a la infraestructura de red en cada una de las fases del ciclo de vida del ataque (Tarnowski, 2017).

El principal objetivo de un sistema de seguridad es poder detener el ataque en cualquiera de sus etapas de ciclo de vida, como lo muestra la Figura 1-2 , con excepción de la última etapa donde la red o el sistema ya se encuentra comprometido.

Para alcanzar este objetivo es necesario reconocer las técnicas y herramientas que se pueden utilizar para neutralizar un ataque. Existen cinco tareas principales que permites a una arquitectura de seguridad estar preparada para la defensa frente un ataque.

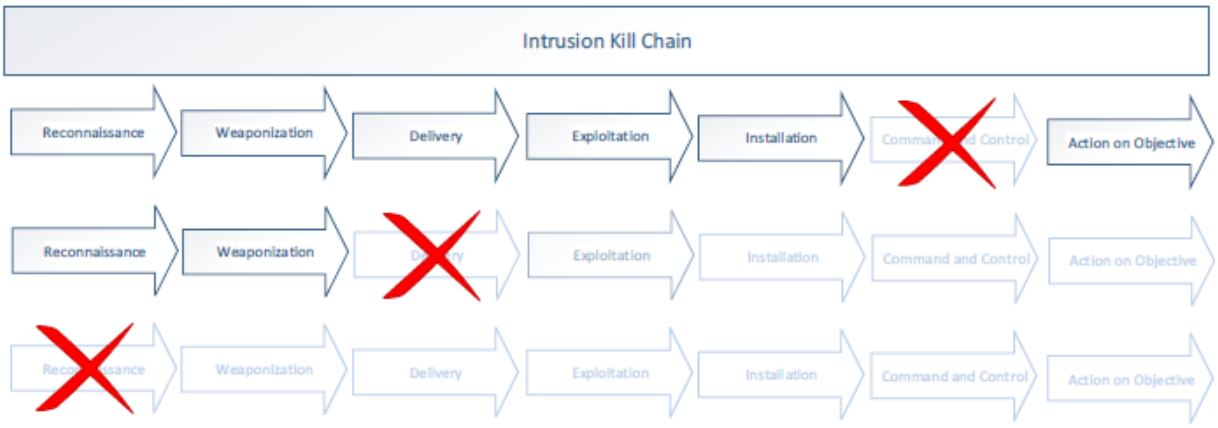


Figura 1-2 Neutralización del clico de vida de un ataque
Fuente: (Tarnowski, 2017)

1.3.1 Detección

La detección de ataques es la funcionalidad más importante de un sistema de seguridad para la defensa, herramientas y equipamiento que permitan la detección son considerados la primera línea de defensa, como por ejemplo los firewalls, antivirus, analizadores de tráfico, HIDS (Host-based intrusion detection system), correlacionadores de eventos entre otros (Tarnowski, 2017).

1.3.2 Prevención

Las técnicas de prevención de ataques dependen de las políticas de seguridad de información que maneje la empresa, es por esto que se las debe definir con claridad para evitar brechas de seguridad demasiado obvias para los atacantes. Dentro de las técnicas de prevención se encuentra los IPS (Intrusion Prevention System), los firewalls, sandboxing, sistemas de actualizaciones automáticas, ACL (Access list), entre otros (Tarnowski, 2017).

1.3.3 Disrupción

Conocido como interrupción del ataque, estas técnicas son utilizadas para impedir que el ciclo del ataque se cumpla o a su vez hace que el ataque sea menos efectivo, retrasando su ejecución o con la implementación de trabas de seguridad (Tarnowski, 2017).

Una de las técnicas más utilizadas para la interrupción de un ataque es el hardening de los sistemas, comúnmente, son configuraciones recomendadas por los fabricantes de cada dispositivo o software con el fin de endurecer los sistemas de seguridad y volver el ciclo de vida del ataque mucho más complejo (Tarnowski, 2017).

1.3.4 Degradación

La degradación del ataque consiste en disminuir la eficacia del ataque, el ataque en si se puede efectuar, pero con mínimas consecuencias para la empresa debido a las técnicas de degradación. Entre las diferentes técnicas de degradación se puede mencionar a los cambios de configuración para tiempos de sesión, implementación de políticas de conexión de acuerdo al tipo de usuario, como por ejemplo la limitación de tiempo de conexión (Tarnowski, 2017).

1.3.5 Engaño

Conocido como obstaculización del ataque, esta técnica tiene como objetivo engañar al atacante entregando falsa información referente a las vulnerabilidades del sistema, lo que conlleva a una selección errónea del vector de ataque. Entre las herramientas que se pueden utilizar para

generar este engaño se encuentra los honeypot los cuales son sistemas informáticos usados como señuelos para simular ser un objetivo de ataque y así confundir a los atacantes o distraerlos del objetivo principal, adicionalmente son como contraataque obteniendo información de los atacantes utilizando sus intentos de intrusión (Tarnowski, 2017).

En la Tabla 1-2 presentada por (Tarnowski, 2017) en su estudio, se puede identificar las diferentes técnicas de defensa que se puede utilizar ante un ataque, en relación con cada una de las etapas del ciclo de vida del ataque.

Tabla 1-2 Lista de técnicas para la defensa en diferentes etapas del ciberataque

	DETECCIÓN	**PREVENCIÓN**	**DISRUPCIÓN**	**DEGRADACIÓN**	**ENGAÑO**
Reconocimiento	• IDS • HoneyPot • Análisis Web	• IPS • Negar el escaneo de puertos • Firewall • ACL	• Honeynet • IPS • Límite de conexiones • Límite de data	• Configuración de timeout	• Honeypot • Ofuscación de versión
Armamento	• Intercambio información de amenazas • Inteligencia vulnerabilidad • NIDS (Network Intrusion Detection System)	• Intercambio información de amenazas • Pruebas de penetración • Ofuscación de aplicaciones • Aplicación de parches • Versión oculta • NIPS	• Hardening • Ofuscación de versión	• Ofuscación de aplicaciones • Deshabilitar servicios no usados	
Entrega	• IDS • Firewall • Análisis de red	• IPS • Firewall • Port knocking • ACL • Cambiar configuraciones de fábrica	• Hardening • Antivirus en línea	• Integridad obligatoria	• Honeypot

Explotación	• HIDS • Análisis de trafico	• Sandbox local • Actualizaciones de sistema	• Hardening • Prevención ejecución de datos	• Configuración de reversión automática	• Honeypot
Instalación	• HIDS • Sonda IP • Verificación de integridad • Comprobación configuración	• Listas blancas de aplicaciones • IPS • Aislar procesos (Jail chroot)	• Hardening • Antivirus	• Configuración de reversión automática • Tarpit	• Honeypot • Redireccion de DNS
Comando y Control	• NIDS • SIEM • Inteligencia de amenazas	• Listas blancas de aplicaciones • Firewall • ACL	• NIPS	• Calidad de servicio (QoS)	• Honeypot
Acción	• Análisis de logs				

Fuente: (Tarnowski, 2017)

1.4 ARQUITECTURA DE SEGURIDAD PERIMETRAL

La arquitectura de seguridad perimetral se maneja en una estructura en capas, protegiendo desde el perímetro, la red interna, el dispositivo final y la información (Uctu, Alkan, Dogru, & Dorterler, 2019). Utiliza el concepto de zonas de seguridad para reducir la superficie de ataque y establecer límites de seguridad moviendo la seguridad lo más cercano a la data que se quiere proteger (Lyons, 2012).

También se emplea el modelo de seguridad Zero Trust en el cual se trata todo el tráfico de red como hostil, incluso si está dentro del perímetro (Weever & Andreou, 2020). Este modelo se basa en el concepto de "nunca confíes, siempre verifica", las soluciones de seguridad perimetral están obligadas a verificar cada paquete transmitido a través de la red entre las zonas, independientemente del tipo de data que se esté transmitiendo (Uttarwar & Kalia, 2019).

1.4.1 Zonas de seguridad

El concepto de zonas de seguridad es una de las mejores prácticas aceptadas para establecer límites de seguridad, puntos de control, responsabilidades y restricciones. Las zonas de

seguridad son segmentaciones lógicas que agrupan servicios o usuarios con requisitos de seguridad o niveles de riesgo similares (Lyons, 2012).

A nivel de redes, un switch puede segmentar las redes en diferentes redes virtuales conocidas como VLANs, de acuerdo a su direccionamiento IP, y únicamente a través de protocolos de ruteo estas redes pueden comunicarse entre ellas. En la parte de seguridad el concepto es similar, el dispositivo que segmenta las zonas de seguridad comúnmente es un firewall de siguiente generación; esta segmentación no solamente la realiza a nivel de direccionamiento IP, sino más bien se enfoca en el tipo de servicio y de riesgo que se puede tener en esa zona. Una zona de seguridad no puede comunicarse con otra zona a menos que el dispositivo intermediario permita esa conexión.

Se pueden definir las diferentes zonas de seguridad dependiendo del funcionamiento y el servicio de las mismas, entre las zonas más comúnmente utilizadas en arquitecturas empresariales se encuentran:

- *Intra-zone*: es un concepto general que define la conectividad de los dispositivos que pertenecen a una misma zona. Comúnmente este tráfico es permitido por los dispositivos de seguridad perimetral, como los firewalls, sin embargo, se depende del ruteo manejado a través de los dispositivos de capa 3 (Lyons, 2012).
- *Inter-zone*: es un concepto general que define la conectividad de los dispositivos que pertenecen a diferentes zonas. En base a la definición principal de zonas de seguridad un dispositivo perteneciente a la zona A no puede comunicarse con un dispositivo perteneciente a la zona B a si se tenga los protocolos de ruteo necesarios, quien define esa conexión es el dispositivo de seguridad como por ejemplo el firewall (Lyons, 2012).
- *Zona de Internet*: conocida como la zona de desconfianza, los dispositivos de seguridad perimetral deben enfocar su esfuerzo a la protección de accesos no autorizados provenientes de esta zona en particular, de donde generalmente se inicia los ataques.
- *Zona DMZ*: la zona desmilitarizada es un área intermedia entre la red interna y el último dispositivo de salida hacia el mundo o hacia la red de Internet. En esta zona se sitúan los servidores que necesitan publicar sus servicios al mundo, como por ejemplo servidores web, servidores de correo electrónico entre otros (Lyons, 2012).

- *Zona Intranet*: la zona intranet, como su nombre lo indica, limita sus servicios a la red interna. Está compuesta por los servidores que no requieren ser publicados al exterior como por ejemplo servidores de repositorios de archivos confidenciales, servidores de directorio activo, bases de datos entre otros.
- *Zona Usuarios de Confianza*: es la zona general de todos los usuarios, normalmente esta zona se integra con el directorio activo de la empresa para permitir la conexión únicamente de dispositivos registrados en el directorio activo y delimitar de esta manera el acceso a los servicios internos de las empresas. Dependiendo de las políticas de seguridad, esa zona puede subdividirse de acuerdo a los tipos de servicio o niveles de riesgo por ejemplo en zonas de usuarios de contabilidad, usuarios de desarrollo, usuarios gerenciales, usuarios administrativos, etc.

1.4.2 Modelo de seguridad Zero-Trust

El concepto de Zero-Trust fue establecido en 2004 por Jericho Forum, un grupo de especialista de seguridad de la información en la sede de Reino Unido, debido al aumento de conexiones a la nube y por dispositivos móviles (Uttarwar & Kalia, 2019). Su principio se basa en nunca confiar sino siempre verificar.

Los dispositivos de seguridad perimetral actuales utilizan este concepto como base de sus arquitecturas, enfocando el análisis de todo tipo de tráfico que atraviesa la red, sin importar que las zonas de origen y destino estén permitidas de comunicarse.

Según John Kindervag quien introdujo la estrategia de Zero-Trust en Estados Unidos, este modelo de seguridad presenta los siguientes cinco conceptos principales (ON2IT, 2020):

- Verifique siempre y nunca confíe.
- Inspeccione y registre todo el tráfico.
- Se accede a todos los recursos de forma segura, independientemente de la ubicación.
- Privilegio mínimo: el control de acceso se basa en la "necesidad de conocer" y se aplica estrictamente.
- La red está diseñada de adentro hacia afuera.

El uso del modelo de seguridad Zero-Trust resulta beneficioso para las empresas ya que vuelve su arquitectura de red mucho más segura. Entre los beneficios que este modelo le brinda a las empresas se encuentra, reducción de impactos negativos sobre la información crítica (pérdidas o robos), mejora en el acceso a las aplicaciones empresariales, mayor visibilidad del tráfico que circula por la red para análisis de tráfico y correlacionadores de eventos, menor costo de inversión en ciberseguridad (Uttarwar & Kalia, 2019).

1.4.3 Componentes de una arquitectura de seguridad

Una vez determinado los conceptos básicos de seguridad, es necesario determinar las herramientas o dispositivos que permiten alcanzar el objetivo de asegurar la red y sus servicios. Estos dispositivos deben ser correctamente configurados y aprovisionados de manera que se minimice al máximo las vulnerabilidades de la arquitectura y evitar un posible ataque.

Entre las herramientas y dispositivos que se utilizan en una arquitectura de red se encuentran los siguientes (Uctu, Alkan, Dogru, & Dorterler, 2019):

- *Firewall*: el firewall es el punto entre la red interna y el Internet u otras redes internas, proporciona los permisos de conexión entre las diferentes zonas además de realizar las funciones como NAT (Network Address Translation), ruteo, VPN (Virtual Private Network). Anteriormente, los firewalls utilizaban únicamente los conceptos de filtrado de paquetes estático donde solo se discriminaba el tráfico por la cabecera del paquete. Con el pasar del tiempo, se integró el concepto de Statefull Inspeccion donde el firewall ya no solo discriminaba por cabeceras, sino que era capaz de distinguir direccionamiento IP y puertos de comunicación a estos dispositivos se los conocía como UTM (Unified Threat Management).

  Sin embargo, con la evolución de la tecnología y sus servicios, se vio la necesidad de realizar inspección de tráfico a mayor profundidad, no solo usando la capa 4 del modelo OSI, sino también haciendo inspección a nivel de la capa de aplicación. Este último modelo de dispositivo es conocido como NGFW (Next Generation Firewall).

  Las empresas desarrolladoras de soluciones de seguridad han enfocados sus esfuerzos en repotenciar sus dispositivos NGFW, permitiéndoles hacer análisis de filtrado URL,

análisis inteligente de amenazas, incluir módulos como antivirus, IPS e integrarlos con las soluciones de sandboxing.

- *Intrution Detection/Prevention System*: los sistemas de prevención y detección de intrusiones son una de los más importantes defensas de un sistema de seguridad. Anteriormente, la detección de anomalías se lo realizaba de manera manual, con herramientas que consumían demasiados recursos y tiempo. Actualmente estas irregularidades y anomalías se las detecta mediante métodos automáticos de lectura de archivos de registro. La detección de intrusiones es denominada basada en comportamiento, y permite la comparación de firmas predefinidas obtenidas del flujo de tráfico mediante técnicas estadísticas.

  Sin embargo, la detección de intrusos requiere de una intervención manual para dar respuesta a dichos ataques. Es por esto que se integra los sistemas de prevención de intrusiones los cuales son similares a los sistemas de detección en términos de velocidad y basado en contenido.

  Los IPS emplean técnicas para prevenir intrusiones basados en ataques predefinidos como por ejemplo malware basado en red (como gusanos), formato RFC (solicitud de comentarios), paquetes incompatibles, escaneos de puertos, códigos de explotación (exploit), ataques web, entre otros.
- *Data Leak Protection*: la pérdida o fuga de información es uno de los mayores retos en la seguridad de una empresa. La información confidencial en manos equivocadas puede generar pérdidas económicas considerables para las empresas.

  Los sistemas de prevención de pérdida/fugas de datos (DLP) no eliminan por completo este problema, pero son una de las herramientas más efectivas para prevenir la fuga de datos. La principal diferencia con los firewalls y los IPS/IDS es que el DLP se enfoca en identificas datos sensibles en lugar de identificar amenazas a la red.

  En los sistemas DLP se configura parámetros para identificar la información sensible lo cuales general alertas al sistema en el momento que se produce la figa de información. Dentro de estos parámetros se puede mencionar el tipo de archivo como por ejemplo excel, word, pdf, nombre de los archivos como registro_bancario, personal_empresa, e

inclusive los sistemas DLP tienen la capacidad de hacer análisis de la información dentro del archivo que se pretende enviar.

Los DLP además de evitar fugas de información, permite detectar fallas durante el funcionamiento de la empresa, tales como envíos intencionales de documentos confidenciales por parte usuarios de la empresa hacia otros destinos no autorizados.

- *Sandbox System*: la principal funcionalidad de los sistemas de sandbox es realizar análisis dinámicos y estáticos de malware para detectar nuevas técnicas y generar la firma adecuada para contrarrestar estas nuevas técnicas.

  Los sistemas de sandbox poseen sistemas operativos virtuales que simulan ser los sistemas operativos de los clientes protegidos, la idea es hacer el análisis en base a los resultados de la ejecución de un archivo que circula por la red y determinar un veredicto con su correspondiente firma de ser el caso.

  Los sandbox actualmente residen en la nube, cada fabricante de ciberseguridad ha desarrollado su propio sistema de sandbox en base a sus arquitecturas y permite compartir la información recopilada de los análisis con todos sus clientes.

1.5 METODOLOGÍA DE SEGURIDAD PERIMETRAL DE PALO ALTO

Palo Alto Networks, es una de las empresas líderes en el cuadrante de Gartner de firewalls de red (Gartner, 2020), sus soluciones de seguridad perimetral se basan en una arquitectura zonal y su fortaleza radica en su motor de procesamiento paralelo de un solo paso (Single Pass Parallel Procesing SP3).

Cada característica de protección en el equipo (antivirus, antispyware, filtrado de datos y protección contra vulnerabilidades) usa el mismo formato de firma basado en transmisión. Como resultado, el motor SP3 puede buscar todos los riesgos simultáneamente (Palo Alto Networks, 2015).

1.5.1 Arquitectura de seguridad de Palo Alto Networks

Las soluciones de Palo Alto Networks son diseñadas desde cero para hacer control en base a aplicaciones, es decir, desde su aparición en el mercado Palo Alto Networks ha sido considerado un firewall de siguiente generación.

La plataforma de Palo Alto Networks integra soluciones para seguridad perimetral, dispositivo final y la nube, por lo que ha dividido sus soluciones en tres sectores estratégicos (Palo Alto Networks, 2020b).

- *Strata*: es la plataforma orientada a la seguridad de la red empresarial que ofrece protección por hardware, software y basada en la nube.
- *Prisma*: es la solución de seguridad de Palo Alto Networks orientado a la nube contiene un paquete de productos diseñado para proteger los complejos entornos de TI actuales.
- *Cortex*: se enfoca en el análisis y visibilidad de tráfico, ofrece a las empresas funciones insuperables de detección, investigación, automatización y respuesta.

Figura 1-3 Soluciones de Palo Alto Networks
Fuente: (Palo Alto Networks, 2020b)

Todas las soluciones de Palo Alto Networks se integran entre si y alimentan sus bases de inteligencia para garantizar la mayor protección ante las técnicas de ataque actuales.

Esta sección se enfoca en el análisis de las funcionalidades que STRATA ofrece debido a que se pretende orientar el estudio a nivel de seguridad perimetral empresarial mas no de la nube.

Una de las diferencias fundamentales los dispositivos de Palo Alto Networks es su forma de procesar el tráfico que llega a su NGFW. La arquitectura de procesamiento paralelo de único paso como muestra la Figura 1-4, permite el análisis de todos los componentes en una sola inspección sin la necesidad de abrir y cerrar el paquete en cada módulo, disminuyendo el procesamiento de los equipos y mejorando su respuesta (Palo Alto Networks, 2015).

Figura 1-4 Arquitectura SP3
Fuente: (Palo Alto Networks, 2020b)

La principal ventaja de SP3 es que el tráfico se escanea y analiza a medida que cruza el dispositivo con una cantidad mínima de almacenamiento en búfer. Esta velocidad le permite habilitar funciones avanzadas, como el análisis de virus y malware, sin reducir el rendimiento del NGFW (Palo Alto Networks, 2019).

Además del SP3, los equipos de Palo Alto Networks están diseñados de manera que se separa el plano de administración del plano de datos, lo que permite tener acceso al dispositivo en caso de saturación o de un ataque de denegación de servicio con el fin de solventar el inconveniente presentado. Cada plano tiene su propio CPU, memoria y disco para el procesamiento de la información y de igual manera se segmenta físicamente las conexiones como se muestra en la Figura 1-5.

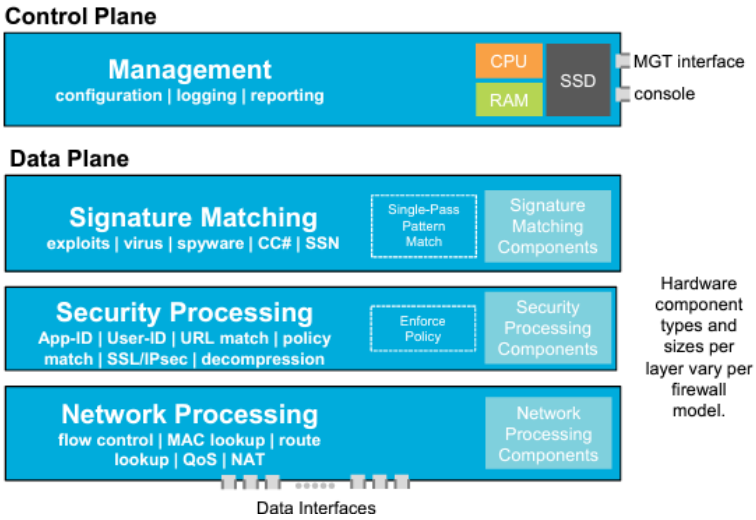


Figura 1-5 Plano de control y plano de datos
Fuente: (Palo Alto Networks, 2019)

Considerando que la seguridad de la red no debe enfocarse solo al perímetro (tráfico de norte a sur) sino también considerar el tráfico interno por el desplazamiento lateral (tráfico de este a oeste), Palo Alto Networks utiliza el modelo Zero-Trust en su arquitectura de seguridad. Zero-Trust no presenta una zona de seguridad de confianza predeterminada y está destinado a remediar las deficiencias con estrategias centradas en el perímetro, los dispositivos y las tecnologías, utilizando como vector principal el “nunca confiar, siempre verificar”. Este enfoque difiere de los modelos de seguridad convencionales que operan sobre la base de "confiar pero verificar" (Palo Alto Networks, 2019).

Finalmente, la administración de toda la plataforma se lo realiza de manera centralizada mediante acceso HTTPS completamente seguro. Dentro del administrador se pueden realizar configuraciones de políticas de seguridad, de nateo, calidad de servicio, desencripción en base a aplicaciones, usuarios o dispositivos. Además, permite el monitoreo proactivo de logs del sistema y de tráfico, así como de amenazas, filtrado URL entre otros.

También permite la generación de reportes de manera calendarizada y presenta un módulo de correlación de eventos donde se puede visualizar gráficamente la actividad dentro de la red, lo que permite hacer un análisis a profundidad de los eventos y poder corregir posibles brechas de seguridad.

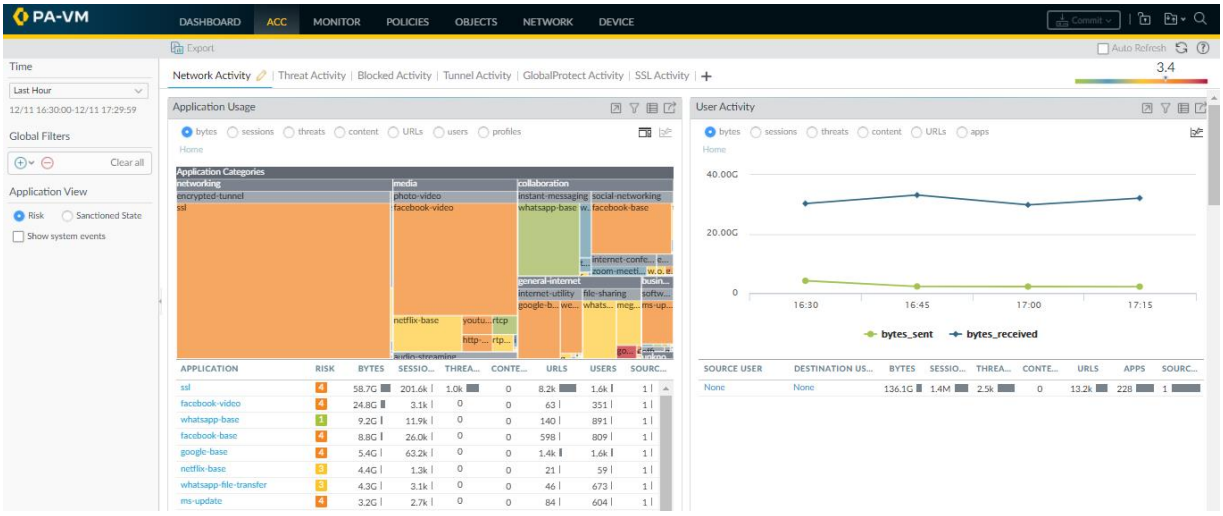


Figura 1-6 Administración centralizada de NGFW Palo Alto Networks
Fuente: (Palo Alto Networks, 2020d)

1.5.2 Funcionalidades principales de NGFW de Palo Alto Networks

Los dispositivos de Palo Alto Networks además de presentar las funciones de ruteo, VPN y zonificación, por ser considerados de siguiente generación (Next Generation Firewall), también vienen integrados con ciertas funcionalidades por defecto que para otros fabricantes representan un módulo adicional a contratar, entre estas funcionalidades están (Palo Alto Networks, 2020b):

- *APP-ID*: este módulo permite la clasificación e identificación del, independientemente del puerto, el protocolo o el tipo de cifrado. APP-ID identifica la aplicación de manera precisa, aplicando al tráfico varios mecanismos de clasificación, como las firmas de aplicaciones, la descodificación de protocolos de aplicaciones o la metodología

heurística. Utilizar APP-ID para clasificar el tráfico en vez de clasificarlo en base a puertos, reduce sustancialmente las posibilidades de ser víctima de un ataque.

- *Content-ID*: utiliza distintas tecnologías de prevención de amenazas avanzadas para analizar a fondo todo el tráfico permitido con un solo análisis. Mediante Content-ID se puede bloquear los exploits de vulnerabilidad, los desbordamientos de búfer y los análisis de puertos; defenderse de los métodos de evasión y ofuscación; detener comunicaciones salientes de malware; bloquear el acceso a sitios web conocidos de descarga de malware y phishing; y reducir los riesgos asociados a la transferencia de archivos y datos no autorizados.
- *User-ID*: permite definir políticas de seguridad en función de los usuarios o de los grupos de usuarios, la política sigue a los usuarios sin considerar el dispositivo que utilicen o el sitio donde se encuentre sea en la matriz de la empresa, en una sucursal o en casa. Esto permite ver la actividad de las aplicaciones por usuarios (y no solo por direcciones IP) y generar informes sobre las actividades de los usuarios.

1.5.3 Funcionalidades bajo suscripción de Palo Alto Networks

A pesar de que las funcionalidades por defecto que vienen embebidos en los dispositivos de Palo Alto Networks son sumamente útiles y podrían sustentar el tema de seguridad perimetral, es importante mencionar las funcionalidades bajo suscripción que repotencian el análisis y la visibilidad del tráfico, para tener una protección robusta en la red empresarial. Las funcionalidades bajo suscripción son las siguientes (Palo Alto Networks, 2020b):

- *Threat Prevention*: ofrece protección antimalware en línea, bloquea el tráfico saliente de comando y control e incluye un sistema de prevención de intrusiones (IPS) capaz de detener automáticamente exploits conocidos. Inspecciona todo el tráfico independientemente del puerto, el protocolo y el tipo de cifrado. El sistema de prevención de intrusiones aplica medidas basadas en la búsqueda de firmas coincidentes y la detección de anomalías, permite importar y aplicar automáticamente firmas y reglas de formatos conocidos. Su mecanismo de defensa está basado en el modelo Zero-Trust y busca amenazas en todos los puntos del ciclo de vida del ataque, no solo cuando las amenazas entran en la red por primera vez.

- *URL Filtering*: es un servicio basado en la nube, identifica las amenazas mediante una combinación única de técnicas de análisis estático y dinámico y aprendizaje automático. Mediante un motor de categorización de URL que se actualiza constantemente, el NGFW tiene la capacidad de contener el trafico proveniente de URLs maliciosas, esta categorización se la realiza en base al contenido de sitio web. Las medidas de protección automáticas bloquean el acceso a los sitios utilizados para la distribución de *malware* y el robo de credenciales, lo que evita la pérdida de datos.
- *Wildfire*: es el motor de análisis y prevención basado en la nube para enfrentar amenazas de día cero como son los exploits y malware de día cero especialmente evasivos. WildFire combina las ventajas de varias técnicas complementarias para crear un sistema de detección de alta fidelidad y resistente a las evasiones.

  Entre estas técnicas se encuentran el aprendizaje automático y el análisis estático, dinámico y de hardware. WildFire cuenta con una de las mayores comunidades empresariales de análisis de malware, que permite la alimentación de este motor de análisis de distintas fuentes. Todos los dispositivos a nivel mundial de Palo Alto Networks son fuente de alimentación para el motor de análisis, cuando un dispositivo con suscripción de de WildFire detecta malware y exploits de día cero, el servicio orquesta la aplicación de medidas de protección de alta fidelidad y resistentes a las evasiones al resto de los suscriptores. El proceso se lleva a cabo automáticamente, segundos después de la primera detección en cualquier lugar del mundo.
- *Device-ID*: proporciona reglas de políticas basadas en un dispositivo específico, aunque cambie su dirección IP o su ubicación. Device-ID permite relacionar cada evento con determinados dispositivos, así como escribir políticas vinculadas a dispositivos fijos. Esta funcionalidad es primordial en arquitecturas IoT.
- *DNS Security*: este servicio permite la protección contra *malware* que utiliza DNS para establecer un canal de comando y control. DNS Security aplica técnicas de análisis predictivo, aprendizaje automático y automatización para bloquear los ataques que utilizan DNS. Su integración perfecta con el NGFW pone a su alcance mecanismos de protección automatizados, impide que los atacantes sorteen las medidas de seguridad y permite prescindir de las herramientas independientes sin cambiar el enrutamiento DNS.

Permite predecir rápidamente la existencia de dominios maliciosos, neutralizar las amenazas ocultas en la tunelización de DNS y aplica la automatización para localizar y contener los dispositivos infectados sin demora.

- *Data Loss Prevention*: este servicio basado en la nube garantiza una protección coherente y fiable de los datos sensibles en todo el tráfico, en todas las aplicaciones y para todos los usuarios. DLP permite detectar, clasificar, supervisar y proteger los datos sensibles de forma coherente, independientemente de dónde residan y se transfieran.
- *Global Protect:* es la solución de movilidad de Palo Alto Networks, lo que permite utilizar todas las funcionalidades del NGFW en los dispositivos sin importar el lugar en donde este. Esta funcionalidad lo realiza mediante un agente que se instala en los dispositivos ya sean laptops o smartphones.

  Adicionalmente, Global Protect permite el uso de aplicaciones alojadas en la nube o en el centro de datos de la empresa a través de una conexión segura y encriptada mediante el uso de una VPN sin cliente.

1.6 METODOLOGÍA DE SEGURIDAD PERIMETRAL DE FORTINET

Otra de las empresas líderes en seguridad de red es Fortinet (Gartner, 2020). Su solución permite una amplia protección integrada y automatizada contra amenazas, utiliza unidades de procesamiento de seguridad (SPU) especialmente diseñadas y se integra con los servicios de inteligencia de amenazas de FortiGuard Lab para brindar seguridad y protección contra amenazas (Fortinet, 2019).

1.6.1 Arquitectura de seguridad de Fortinet

La arquitectura de seguridad de Fortinet es conocida como Security Fabric la cual segmenta toda la red, desde el Internet de las cosas (IoT) hasta la nube, para proveer protección contra amenazas sofisticadas.

Los NGFW de Fortinet inspeccionan el tráfico a medida que entra y sale de la red, estas inspecciones ocurren a una velocidad, escala y rendimiento incomparables para garantizar que solo se permita el tráfico legítimo, sin degradar la experiencia del usuario (Fortinet, 2020e).

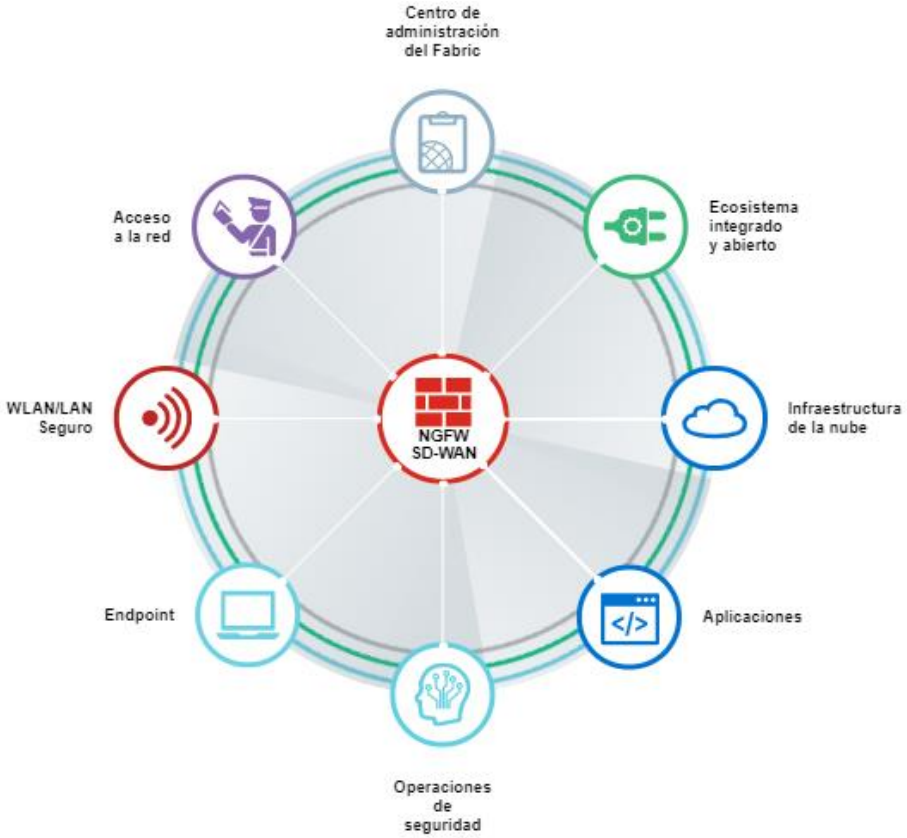


Figura 1-7 Arquitectura Security Fabric de Fortinet
Fuente: (Fortinet, 2020g)

La base principal de los dispositivos de seguridad de Fortinet son sus unidades de procesamiento de seguridad (SPU) que cumplen con su principio fundador clave el cual es que los dispositivos de seguridad nunca deben convertirse en un cuello de botella de rendimiento dentro de una arquitectura de red y seguridad, ni deben sacrificar la visibilidad, experiencia del usuario o seguridad para lograr el rendimiento requerido de una aplicación (Fortinet, 2020d).

Las unidades de procesamiento de seguridad han ido mejorándose a lo largo del tiempo y a continuación, se detalla los tres componentes principales de las SPU (Fortinet, 2020d):

- *Unidad de procesamiento de redes*: los procesadores de red, como el NP7, se ejecutan en la capa de red para acelerar el funcionamiento que suele ralentizar al CPU como por ejemplo IPv4, IPv6 entre otros. Operan en línea y aceleran la desencriptación IPsec, la terminación VXLAN y la traducción de direcciones, mientras que proporciona el registro de hardware y la aplicación de políticas.

- *Unidad de procesamiento de contenido*: opera como coprocesador de la CPU principal, sumiendo funciones de seguridad de muchos recursos como el descifrado SSL/TLS, IPS y antivirus. Fortinet desarrollo el procesador de novena generación, CP9 que también realiza una inspección rápida del tráfico en tiempo real para identificar aplicaciones sin comprometer la experiencia del usuario. Su propósito es descargar el procesamiento del CPU principal para acelerar las funciones de seguridad.
- *Sistema de chip*: es el encargado de consolidar las funcionalidades de procesamiento de red y de contenido en un solo chip lo cual proporciona una identificación rápida de las aplicaciones, dirección y rendimiento de superposición. Fortinet fabricó el chip de cuarta, SoC4, que es un conjunto de funciones de seguridad completamente integrado, incluido un firewall de Capa 7, en un chip rápido y rentable.

1.6.2 Servicios de seguridad de Fortinet

Los NGFW de Fortinet se integran con todas las soluciones del fabricante y de terceros, e inclusive se beneficia de los servicios de FortiGuard, y FortiSandbox que son impulsados por inteligencia artificial para amenazas de día cero (Fortinet, 2020e).

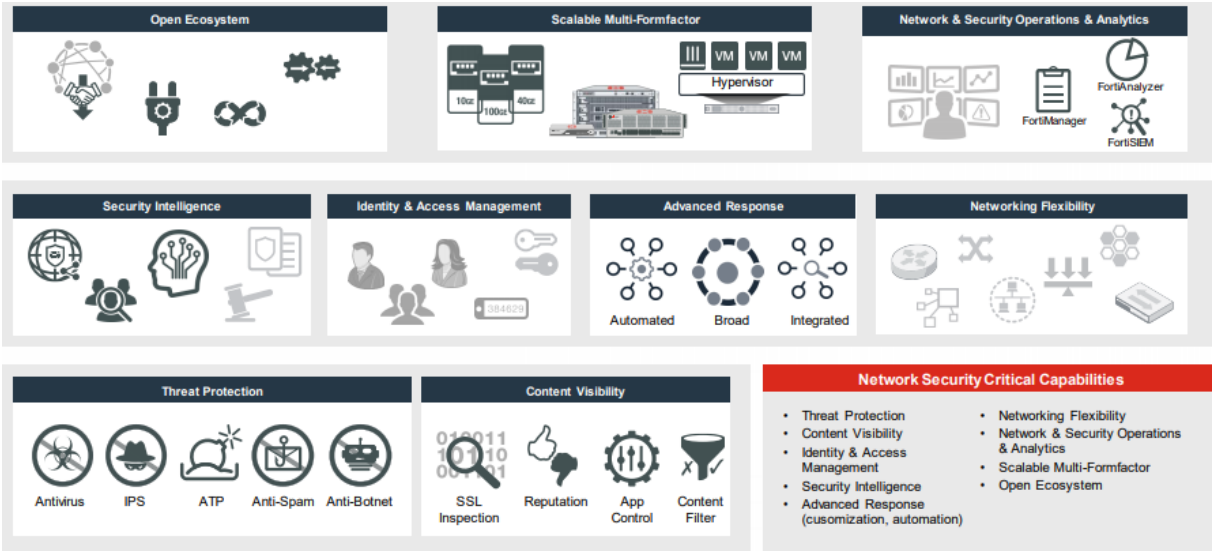


Figura 1-8 Componentes de la arquitectura de Fortinet
Fuente: (Samote, 2020)

Fortinet en base a su arquitectura Security Fabric mostrada en la Figura 1-8, segmenta sus servicios dependiendo de las capacidades críticas para la seguridad de la red. Los servicios que Fortinet ofrece para sus NGFW son los siguientes (Fortinet, 2020e):

- *FortiManager Cloud:* los NGFW al igual que otros dispositivos de la solución pueden ser administrados y aprovisionados de manera centralizada y sin intervención a través de este servicio en la nube. Esta es una consola que permite funciones de configuración, cambios y cumplimiento de mejores prácticas.
- *FortiAnalyzer Cloud:* es un servicio basado en la nube que permite el análisis en tiempo real de anomalías en la red.
- *FortiSandbox Cloud:* es una solución basada en la nube para la detección de amenazas avanzadas que realiza análisis dinámicos para identificar *malware* desconocido o de día cero. La inteligencia accionable que genera FortiSandbox retroalimenta a los controles preventivos dentro de la red de los clientes de Fortinet.
- *Application Control*: esta funcionalidad del NGFW tiene la capacidad de crear rápidamente políticas para permitir o restringir el acceso a aplicaciones o a categorías enteras de aplicaciones.
- *Web Filtering*: es capaz de bloquear el acceso a sitios web malicioso, pirateados o inapropiados, inclusive previene la descarga de malware a través de Internet en sitios web hackeados.
- *Antivirus*: es el modulo encargado de la protección contra los más recientes virus, spyware y otras amenazas a nivel de contenido. Utiliza los motores de detección avanzada para evitar que las amenazas nuevas y en evolución obtengan una posición establecida dentro de su red y accedan a contenido valioso.
- *Prevención de intrusiones*: permite la detección y bloqueo de amenazas de intrusión antes de llegar a los dispositivos de red. Realiza su análisis en base a firmas de vulnerabilidades y exploits conocidos, aunque en conjunto con FortiGuard, también puede detectar vulnerabilidades de día cero.
- *Protección contra brotes de virus*: este servicio trabaja en conjunto con FortiGuard y FortiSandbox, cierra la brecha de seguridad al momento de realizar actualizaciones de antivirus, detecta y detiene las amenazas de malware que se descubren hasta que las firmas se propaguen por todos los clientes de Fortinet. Esto es posible ya que este servicio está constantemente realizando búsquedas en tiempo real de la base de datos de inteligencia frente amenazas.

- *Reputación de IP y seguridad antibotnet*: utiliza el servicio de FortiGuard el cual agrega la información de reputación de un IP de tal manera que se pueda tener una base actualizada de fuentes hostiles para prevenir su acceso. Tanto las firmas como los bots evolucionan constantemente y los hosts comprometidos pueden ser una brecha de seguridad que permita el acceso de malware a la empresa lo cual puede llegar a la etapa de comando y control en el ciclo de vida del ataque; al tener una base de reputación de IP, es factible el bloqueo de ese tráfico y así neutralizar la amenaza.

Estos servicios Fortinet los ofrece en bundles que dependiendo de la necesidad de la red pueden ser útiles unos más que otros. A continuación la Tabla 1-3, muestra los bundles y los servicios de cada uno de ellos.

Tabla 1-3 Bundles ofertados por Fortinet

Servicio	Advanced Threat Protection (ATP)	Unified Protection (UTM)	Enterprise Protection (ENT)	360 Protection
FortiManager Cloud				✓
FortiAnalyzer Cloud				✓
Monitoreo asistido en la nube de la SD-WAN				✓
Superposición de VPN de un clic de SD-WAN				✓
Servicio FortiConverter				✓
Servicio de seguridad industrial			✓	✓
Clasificaciones de seguridad			✓	✓
CASB			✓	✓
Filtro de correo no deseado		✓	✓	✓
Web Filtering		✓	✓	✓
Protección contra malware avanzado	✓	✓	✓	✓
IPS	✓	✓	✓	✓
FortiCare + Application Control	✓	✓	✓	✓

Fuente: (Fortinet, 2020e)

1.7 METODOLOGÍA DE SEGURIDAD PERIMETRAL DE CHECK POINT

Check Point se encuentra en el cuadrante de Gartner de firewalls de red también como líder (Gartner, 2020) su metodología se basa no únicamente en detectar y mitigar, sino también en prevenir. Su arquitectura proporciona una prevención inteligente, automática e inmediata de amenazas que sella las brechas de seguridad, además, presenta una gestión de seguridad unificada para una operación más eficiente (Check Point, 2020c).

1.7.1 Arquitectura de seguridad de Check Point

La arquitectura de Check Point actualmente conocida como Infinity, permite la protección de ciberataques a nivel de la red, el dispositivo final, dispositivo móvil y de la nube, combinando una infraestructura multicapa de soluciones de prevención de amenazas. Esta arquitectura se basa en tres elementos principales (Check Point, 2020a):

- *Prevención de amenazas*: Check Point ha enfocado sus esfuerzos en innovar tecnología y productos que prevengan los ataques a diferencia de otras marcas que se enfocan en la detección y remediación. Estas tecnologías de prevención están diseñadas para detener ataques de día cero e inclusive tienen la capacidad de detener la comunicación de comando y control en caso de que el atacante haya penetrado el perímetro.
- *Plataforma unificada*: todos los dispositivos de la arquitectura comparten un software en común y son administrados y monitoreados por la misma plataforma a través de la cual se comparte la inteligencia de amenazas recolectada. Infinity es la arquitectura sobre la que opera toda la infraestructura de seguridad como un muro de protección único y cohesivo.
- *Theat Intelligence*: conocida como ThreatCloud es la que distribuye las actualizaciones de nuevas amenazas en tiempo real a toda la solución. Esta nube de inteligencia permite la integración a través de APIs con el fin de implementar estrategias de protección orientadas a los beneficios de la empresa.

La arquitectura de Check Point Infinity además, utiliza el modelo de *Zero-Trust* y permite la segmentación para aplicar el concepto de “dividir y gobernar”, disminuyendo el riesgo de

movimiento lateral. La segmentación que permite Infinity puede realizarse a nivel de la red privada así como también de la nube sea privada o pública (Check Point, 2020g).

Check Point Infinity posee una visibilidad detallada de los usuarios, los grupos, las aplicaciones, las máquinas y los tipos de conexión en la red, lo que permite establecer y hacer cumplir una política de acceso de menos privilegios. Por lo tanto, solo los usuarios y dispositivos adecuados pueden acceder a sus activos protegidos (Check Point, 2020g).

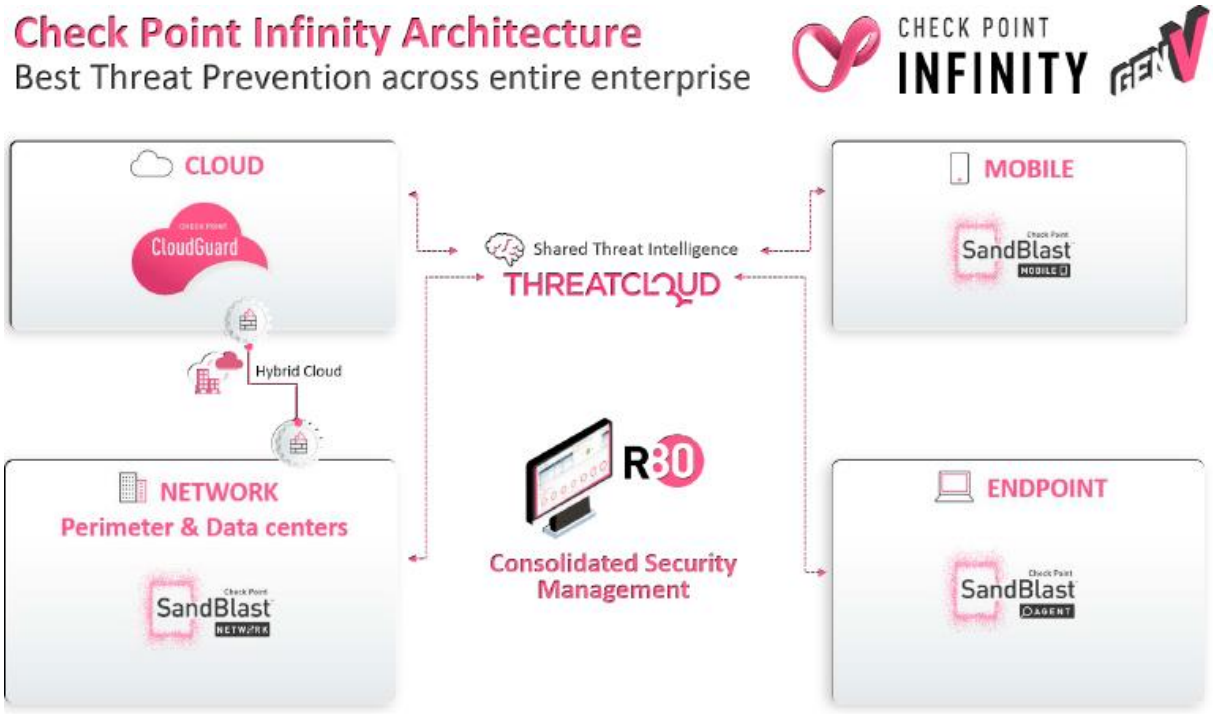


Figura 1-9 Componentes de la arquitectura de Check Point Infinity
Fuente: (Check Point, 2020a)

A partir de la versión R80, Check Point unificó su arquitectura de administración y configuración de políticas para realizarlo en un solo paso como muestra la Figura 1-10 ya no por módulos.

Name	Source	Destination	Services & Applications	Content	Action	Install On
Access to Internet according to Web control policy	InternalZone	Internet	Any	Any	Web Control	Policy Targets
DNS server should have access to	DNS Server	ExternalZone	domain-udp-Protocol-Signature... domain-tcp-Protocol-Signature-...	Any	Accept	Policy Targets
Block abuse/ high risk applications	Corporate LANs Branch Office LAN	Internet	Inappropriate Sites	Any	Drop Blocked Message - Access Control	Corporate-GW
HR can access to social network applications	HR	Internet	Facebook Twitter LinkedIn	Any	Inform Access Approval Once a day Per application/site	Policy Targets

Figura 1-10 Configuración de políticas de seguridad en Chek Point
Fuente: (Check Point, 2020a)

Esto facilitó enormemente a los administradores ya que con la configuración de una sola política se puede aplicar diferentes módulos de protección como lo son antivirus, IPS, entre otros.

Ahora con Integrated Security & Threat Management se tiene un entorno de gestión de seguridad unificado multidispositivo, multidominio y multi-administrador. Permite la visualización completa de amenazas que permite la recopilación, correlación y análisis de ataques, y herramientas de informes para el cumplimiento y auditoría (Check Point, 2020b).

1.7.2 Módulos de seguridad de Check Point

Check Point al tener una arquitectura en base a módulos, estos se activan dependiendo del tipo de solución y las necesidades que se requieran. A continuación, se detalla las funcionalidades que incluye cada uno de los módulos (Check Point, 2017):

- *Módulo Firewall*: este módulo es la base con la que inició Check Point en el mundo de seguridad perimetral, incluye las funcionalidades de Statefull Inspection Firewall.
- *Módulo VPN*: integra control de acceso, autenticación y cifrado para garantizar una conectividad segura a las redes corporativas para usuarios remotos y móviles, sucursales a través de Internet.
- *Módulo IPS*: este modulo ofrece una prevención de intrusiones completa y proactiva, con las ventajas de implementación y administración de una solución de firewall unificada
- *Módulo Application Control*: con este módulo se puede crear fácilmente políticas granulares en base a usuarios o grupos de usuarios y permite la identificación de aplicaciones, mantiene un motor de más de 7000 aplicaciones y widgets que se actualiza constantemente.
- *Módulo Content Awareness*: este módulo permite la visibilidad del contenido del tráfico que circula por la red, permitiendo la configuración de políticas de acceso que incluya los permisos de dirección y el tipo de archivo que puede ser transmitido.
- *Módulo URL Filtering*: integra las funcionalidades de Application Control unificándolo con aspectos de seguridad web.

- *Módulo Anti-Bot*: detecta los dispositivos comprometidos por botnets, previene los daños de los bots al bloquear la comunicación de comando y control, y se actualiza continuamente desde la nube de Check Point conocida como ThreatCloud.
- *Módulo Anti-Virus*: detiene los archivos maliciosos entrantes utilizando firmas de virus en tiempo real y protecciones basadas en anomalías que se integran también con ThreatCloud.
- *Módulo Anti-Spam*: proporcional una protección integral para la infraestructura de mensajería de una empresa.
- *Módulo SandBlast Threat Emulation*: este módulo es el encargado de evita infecciones de amenazas de día cero, nuevo malware y ataques dirigidos. Este innovador motor ofrece una alta tasa de detección de amenazas posible y es prácticamente inmune a las técnicas de evasión de los atacantes.
- *Módulo SandBlast Threat Extraction*: elimina el contenido explotable, incluido el contenido activo y los objetos incrustados, reconstruye archivos para eliminar amenazas potenciales y entrega contenido desinfectado a los usuarios.

Con la arquitectura de Check Point Infinity se presentan tres esquemas o bundles que se pueden activar para los módulos de seguridad los cuales se presentan en la Tabla 1-4.

Tabla 1-4 Bundles de funcionalidades de Check Point

Technology	NGFW	NGTP	SandBlast
Firewall	✔	✔	✔
VPN (IPsec)	✔	✔	✔
IPS	✔	✔	✔
Application Control	✔	✔	✔
Content Awareness	✔	✔	✔
URL Filtering		✔	✔
Anti-bot		✔	✔
Anti-Virus		✔	✔
Anti-Spam		✔	✔
SandBlast Threat Emulation			✔
SandBlast Threat Extraction			✔

Fuente: (Check Point, 2020g)

1.7.3 Funcionalidades bajo suscripción de Check Point

Check Point permite el uso de sus servicios de seguridad en modalidad de suscripción anual, dentro de estas funcionalidades se encuentran las siguientes (Check Point, 2020b):

- *Real-time Threat Prevention*: es el servicio encargado de la protección de amenazas persistentes avanzadas, de malware de día cero, de ransomware y botnet. Utiliza los beneficios de sandbox en la nube que utiliza aprendizaje automático de nuevas amenazas.
- *Advanced Network Security*: este servicio integra la prevención de intrusiones y control de aplicaciones para el soporte de cualquier tipo de red hasta redes de empresas a nivel mundial orientado a la nube privada y pública.
- *Data Protection*: servicio orientado a la protección de ransomware conocido y desconocido, ofrece protección de datos y cifrado de documento, seguridad de navegador y análisis forense de seguridad.
- *Security Services*: servicio encargado de las actualizaciones de seguridad en tiempo real (ThreatCloud), actualizaciones de software, hardware. Check Point ofrece dentro de sus servicios bajo suscripción soporte y mantenimiento 24x7, clases de formación, talleres de consultoría, chequeos de seguridad y respuesta a incidentes para sus clientes finales.

1.8 NORMA ISO/IEC 27000

La norma ISO/IEC 27000 incluye una visión general de la familia de normas y una introducción a los Sistemas de Gestión de Seguridad de la Información (SGSI) describiendo el ciclo de mejora continua. La norma principal de esta serie es la ISO/IEC 27001 la cual contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (Inteco, 2012). Mediante la aplicación de un SGSI basado en las normas ISO/IEC 27000, se puede determinar la arquitectura y las políticas de seguridad acorde a las necesidades de la empresa manteniendo una gestión de riesgos y minimizando las vulnerabilidades de la red y de la información.

La familia de estándares relacionados con SGSI se muestra en la Figura 1-11. Los cuales han sido segmentados de acuerdo a las funcionalidades de los mismos.

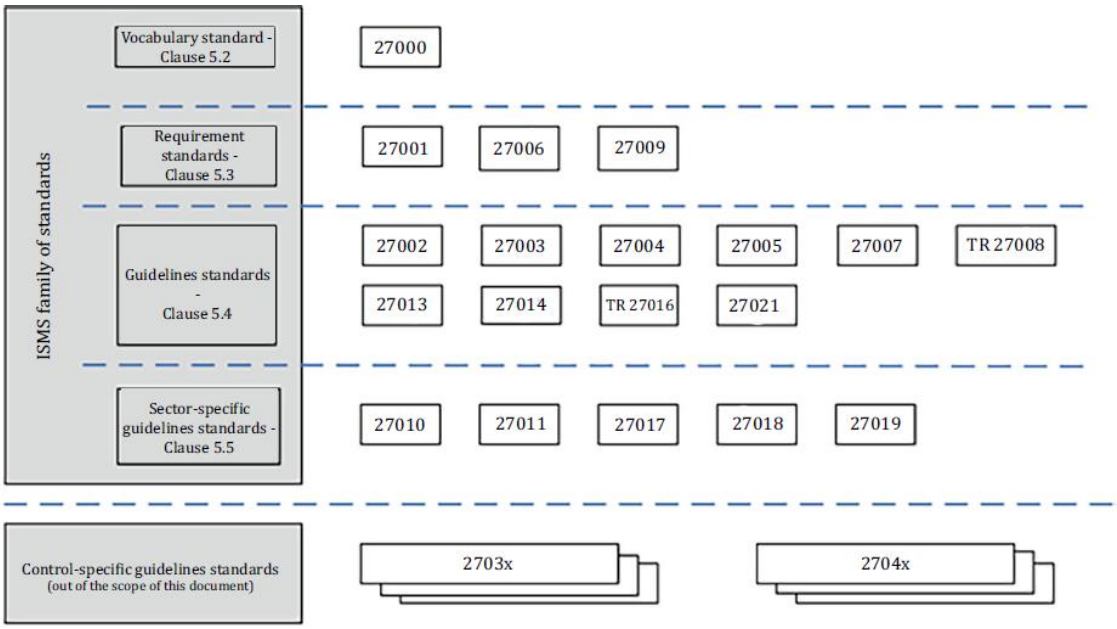


Figura 1-11 Familia de estándares relacionados con SGSI
Fuente: (ISO/IEC, 2018)

1.8.1 Clausula 5.2 Descripción general y terminología

- *ISO/IEC 27000*: describe de manera general los fundamentos de un sistema de gestión de la información, las tecnologías de información, las técnicas de seguridad y además la definición de los términos utilizados a lo largo de todo el documento relacionado con esta norma (ISO/IEC, 2018).

1.8.2 Clausula 5.3 Requerimientos específicos

Dentro de esta cláusula se encuentra tres normas que permiten determinar los requerimientos específicos para que una organización cuente con un SGSI adecuado y si es factible con su respectiva certificación, a continuación se detallan dichas normas (ISO/IEC, 2018):

- *ISO/IEC 27001*: especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar los sistemas de administración de seguridad de la información (SGSI) formalizados dentro del contexto de los riesgos generales de la organización. Especifica los requisitos para la implementación de controles de seguridad de la información personalizados para las necesidades de organizaciones individuales o partes de las mismas.
- *ISO/IEC 27006*: especifica los requisitos y proporciona orientación para los organismos que proporcionan auditoría y certificación SGSI de acuerdo con ISO/IEC 27001, además

de los requisitos contenidos en ISO/IEC 17021. Su objetivo principal es respaldar la acreditación de los organismos de certificación que proporcionan la certificación SGSI de acuerdo con ISO/IEC 27001.

- *ISO/IEC 27009*: define los requisitos para el uso de ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector de mercado). Explica cómo incluir requisitos adicionales a los de ISO/IEC 27001, cómo refinar cualquiera de los requisitos de ISO/IEC 27001 y cómo incluir controles o conjuntos de control además de ISO/IEC 27001:2013.

1.8.3 Clausula 5.4 Descripción de pautas generales

Esta cláusula incluye 10 normas que describen de manera general las guías para que las organizaciones puedan implementar un SGSI, a continuación, en la Tabla 1-5 se detalla de manera general estas normas (ISO/IEC, 2018):

Tabla 1-5 Estándares de descripción de pautas generales

NORMA ISO/IEC	ALCANCE
27002	Proporciona una lista de objetivos de control comúnmente aceptados y controles de mejores prácticas que se utilizarán como guía de implementación al seleccionar e implementar controles para lograr la seguridad de la información.
27003	Proporciona una explicación y orientación sobre ISO/IEC 27001:2013. Además, proporciona antecedentes para la implementación exitosa del SGSI de acuerdo con ISO/IEC 27001.
27004	Proporciona directrices destinadas a ayudar a las organizaciones a evaluar el desempeño de la seguridad de la información y la eficacia del SGSI para cumplir con los requisitos de ISO / IEC 27001:2013.
27005	Proporciona pautas para la gestión de riesgos de seguridad de la información. El enfoque respalda los conceptos generales especificados en ISO/IEC 27001.
27007	Proporciona orientación sobre la realización de auditorías de SGSI, así como orientación sobre la competencia de los auditores de sistemas de gestión de seguridad de la información, además de la orientación contenida en ISO 19011, que es aplicable a los sistemas de gestión en general.

TR 27008	Proporciona orientación sobre la revisión de la implementación y operación de los controles, incluida la verificación del cumplimiento técnico de los controles del sistema de información, de conformidad con los estándares de seguridad de la información establecidos por una organización.
27013	Se centra exclusivamente en la implementación integrada de un sistema de gestión de seguridad de la información (SGSI) como se especifica en ISO/IEC 27001 y un sistema de gestión de servicios (SMS) como se especifica en ISO/IEC 20000-1.
27014	Proporciona orientación sobre los principios y procesos para la gobernanza de la seguridad de la información, mediante los cuales las organizaciones pueden evaluar, dirigir y supervisar la gestión de la seguridad de la información.
TR 27016	Proporciona una metodología que permite a las organizaciones comprender mejor económicamente cómo valorar con mayor precisión sus activos de información identificados, valorar los riesgos potenciales para esos activos de información, apreciar el valor que los controles de protección de la información brindan a estos activos de información y determinar el nivel óptimo de recursos a ser aplicada para asegurar estos activos de información
TR 27021	Especifica los requisitos de competencia para los profesionales de SGSI que lideran o participan en el establecimiento, implementación, mantenimiento y mejora continua de uno o más procesos del sistema de gestión de seguridad de la información que cumplen con ISO/IEC 27001:2013.

Fuente: (ISO/IEC, 2018)

1.8.4 Clausula 5.5 Descripción de pautas específicas

Dentro de la cláusula de descripción de pautas especificas se presentan 6 normas que definen de manera más explícita los lineamientos para un sistema SGSI dependiendo del servicio al que se oriente. En la Tabla 1-6 se detalla el alcance de estas normas (ISO/IEC, 2018):

Tabla 1-6 Estándares de descripción de pautas específicas

NORMA ISO/IEC	ALCANCE
27010	Proporciona directrices además de la orientación proporcionada en la familia de normas ISO / IEC 27000 para implementar la gestión de la seguridad de la información dentro de las comunidades de intercambio de información.

	Además, proporciona controles y orientación específicamente relacionados con el inicio, implementación, mantenimiento y mejora de la seguridad de la información en las comunicaciones entre organizaciones e intersectoriales.
27011	Proporciona directrices que respaldan la implementación de controles de seguridad de la información en organizaciones de telecomunicaciones. Permite a las organizaciones de telecomunicaciones cumplir con los requisitos básicos de gestión de seguridad de la información de confidencialidad, integridad, disponibilidad y cualquier otra propiedad de seguridad relevante.
27017	Proporciona pautas para los controles de seguridad de la información aplicables a la prestación y el uso de servicios en la nube al proporcionar un guía de implementación adicional para los controles relevantes especificados en ISO/IEC 27002 y controles adicionales con orientación de implementación que se relacionan específicamente con los servicios en la nube.
27018	Establece objetivos de control, controles y pautas comúnmente aceptados para implementar medidas para proteger la información de identificación personal (PII) de acuerdo con los principios de privacidad en ISO/IEC 29100 para el entorno de computación en la nube pública.
27019	Proporciona orientación basada en la norma ISO/IEC 27002:2013 aplicada a los sistemas de control de procesos utilizados por la industria de servicios de energía para controlar y monitorear la producción o generación, transmisión, almacenamiento y distribución de energía eléctrica, gas, petróleo y calor, y para el control de procesos de apoyo asociados. No se aplica al dominio de control de procesos de las instalaciones nucleares, este dominio está cubierto por IEC 62645. También incluye un requisito para adaptar los procesos de evaluación y tratamiento de riesgos descritos en ISO/IEC 27001:2013 a la guía específica del sector de la industria de servicios públicos de energía.
27799	Proporciona pautas para los estándares de seguridad de la información de la organización y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles, teniendo en cuenta el entorno de riesgo de seguridad de la información de la organización.

	Proporciona una guía de implementación para los controles descritos en ISO/IEC 27002 y los complementa cuando es necesario, de modo que se puedan usar de manera efectiva para administrar la seguridad de la información de salud.

Fuente: (ISO/IEC, 2018)

1.9 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN

Un sistema de gestión de la seguridad de la información (SGSI) está conformado por las políticas, procedimientos, pautas, recursos y actividades orientados a proteger los activos de información de una empresa. El diseño e implementación de un SGSI está influenciado por las necesidades y objetivos de cada empresa y esta estandarizado bajo el conjunto de normas ISO/IEC 27000 (ISO/IEC, 2018).

1.9.1 Características de un SGSI

Un SGSI es un sistema que permite establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización. Los SGSI se basan en la evaluación de riesgos y los niveles de aceptación de riesgos que una empresa puede aceptar. Para una implementación exitosa de un SGSI, es necesario conocer los requisitos de protección de la información de la empresa y así poder determinar los controles adecuados para garantizar dicha protección (ISO/IEC, 2018).

Un SGSI está definido en base a la familia de estándares de la norma ISO/IEC27000 y se orienta a la protección de la confidencialidad, integridad y disponibilidad de la información de una empresa. Es por esto que las medidas de control o seguridad se presentan bajo políticas definidas y orientadas al giro de negocio y a las recomendaciones técnicas de seguridad de información (Delgado, 2018).

La seguridad de la información se logra mediante la implementación de un conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgos elegido y gestionados mediante un SGSI, que incluye políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados (ISO/IEC, 2018).

Un sistema de gestión utiliza los recursos que permiten lograr los objetivos de la empresa, el cual incluye una estructura organizativa, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos y procesos (ISO/IEC, 2018).

Un sistema de gestión con relación a la seguridad de la información permite lo siguiente (ISO/IEC, 2018):

- Satisfacer los requisitos de seguridad de la información de los clientes y otras partes interesadas.
- Cumplir con los objetivos de seguridad de la información de la organización.
- Cumplir con las regulaciones, la legislación y los mandatos de la industria.
- Administrar los activos de información de una manera organizada que facilite la mejora continua y el ajuste a los objetivos organizacionales actuales

Una empresa que adopta el sistema de gestión de seguridad de la información debe realizar los siguientes pasos descritos en la Tabla 1-7 para establecer, monitorear, mantener y mejorar su SGSI. Para garantizar que el SGSI esté protegiendo eficazmente los activos de información de la empresa, es necesario que estos pasos se repitan continuamente para identificar cambios en los riesgos o en las estrategias comerciales de la empresa (ISO/IEC, 2018).

Tabla 1-7 Pasos para garantizar un correcto funcionamiento de un SGSI

	DESCRIPCION
Identificación de los requisitos de seguridad de la información	Los requisitos de seguridad de la información se pueden identificar mediante la comprensión de lo siguiente: • Activos de información identificados y su valor. • Necesidades de procesamiento, almacenamiento y comunicación. • Requisitos legales, reglamentarios y contractuales. Al identificar los requisitos, es necesario evaluar el riesgo y el impacto que provocaría una amenaza materializada, de esta forma se podría determinar los controles de manera proporcional al impacto del riesgo.
Evaluación de riesgos de seguridad de la información	La gestión de los riesgos de seguridad de la información requiere una evaluación adecuada y un método de tratamiento de riesgos que puede incluir estimación de los costos y beneficios, requisitos legales, preocupaciones de las partes interesadas y otras entradas y variables según corresponda.

	La ISO/IEC 27005 proporciona una guía de gestión de riesgos de seguridad de la información, que incluye asesoramiento sobre evaluación, tratamiento, aceptación, informes, monitoreo y revisión de riesgos.
Tratar los riesgos de seguridad de la información	En este punto es necesario definir el nivel de aceptación de los riesgos antes de tratarlos, ya que pueden existir riesgos de bajo impacto que no requieran un tratamiento o riesgos que el costo de tratamiento no sea rentable. En caso de decidir tratar los riesgos, el tratamiento debe incluir lo siguiente: • Aplicar controles adecuados para reducir los riesgos. • Aceptar los riesgos de forma consciente, siempre que satisfagan la política y los criterios de la empresa para la aceptación de riesgos. • Evitar riesgos al no permitir acciones que causarían que ocurrieran. • Compartir los riesgos asociados con otras partes, por ejemplo, aseguradoras o proveedores.
Seleccionar e implementar controles	Los controles deben garantizar que los riesgos se reduzcan a un nivel aceptable teniendo en cuenta lo siguiente: • Requisitos y limitaciones de la legislación y los reglamentos nacionales e internacionales; • Objetivos de la empresa • Requisitos y limitaciones operacionales. • Su costo de implementación y operación. • Sus objetivos para monitorear, evaluar y mejorar la eficiencia y efectividad de los controles de seguridad de la información. • La necesidad de equilibrar la inversión en la implementación y operación de controles con la pérdida que probablemente resulte de los incidentes de seguridad de la información. Los controles especificados en ISO/IEC 27002 se reconocen como las mejores prácticas aplicables a la mayoría de las empresas y se adaptan fácilmente.
Monitorear, mantener y mejorar la efectividad del SGSI	Una empresa debe mantener y mejorar el SGSI mediante el seguimiento y la evaluación del desempeño frente a las políticas y los objetivos de la organización, reportando los resultados a la gerencia para su revisión.

	Además, con base en al monitoreo continuo se proporciona evidencia de verificación y trazabilidad de acciones correctivas, preventivas y de mejora.
Mejora continua	El objetivo de la mejora continua de un SGSI es aumentar la probabilidad de lograr objetivos relacionados con la preservación de la confidencialidad, disponibilidad e integridad de la información. Es la búsqueda constante de oportunidades de mejora, sin asumir que las actividades existentes son suficientes.

Fuente: (ISO/IEC, 2018)

1.9.2 Beneficios de un SGSI

Uno de los principales beneficios de la implementación de un sistema de gestión de seguridad de la información, es a reducción significativa de riesgos de seguridad y pérdida de información. También puede incluir otros beneficios que se mencionan a continuación (ISO/IEC, 2018):

- Un marco estructurado que respalda el proceso de especificar, implementar, operar y mantener un SGSI integral, rentable, que crea valor y que satisfaga las necesidades de la organización en diferentes operaciones y sitios.
- Asistencia en la administración de manera consistente y responsable con enfoque hacia la seguridad de la información, dentro del contexto de riesgos corporativos, incluida la educación y capacitación de los propietarios de negocios y sistemas sobre la administración integral de la seguridad de la información.
- La promoción de buenas prácticas de seguridad de la información globalmente aceptadas de manera no prescriptiva, dando a las organizaciones la libertad de adoptar y mejorar los controles relevantes que se adapten a sus circunstancias específicas y para mantenerlos frente a cambios internos y externos.
- Provisión de un lenguaje común y una base conceptual para la seguridad de la información, lo que facilita la confianza en los socios comerciales con un SGSI compatible, especialmente si requieren la certificación según ISO/IEC 27001 por parte de un organismo de certificación acreditado.
- Una gestión económica más eficaz de las inversiones en seguridad de la información.

1.9.3 Ciclo de Deming

Conocido también como ciclo de mejora continua o por sus siglas en inglés PDCA, es la metodología que describe en cuatro pasos esenciales y de manera sistemática los procesos para poder llegar al mejoramiento continuo de la calidad (MINTEL, 2020).

Para los sistemas de gestión de la información (SGSI), el ciclo de Deming permite descubrir los puntos vulnerables de una empresa y provee herramientas valiosas para diseñar procesos y procedimientos de seguridad eficaces para corregir esos puntos de vulnerabilidad (MINTEL, 2020). En la Tabla 1-8 se presenta las cuatro etapas del ciclo de Deming con sus funcionalidades correspondientes (MINTEL, 2020):

Tabla 1-8 Etapas del ciclo de Deming

ETAPA	DESCRIPCION
Planificar (Plan)	Esta etapa se enfoca en la identificación del alcance del SGSI, la elaboración de la política de seguridad de la información, la definición de la metodología de análisis y evaluación de riesgos, la elaboración del plan de comunicación, y su ejecución. En los procesos de mejora continua, en esta etapa se planifica los cambios y se define el alcance de los mismos, se realiza un esquema en papel de los pasos a seguir para la ejecución de los cambios.
Hacer (Do)	Utilizando el esquema realizado en la etapa anterior, se pone en ejecución todo lo planificado en el orden estipulado.
Verificar (Check)	Esta etapa monitorea y revisa los resultados para determinar si están alineados con los objetivos e intenciones que son: proteger la confidencialidad, integridad y disponibilidad de la información de la empresa. Estos resultados están enfocados tanto en procesos de gestión como controles de seguridad de la información. Para revisar los resultados se realizan auditorías internas, ejecución planificada de análisis y evaluación de riesgos, revisiones gerenciales.
Actuar (Act)	En esta etapa final, se realizan mejoras al SGSI en caso de que la etapa anterior haya encontrado situaciones que no estuvieron alineadas con los objetivos. De haber existido recomendaciones para las mejoras al SGSI, el proceso se debe repetir para aplicar acciones correctivas y confirmar su efectividad en cerrar las causas de las situaciones anómalas.

Fuente: (MINTEL, 2020)

Los procesos del clico de Deming forman parte de varias normas de la ISO, sin embargo, en la norma ISO/IEC 27001:2013 se lo ha eliminado, a pesar de que se requiere una gestión de mejora, no obliga a usar el modelo de ciclo de PDCA. Cabe recalcar que sigue siendo utilizado hasta la actualidad aunque no se lo mencione en la norma y en la Figura 1-12 se puede observar los procesos para cada uno de las etapas del ciclo PDCA orientado al SGSI (MINTEL, 2020).

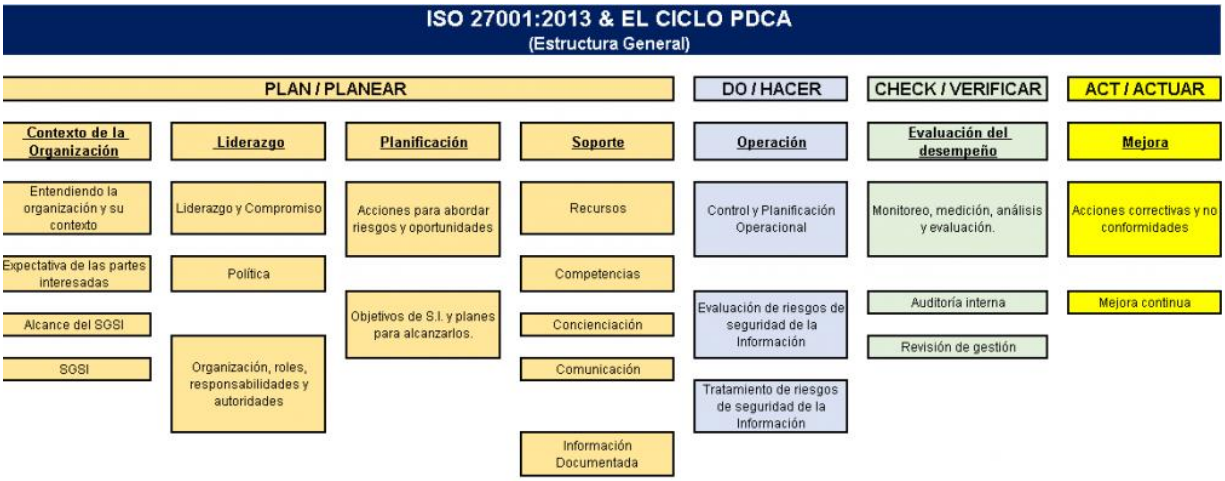


Figura 1-12 Ciclo PDCA orientado a la norma ISO/IEC 270001 para SGSI
Fuente: (MINTEL, 2020)

CAPÍTULO 2: MODELO Y METODOLOGÍA DE SEGURIDAD PERIMETRAL

Este capítulo se orienta a la definición del modelo y metodología de seguridad perimetral que permita a la empresa tener un control de acceso a la información a través de la red; el análisis se basa en las recomendaciones propuestas por la familia de normas de la ISO 27000 para el diseño e implementación de un sistema de gestión de seguridad de la información (SGSI).

Para poder determinar el modelo y la metodología de seguridad perimetral que opere de mejor manera en la empresa, es esencial determinar las necesidades a nivel de seguridad de la información, la arquitectura actual y los servicios que se encuentra funcionando en la empresa.

2.1 LEVANTAMIENTO DE INFORMACIÓN DE LA EMPRESA

2.1.1 Descripción de la empresa

AKEA S.A es una compañía con presencia en territorio ecuatoriano, cuyo principal objetivo se basa en ofrecer soluciones innovadoras que permitan incrementar la productividad de las organizaciones, tomando como insumo las tendencias mundiales de la industria en materia de tecnología. AKEA S.A cuenta con un equipo de profesionales especializados en distintas áreas, con amplia experiencia en la integración de soluciones, el cual tiene un propósito claro; servir con excelencia (AKEA, 2020).

La empresa AKEA S.A cuenta con sus oficinas en la Av. Portugal y Av. 6 de diciembre en la ciudad de Quito, en la cual operan alrededor de 25 personas, además cuenta con personal en campo a nivel nacional, principalmente en Guayaquil, Ambato y Loja.

Debido a la pandemia del COVID-19, la cantidad de personas que trabajan de manera presencial en las oficinas de Quito se redujo a la mitad, mientras que los demás realizan sus funciones mediante teletrabajo.

2.1.2 Misión de la empresa

AKEA S.A es una organización que provee soluciones tecnológicas corporativas, basadas en la integración o desarrollo de productos de vanguardia y servicios de alta calidad, que permiten satisfacer las necesidades de nuestros clientes y aportan en el incremento de su productividad (AKEA, 2020).

2.1.3 Visión de la empresa

Ser una empresa altamente reconocida en el territorio ecuatoriano por su calidad en la integración y entrega de soluciones llave en mano, y por promover el uso de nuevas tecnologías de acuerdo a las tendencias mundiales de la industria (AKEA, 2020).

2.1.4 Organigrama empresarial

De acuerdo al levantamiento de información y a lo indicado por el personal de la empresa, el organigrama empresarial en resumen se muestra en la Figura 2-1.

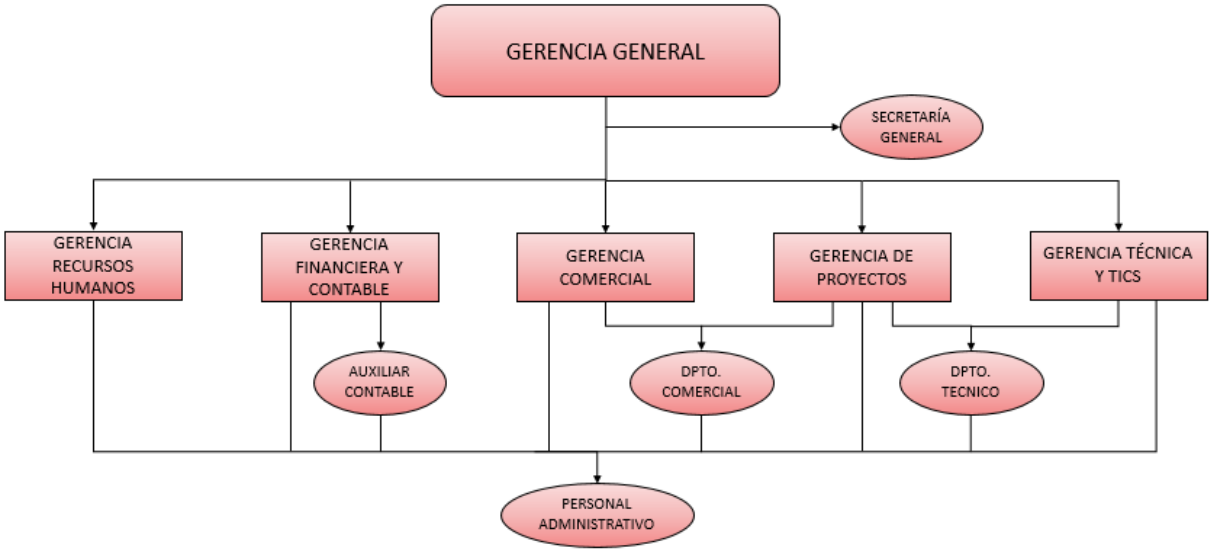


Figura 2-1 Organigrama de la empresa AKEA S.A

Se tiene definido las diferentes áreas que laboran en la empresa, así como los servicios a los cuales tienen acceso. Las políticas de seguridad y accesos son determinadas por gerencia general en conjunto con el gerente técnico y el departamento técnico.

En base al organigrama se determinar las políticas de acceso a la información y a los recursos tecnológicos que maneja la empresa de la siguiente manera:

- La información contable y financiera solo debe estar disponible para el personal del departamento contable y financiero, la gerencia general y los socios de la empresa con supervisión del gerente general.
- La información del personal que colabora en la empresa, sean empleados o contratistas solo debe estar disponible para el área de recursos humanos, secretaría general y gerencia general.

- La información confidencial referente a la infraestructura de los clientes a quienes se ha brindado servicio únicamente está disponible a través del personal del departamento de técnico, gerencia de proyectos y gerencia técnica y, en base a los acuerdos de las políticas de confidencialidad, esta información no puede ser divulgada con otros clientes o mayoristas sin consentimiento del propietario de la información de la infraestructura.
- La información de clientes a nivel comercial, como son contactos, presupuestos de proyectos, detalles institucionales solo deben estar disponibles para cada agente comercial responsable de la cuenta del cliente, así como a la gerencia comercial y a la gerencia general.
- Finalmente, el acceso y administración de los activos tecnológicos debe ser exclusivo para el personal del departamento técnico, quien debe configurar la infraestructura tecnológica con el fin de cumplir con las políticas de seguridad y de acceso de la información que defina gerencia.

2.1.5 Descripción del equipamiento

Para realizar el levantamiento de información de la infraestructura actual de la empresa, se solicitó al Gerente Técnico el acceso al rack de comunicaciones y a los servidores para el levantamiento físico y lógico, de esta manera se pudo determinar con exactitud los componentes que forman parte de la arquitectura y los servicios que circulan en la red. Por motivos de confidencialidad, se omitirá descripciones a profundidad de los servicios y direccionamiento IP. La empresa cuenta con los siguientes equipos dentro de su infraestructura, los cuales se describen a continuación en la Tabla 2-1:

Tabla 2-1 Equipamiento de la infraestructura de la empresa AKEA S.A

EQUIPO	FUNCIÓN	CARACTERÍSTICAS
Router Huawei – Netlife	ISP principal	Equipo instalado por el proveedor de servicio Netlife para el consumo de Internet a través de fibra óptica. AKEA S.A cuenta con un plan de 50Mbps para el servicio de Internet, además se tiene contratado una dirección IPv4 Pública para los servicios que son utilizados desde Internet.

Router Arris – TvCable	ISP secundario	Equipo instalado por el proveedor de servicio TVCable para el consumo de Internet a través de fibra óptica. AKEA S.A cuenta con un plan de 25Mbps para el servicio de Internet a través de una IP pública estática.
Mikrotik RouterBoard 1100AHx2	Router/Firewall	Equipo instalado por la empresa para cumplir las funciones de router y de seguridad perimetral. Este equipo de capa tres, cuenta con 13 interfaces de 1Gbps, dos switch virtuales de 5 interfaces cada uno, una memoria RAM de 2GB, un CPU de doble núcleo lo que permite hasta un millón de paquetes por segundo. Además tiene la capacidad de la creación de políticas de seguridad basadas en direccionamiento y puerto y cuenta con un módulo básico de aplicaciones (Mikrotik, 2013).
Cisco Catalyst 2960-48TC-L	Switch de acceso	Equipo instalado por la empresa para cumplir con la conexión de los equipos finales, puntos de acceso inalámbricos y servidores mediante la segmentación de VLANs. Este equipo es de capa dos, cuenta con 48 interfaces de 10/100Mbps y dos interfaces *uplink* de 1Gbps. Soporta hasta 16Gbps de reenvío de paquetes, con un máximo de 255 VLANs activas, cuenta con una transacción de 10 millones de paquetes por segundo y se lo puede instalar en 1ur de rack (Cisco, 2019).
UniFi AP-AC-Lite	Access Point	Equipos instalados por la empresa con el fin de cumplir con la conectividad inalámbrica de equipos permitiendo de esta manera la

		movilidad. Se encuentran instalados dos equipos para garantizar la cobertura total de la oficina de la empresa. Estos equipos presentan un diseño ultra compacto y operan en la banda de 2.4GHz y 5GHz a 300 Mbps y 867Mbps de velocidad respectivamente con la capacidad de 2x2 MIMO, además son administrados de manera centralizada a través de un controlador inalámbrico virtual (Ubiquiti, 2019).
UniFi Controller 5.10.25	Controlador inalámbrico	Software instalado por la empresa para la administración y monitoreo de la red inalámbrica. Este software permite la configuración centralizada de cientos de APs UniFi, permite la visualización gráfica de estado de la red, de los clientes y de los puntos de acceso, además del análisis de estadísticas de consumo y de la creación de mapas de calor de acuerdo al plano de instalación (Ubiquiti, 2019).
Yeastar MyPBX-Standard V4	Central Telefónica IP	Equipo instalado por la empresa para cumplir con la necesidad de comunicación mediante telefonía fija. Este equipo basado en Asterisk soporta hasta 100 usuarios con 22 llamadas concurrentes, posee dos puertos 10/100 Mbps, cuenta con 16 puertos para troncales análogas, 4 puertos GSM y 8 puertos BRI, soporta el protocolo SIP y los códec G.711 A/u-law, G.722, G.726, G.729 A (Yeastar, 2014).
Denwa DW-210P	Teléfonos IP	Equipos instalados por la empresa para la comunicación de telefonía fija.

		Cada usuario de la empresa que trabaja en oficina cuenta con un teléfono IP, para la comunicación con proveedores, clientes, y personal en campo. Estos equipos cuentan con 2 puertos 10/100Mbps con soporte de alimentación POE, con la capacidad de un directorio de 500 contactos, conferencia de tres vías, reenvío de llamadas, remarcado y llamada en espera (Denwa, 2020).
Lenovo ThinkSystem ST50	Servidor Contable	Equipo instalado por la empresa para el servicio de contabilidad exclusivamente. El equipo cuenta con una interfaz de red de 1Gbps, 1TB de almacenamiento, 16 Gbps de memoria RAM expandible hasta 64Gbps y 4 CPU de 3.2GHz expandible hasta 6 núcleos (Lenovo, 2020).
Lenovo ThinkServer TS150	Servidor Máquinas Virtuales	Equipo instalado por la empresa para el servicio virtuales como página web, mesa de ayuda entre otros. Este equipo fue uno de los primeros modelos lanzados por Lenovo para *small bussiness* cuenta con 2 interfaz de red de 1Gbps expandible a 9 interfaces, 1TB de almacenamiento, 16 Gbps de memoria RAM expandible hasta 64Gbps y 4 CPU de 3.0GHz (Lenovo, 2015)
HP PageWide Color MFP 586	Impresora/Escáner	Equipo instalado por la empresa para la impresión a color o blanco y negro y el escaneo de documentación. Este equipo se lo puede gestionar desde la interfaz gráfica a través de la dirección IP. Permite la impresión desde cualquier

		dispositivo que se encuentre en red, también permite el copiado y escaneo de documentos, con el envío a través de correo electrónico del documento escaneado (HP, 2019).

Fuente: (Mikrotik, 2013), (Cisco, 2019), (Ubiquiti, 2019), (Yeastar, 2014), (Denwa, 2020), (Lenovo, 2020), (Lenovo, 2015), (HP, 2019)

Adicionalmente a los equipos mencionados anteriormente, cada usuario cuenta con su propio dispositivo, ya sea laptop o PC, los cuales son en su mayoría cuentan con un sistema operativo Windows 10 y unos pocos con sistema operativo MacOS. Además de acuerdo a las políticas de la empresa, los usuarios con los permisos respectivos de gerencia pueden conectar sus dispositivos móviles a la red inalámbrica.

2.1.6 Descripción de los servicios

AKEA S.A es una empresa que se dedica al diseño, implementación y renovación de sistemas de telecomunicaciones enfocándose en las nuevas tecnologías disponibles en el mercado. Sus servicios son más orientados al consumo de tecnología, sin embargo, dentro de su arquitectura de red se encuentran ciertos servicios que ayudan al giro de negocio de la empresa, los cuales se mencionan a continuación:

- *Servidor web:* servicio virtualizado que permite el despliegue de la página web de la empresa para dar a conocer sus servicios, productos y alianzas estratégicas para llegar a ser líder en tecnología. La página web es actualizada constantemente con los eventos en los cuales la empresa suele participar, y está alojada en el rack de comunicaciones de AKEA S.A. Esta página web esta publicada al Internet en el link www.akea.ec.
- *Servidor de la mesa de ayuda:* AKEA S.A al ser una empresa que ofrece servicios de telecomunicaciones, requiere de un sistema para reporte de incidentes y control de clientes. Este servicio se encuentra virtualizado y está alojado en el rack de comunicaciones de AKEA S.A, además es un servicio publicado en Internet, para que sus clientes finales puedan abrir tickets de soporte en cualquier momento y de acuerdo a los SLA (Service Level Agreement) del contrato, obtener la mejor atención y respuesta ante sus inquietudes o problemas.

- *Servidor de contabilidad*: es un servicio virtualizado, alojado en el rack de comunicaciones de AKEA S.A en un servidor físico dedicado, para el despliegue del sistema contable de la empresa, el acceso a dicho servicio es exclusivo para el personal del área de contabilidad y facturación dentro de la red interna de la empresa, sin embargo, por la pandemia del COVID-19, actualmente, este servicio se lo puede acceder desde Internet únicamente con los usuarios registrados en el sistema.
- *Servicio de correo electrónico:* AKEA S.A cuenta con una suscripción al servicio de Office365 que Microsoft ofrece para el sistema de correo electrónico empresarial, el cual está alojado en la nube del fabricante. Esta suscripción permite la creación de buzones de correo electrónicos, agendamiento de eventos en el calendario corporativo, almacenamiento en la nube, uso de archivos compartidos de manera segura y un sistema mensajería instantánea empresarial y segura a través de Microsoft Teams, esto permite mantener una comunicación interna y externa por medio de canales seguros y oficiales.
- *Servicio de almacenamiento:* AKEA S.A al contar con Office365, cada usuario que dispone de una cuenta empresarial con acceso a 1TB de almacenamiento en la nube para documentación relevante de la empresa. Este servicio permite la compartición de documentos entre el personal de la empresa con permisos del autor del documento.

  Sin embargo, la empresa mantiene aún una carpeta compartida alojada en una PC en el rack de comunicaciones con documentación de años anteriores, el acceso es exclusivo para el personal de la empresa únicamente a través de la red interna. La migración de estos archivos a la solución de Office365 se la está realizando paulatinamente.

2.1.7 Arquitectura de red

Una vez definido los componentes y los servicios que forman parte de la infraestructura de la empresa, se define la arquitectura actual de la red, la cual se describe a continuación:

- La empresa cuenta con dos salidas de Internet, con los ISPs Netlife y TVCable, para garantizar la operatividad de los servicios en caso de caída de alguno de los proveedores.
- La red empresarial se encuentra segmentada de la siguiente manera:
  - Red de administración de equipos
  - Red de usuarios de la empresa
  - Red de usuarios invitados

- Red de servidores

- La empresa cuenta con un equipo de capa 3 Mikrotik que permite la salida a Internet de las redes internas mediante NAT (Network Address Translation). También maneja las políticas de navegación, las cuales actualmente permiten la salida de Internet sin restricciones a través del ISP principal únicamente de los dispositivos registrados por su dirección MAC en el router mediante la red de usuarios de la empresa.

  Los usuarios invitados navegan a través del ISP secundario y esta red no tiene acceso a la red de servidores ni a la red de usuarios de la empresa.
- El Mikrotik también ejecuta las funciones como servidor DHCP para cada una de las VLANs configuradas en la red, servidor DNS para la publicación de la página web y el servicio de mesa de ayuda, servicio VPN site to site para la conexión con las sucursales, servicio VPN client to site para acceso remoto desde cualquier dispositivo sea laptop o PC, sin embargo, estas dos últimas funcionalidades no están aplicadas al momento, por lo que si se requiere acceso a los servicios que están alojados en el rack de comunicaciones, es necesario estar conectados a la red interna de la empresa.
- Para la red inalámbrica, el controlador virtual, así como la administración de los puntos de acceso forman parte de la red de administración de equipos.
- A nivel de inalámbrico, se dispone de dos SSID, un SSID oculto para la red de usuarios de la empresa y un SSID abierto con la configuración de un portal cautivo para el acceso a Internet de los usuarios invitados. Esto se lo realiza mediante la generación de un ticket con usuario y contraseña desde el sistema de EasyTicket, el cual debe ser ingresado por el usuario al momento del registro en el portal cautivo, como muestra la Figura 2-2.

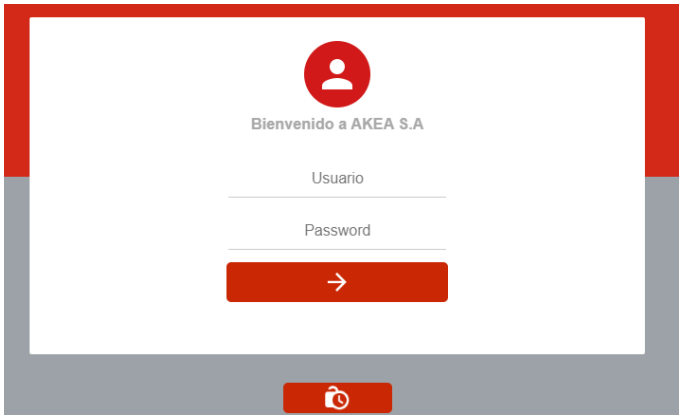


Figura 2-2 Pantalla de registro para la red de invitados

- Los servicios que se encuentran publicados en Internet forman parte de la red de servidores, así como también la plataforma de virtualización que cada servidor tiene.
- El servicio de contabilidad forma parte de la red de usuarios, ya que fue instalado previo a la segmentación de redes.
- La central telefónica y los teléfonos IP, también forman parte de la red de usuarios de la empresa, no se ha realizado segmentación de estos servicios. La central telefónica está operando con dos líneas troncales analógicas para llamadas a nivel local, nacional e internacional, además cuenta con una conexión GSM que permite las llamadas hacia celulares.

2.1.8 Diagrama de conexión

Después de analizar los componentes de la arquitectura actual, así como los servicios y el modo de operación de los mismos, se procede a realizar el diagrama de conexión representado en la Figura 2-3.

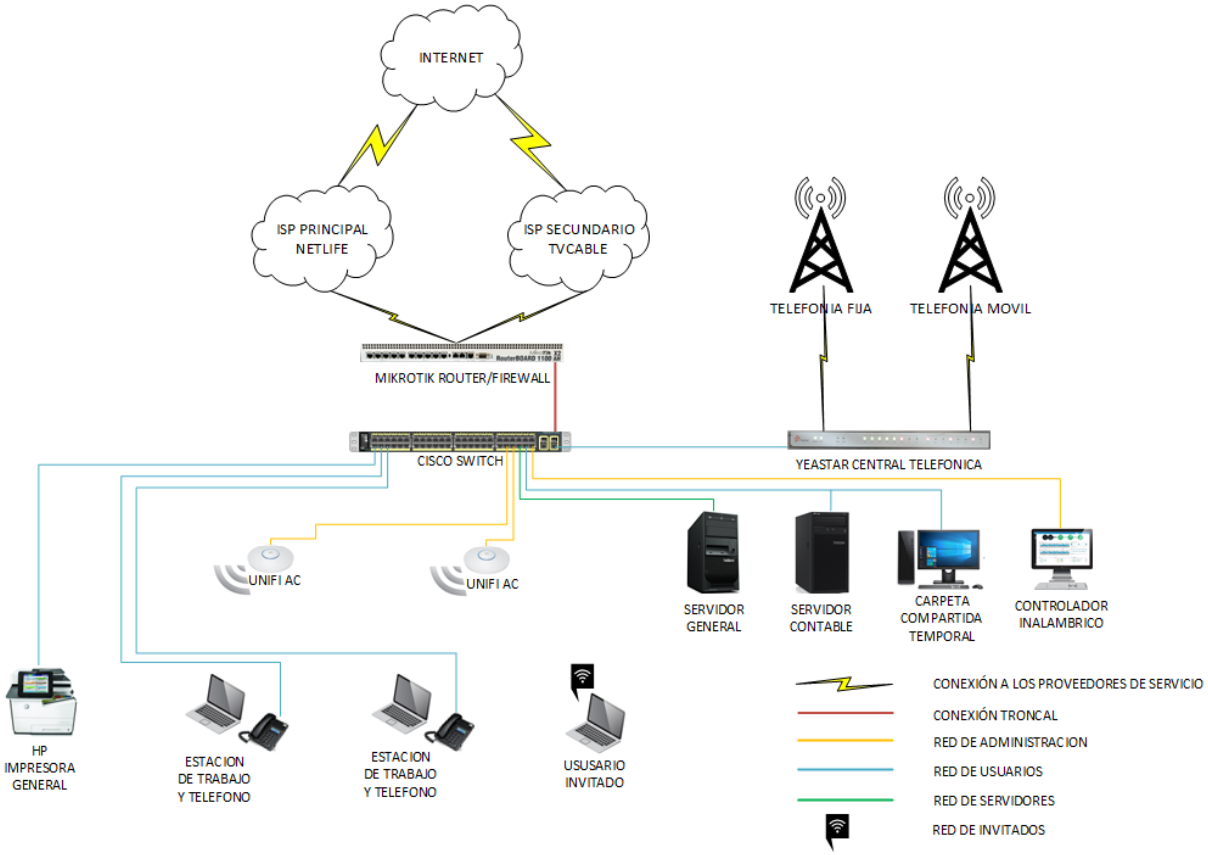


Figura 2-3 Diagrama de conexión actual

2.2 ANÁLISIS DE VULNERABILIDADES DE LA ARQUITECTURA ACTUAL

2.2.1 Identificación de vulnerabilidades

Una vez realizado el levantamiento de información físico y lógico de la empresa se procede a identificar las vulnerabilidades que la arquitectura actual presenta, sobretodo, a nivel de seguridad perimetral con el fin de poder determinar los requerimientos técnicos que debe cumplir el nuevo modelo y metodología de seguridad perimetral que se propone.

En la Tabla 2-2 se describe las vulnerabilidades encontradas para el análisis de las mismas:

Tabla 2-2 Identificación de vulnerabilidades

VULNERABILIDAD	DETALLE	IMPLICACIÓN
Publicación de servicios internos sin seguridad.	La empresa tiene publicado su página web y su servicio de mesa de ayuda hacia Internet en base al protocolo que utiliza	Las amenazas suelen venir camufladas en protocolos conocidos como por ejemplo 443, 80, 8080. Por lo que se está expuesto a ataques a través de estos protocolos.
Segmentación del servicio contable.	El servidor de contabilidad se encuentra configurado en la red de usuarios, mas no en la granja de servidores.	Al no estar segmentado el servicio contable, el acceso hacia este servidor no es controlado y cualquier funcionario podría acceder rompiendo las contraseñas configuradas.
Segmentación del servicio de telefonía IP.	El servicio de telefonía IP también se encuentra en la red de usuarios.	Comúnmente los servicios de telefonía IP se segmentan para garantizar calidad de servicio y no tener afectaciones por el consumo del resto de la red.
Falta de configuración de políticas en base a usuarios.	La empresa no cuenta con un sistema de detección por usuarios; para la red interna se maneja con restricción por Mac Address.	Al no tener un control por usuarios, los servicios internos están vulnerables al acceso de cualquier dispositivo que se

		encuentre dentro de la red interna de la empresa, y no se podría identificar la fuente del ataque.
Falta de configuración para acceso remoto VPN client to site.	La empresa no tiene configurado el acceso remoto VPN client to site por lo que, se tuvo que publicar el servicio de contabilidad para que los usuarios del departamento contable puedan laborar desde sus casa por motivo de la pandemia del COVID-19.	Esto genera una brecha de seguridad importante, ya que la conexión por Internet a un servicio tan sensible es completamente insegura, y puede ser una puerta a ataques de denegación de servicio y de extracción de información.
Falta de configuración de políticas de acceso a los servicios.	En base a las limitaciones del sistema de seguridad actual, la empresa no cuenta con políticas de restricción de acceso.	El no definir políticas de acceso permite que cualquier usuario pueda acceder a los servicios, sea contable o de red. Y no se tiene protección a ataques internos.
Falta de configuración de políticas de navegación.	En base a las limitaciones del sistema de seguridad actual, la empresa no cuenta con políticas de navegación.	Esto provoca que el servicio de Internet pueda ser usado sin restricciones, incluso los usuarios pueden saturar el enlace con servicios que no son orientados al giro de negocio.
Falta de un módulo dedicado a la protección contra las amenazas conocidas (IPS, antivirus, antispyware).	En base a las limitaciones del sistema de seguridad actual, la empresa no cuenta con un módulo para protección de amenazas conocidas	Al no contar con protección contra amenazas conocidas, los servicios de la empresa se encuentran expuestos a cualquier ataque proveniente de Internet o inclusive interno. Y no tendría los mecanismos de defensa para detener el ataque en cualquier fase de su ciclo de vida
Falta de un módulo dedicado a la protección	En base a las limitaciones del sistema de seguridad actual, la	Los servicios de la empresa se encuentran vulnerables a ataques

contra las amenazas de día cero (sandboxing).	empresa no cuenta con un módulo para protección de amenazas de día cero	de día cero, y no cuentan con un módulo de detección y protección que pueda detener el ataque, considerando de los atacantes están en constante desarrollo de nuevas amenazas.

Debido a las vulnerabilidades antes detalladas, la empresa ha recibido notificaciones por parte de la ARCOTEL, indicando una mala configuración en su seguridad perimetral explícitamente para los servicios openDNS y openRDP. Estos servicios pueden ser utilizados en el ciclo del ataque para comando y control, lo que podría terminar en una explotación de vulnerabilidades de los servicios alojados en el rack de comunicaciones o a su vez en un ataque de DDOS. Si estas configuraciones no son corregidas en el tiempo determinado por la ARCOTEL, los ISPs tienen la facultad de bloquear los puertos por defecto de estos servicios e imposibilitar su uso indefinidamente, lo que causaría que los servicios y aplicaciones de la empresa se encuentren inaccesibles y no puedan continuar operando.

Este inconveniente se presentó a raíz de la publicación de los servicios hacia Internet, sobretodo, el servicio contable para accederlo remotamente, debido a la disposición de teletrabajo por la pandemia del COVID-19. El equipo actual de seguridad perimetral está basado en direcciones IP y puertos, por lo que, al realizar esta publicación sin restricciones, se abrió una puerta para que cualquier atacante pueda ingresar a la red de la empresa. Ya que el sistema de seguridad perimetral no cuenta con un módulo avanzado de control de aplicaciones, antivirus, antispyware o IPS, no se pudo detectar esta vulnerabilidad hasta que la ARCOTEL lo reporto.

El área de seguridad del departamento técnico de la empresa procedió con los siguientes procesos correctivos:

- Para los servicios de mesa de ayuda y servicio web, se especificaron los puertos exactos para que la política de seguridad no quede tan abierta. Sin embargo, como se mencionó anteriormente, muchos ataques ingresan camuflados en los puertos 80, 8080 y 443, lo que no asegura al 100% que la red no reciba un ataque, si no se puede hacer inspección en base a aplicaciones.

- Para el servicio contable, al ser un servicio más crítico y de uso exclusivo del área de contabilidad, se procedió a especificar las direcciones IP públicas de origen que pueden acceder al servicio contable, así como los puertos que utiliza este servicio.

  Sin embargo, los usuarios que realizan teletrabajo no cuentan con una dirección IP publica estática, por lo que se han presentado casos en los que se ha tenido que modificar esta política de manera manual debido a que el ISP del usuario le asignó otra dirección IP publica en su servicio de Internet de hogar.

2.2.2 Criterios de evaluación de vulnerabilidades

Para los criterios de evaluación se considera la probabilidad de que suceda un ataque debido a una vulnerabilidad y el impacto que esta podría causar. Se considera una escala del uno al tres para la probabilidad, siendo uno poco probable, dos medianamente probable y tres muy probable.

Para los niveles de impacto igual se considera una escala del uno al tres, siendo uno un impacto leve y tolerable, dos un impacto medianamente considerable y tres un impacto alto que requiere de atención.

De esta manera se define la criticidad de una vulnerabilidad mostrada en la Tabla 2-3.

Tabla 2-3 Tabla de criticidad de vulnerabilidades

IMPACTO / PROBABILIDAD	1	2	3
1	Baja	Baja	Baja
2	Baja	Media	Alta
3	Baja	Media	Alta

2.2.3 Priorización de vulnerabilidades

De acuerdo a los criterios de evaluación se procede a analizar la criticidad de las vulnerabilidades antes expuestas y priorizarlas desde las más altas a las más bajas para poder determinar lo parámetros fundamentales para la solución de seguridad perimetral propuesta.

Tabla 2-4 Priorización de vulnerabilidades

VULNERABILIDAD	PROBABILIDAD	IMPACTO	CRITICIDAD
Segmentación del servicio contable.	**3** Si no se tiene segmentado los servicios de la red de usuarios es muy probable que un usuario acceda sin permiso ya que este tráfico no pasaría por la solución de seguridad y no se podría aplicar controles.	**3** El servicio contable cuenta con información sensible, si no se segmenta este servicio de la red de usuarios y se controla su acceso puede estar expuesto a ataques inclusive desde la red interna.	Alta
Falta de configuración de políticas en base a usuarios.	**3** Es muy probable que, al no tener un control por usuarios, cualquiera pueda realizar acceder a los servicios de la empresa que son restringidos y no dejar rastro.	**3** El impacto es alto, ya que no se puede controlar los accesos a la información y en caso de que esta información sea extraída de los servidores de la empresa, no se podría tener claro que usuario lo realizó y determinar sus propósitos.	Alta
Falta de un módulo dedicado a la protección contra las amenazas conocidas (IPS, antivirus, antispyware).	**3** Es altamente probable que los atacantes detecten que no se dispone de un sistema contra amenazas conocidas y aprovechen para ingresar a la red y vulnerar servicios.	**3** El impacto es sustancial, ya que los dispositivos de la empresa así como la información no tienen seguridad y pueden ser alteradas, incumpliendo con los tres principios de seguridad (integridad, disponibilidad, confidencialidad)	Alta

Falta de un módulo dedicado a la protección contra las amenazas de día cero (sandboxing).	**3** Al igual que en el ítem anterior, las amenazas son creadas a diario y al no tener un módulo de protección en contra de amenazas de día cero, es muy probable que los atacantes vulneren la red y sus servicios.	**3** El impacto es sustancial, ya que los dispositivos de la empresa así como la información no tienen seguridad y pueden ser alteradas, incumpliendo con los tres principios de seguridad (integridad, disponibilidad, confidencialidad)	Alta
Publicación de servicios internos sin seguridad.	**3** Es muy probable que atacantes usen esta vulnerabilidad para acceder a la red y explotar vulnerabilidades	**3** Los atacantes pueden extraer información sensible o a su vez bloquear el acceso a los servicios de la empresa lo que puede causar un impacto sustancial a los servicios e inclusive económico si es que los atacantes piden dinero a cambio de la liberación de la información.	Alta
Falta de configuración para acceso remoto VPN *client to site*.	**3** Al no tener canales seguros para la conexión a los servicios internos desde Internet es muy probable que los atacantes usen esta brecha para acceder a la red y vulnerar los servicios.	**3** Se está expuesto a ataques de denegación de servicio, extracción de información, comando y control que causan impactos altos en la empresa a nivel de información y económicos.	Alta

Falta de configuración de políticas de navegación.	**2** La probabilidad de que los atacantes usen las brechas de seguridad que presenta Internet para engañar a los usuarios y poder explotar sus vulnerabilidades es mediana, depende también de la capacitación a los usuarios sobre el uso de Internet.	**3** El impacto de que un ataque efectivo de phishing o ramsonware los cuales son a través de Internet, es alto ya que comprometería la información tanto del usuario como de la empresa.	Media
Segmentación del servicio de telefonía IP.	**1** Es poco probable recibir un ataque si no se segmenta la telefonía IP.	**1** El impacto es más a la calidad del servicio, pero es tolerable.	Bajo

2.3 MODELO DE ARQUITECTURA DE SEGURIDAD DE RED

En base al levantamiento de información y al análisis de vulnerabilidades descrito anteriormente, en esta sección se determinará los parámetros fundamentales que permitirán elegir un modelo y metodología de seguridad perimetral apropiada para las necesidades de la empresa y para disminuir los riesgos a posibles ataques.

2.3.1 Requerimientos para minimizar vulnerabilidades

El modelo de seguridad perimetral debe permitir a la empresa tener un control de accesos a su información y poder mitigar al máximo la explotación de vulnerabilidades que pueden afectar a los servicios de la empresa.

De acuerdo a lo expuesto anteriormente, en la Tabla 2-5 se presenta los parámetros requeridos para que el modelo de seguridad perimetral se acople a las necesidades de la empresa y que disminuye los riesgos de ataques cibernéticos.

Tabla 2-5 Definición de parámetros del modelo de seguridad perimetral

REQUERIMIENTO	PARÁMETRO	DETALLE
Segmentación de la red interna en vlans.	Zonas de seguridad Zero-Trust	La solución de seguridad perimetral debe operar con zonas de seguridad para la definición de políticas entre las zonas. Dispositivos en diferentes zonas no pueden tener acceso entre sí a menos que una política de seguridad explícitamente lo permita.
Control de accesos por usuarios.	Zero-Trust Control por usuarios	La solución de seguridad perimetral debe inspeccionar todo el tráfico antes de permitir el acceso, lo que permite determinar los permisos a la red de servidores. Además se recomienda aplicar un control basado en usuarios para tener un acceso exclusivo a los servidores solo a los usuarios de la empresa, sin importar el dispositivo con el cual se conecte, eliminando así las políticas por restricción MAC.
Control de amenazas conocidas y de día cero	Antivirus Antispyware IPS Sandboxing	La solución de seguridad perimetral debe garantizar una la navegación a Internet segura, por lo que es necesario que haga análisis a nivel a antivirus, antispyware e IPS. También debe considerar una solución de sandboxing para poder prevenir amenazas tanto conocidas

		como de día cero, en el menor tiempo posible.
Publicación de servicios de manera segura.	Políticas de NAT Control de aplicaciones Antivirus Antispyware IPS Sandboxing	La solución de seguridad perimetral debe permitir la publicación de los servicios de la empresa hacia el Internet mediante políticas de NAT y control de aplicaciones. Al hacerlo en base a aplicaciones y no en base a puertos, se mantiene un control más real del tráfico que ingresa a la red, garantizando que únicamente sea tráfico web, y no algún tráfico camuflado en los puertos 80, 8080 o 443. Además, la solución debe garantizar una publicación segura, por lo que el análisis a nivel de antivirus, antispyware e IPS, con integración a un sandboxing es requerido, para evitar que este acceso se convierta en una brecha de seguridad y una entrada a posibles ataques cibernéticos.
Control de acceso remoto a la red de la empresa.	VPN site to site VPN client to site Control por usuarios	La solución de seguridad perimetral debe permitir la configuración de VPN site to site para la comunicación entre las sucursales principales de la empresa. Además, para cubrir con los requerimientos de teletrabajo, la solución debe permitir la configuración VPN client to site,

		con control de usuarios para que únicamente los usuarios de la empresa puedan tener acceso remoto a los servicios de la misma. Esto eliminaría la publicación del servicio contable a través de Internet.
Control de uso de Internet de los usuario de la empresa y de los usuarios invitados.	Control de aplicaciones Control por usuarios Filtrado URL Perfiles de seguridad Reenvío basado en políticas	Actualmente, no se tiene restricciones en las políticas de navegación por lo que no se tiene un control adecuado del uso de este recurso a nivel empresarial. La solución de seguridad perimetral debe permitir realizar este control de navegación por zonas o por usuarios. Además de permitir el control por aplicaciones, por URL y con perfiles de seguridad (Antivirus, Antispyware, Vulnerabilidades, IPS) en vez de realizado a base de direccionamiento IP y puertos, lo cual no garantiza una protección de red efectiva. También debe considerar políticas de reenvió de paquetes para que los usuarios invitados utilicen el ISP secundario de menor capacidad y no saturen el enlace principal donde operan los servicios de la empresa.

2.4 METODOLOGÍA DE SEGURIDAD PERIMETRAL

Una vez determinados los parámetros necesarios para un correcto funcionamiento de la solución de seguridad perimetral que se acople a las necesidades de la empresa y que mitigue los riesgos potenciales de ataques cibernéticos, se realiza una comparación entre las metodologías de las 3 marcas líderes del cuadrante de Gartner de seguridad perimetral (Gartner, 2020) y también de la solución actual, con el fin de determinar la metodología adecuada que garantice la seguridad de la información y de los servicios de la empresa.

2.4.1 Comparativa de metodologías de seguridad perimetral

En la Tabla 2-6 se presenta el comparativo de cada metodología para determinar cuál se acopla de mejor manera a las necesidades de la empresa:

Tabla 2-6 Comparación entre las metodologías de seguridad perimetral

	MIKROTIK	PALO ALTO	FORTINET	CHECKPOINT
Característica principal	Se basa en la tecnología Stateful Filtering que se puede utilizar para detectar y bloquear muchos escaneos sigilosos (Mikrotik, 2020).	Se basa en su motor de procesamiento paralelo de un solo paso (SP3). La ventaja de SP3 es que el tráfico se escanea y con una cantidad mínima de almacenamiento en búfer. Esto permite habilitar funciones avanzadas sin reducir el rendimiento del NGFW (Palo Alto Networks, 2019).	Se basa en el concepto de que los dispositivos de seguridad nunca deben convertirse en un cuello de botella y utilizan SPU para inspecciones a una velocidad, escala y rendimiento incomparables (Fortinet, 2020d)	Se basa no solo en detectar y mitigar, sino también en prevenir. Su arquitectura está conformada por un sistema d prevención de tipo inteligente, inmediata y automática de amenazas (Check Point, 2020c).
Zonas	**No cumple**	**Si cumple**	**Si cumple**	**Si cumple**
Zero-Trust	**No cumple**	**Si cumple**	**Si cumple**	**Si cumple**
Control usuario	**No cumple**	**Si cumple** User-ID permite la definición de las políticas en base a usuarios, sean de directorio activo o locales del firewall. No requiere suscripción.	**Si cumple** Fortinet permite la definición de políticas en base a usuarios locales o de directorio activo (Fortinet, 2020h). No requiere suscripción.	**Si cumple** Identity Awarness es el modulo que permite la definición de políticas en base a usuarios locales o de directorio activo (Check Point, 2020f) No requiere suscripción.

Control por aplicaciones	**Si cumple parcial** Presenta un módulo muy básico de aplicación, y su configuración es compleja (Mikrotik, 2020).	**Si cumple** El NGFW de Palo Alto es una solución que nació como firewall de aplicación con APP-ID. No requiere de suscripción	**Si cumple** Application Control es el módulo de categorización de aplicaciones. Requiere suscripción.	**Si cumple** Application Control es el módulo de categorización de aplicaciones. Requiere suscripción.
Filtrado URL	**No cumple**	**Si cumple** URL-Filtering para la detección de URL maliciosas. Requiere suscripción	**Si cumple** Web-Filtering es capaz de bloquear el acceso a sitios web malicioso. Requiere suscripción.	**Si cumple** URL-Filtering es capaz de bloquear el acceso a sitios web malicioso. Requiere suscripción.
Antivirus	**No cumple**	**Si cumple** Threat Prevention para prevención en base a firmas de virus conocidos. Requiere suscripción	**Si cumple** El modulo Antivirus es encargado de la protección contra los más recientes virus. Requiere suscripción.	**Si cumple** El módulo Antivirus es encargado de la protección contra los más recientes virus. Requiere suscripción.
Antispyware	**No cumple**	**Si cumple** Threat Prevention es la protección de técnicas de spyware y malware conocido. Requiere suscripción	**Si cumple** El módulo de Antivirus es encargado de la protección contra spyware y otras amenazas a nivel de contenido. Requiere suscripción.	**Si cumple** El módulo Antivirus es encargado de la protección contra los más recientes virus y técnicas de spyware y malware. Requiere suscripción.

IPS	**No cumple**	**Si cumple** Threat Prevention incluye un IPS capaz de detener exploits conocidos. Requiere suscripción.	**Si cumple** IPS realiza el análisis de exploits conocidos en conjunto con FortiGuad. Requiere suscripción.	**Si cumple** IPS es el modulo encargado de realizar el análisis de exploits conocidos. Requiere suscripción.
Sandboxing	**No cumple**	**Si cumple** Wildfire es el motor de análisis y prevención basado en la nube para enfrentar amenazas de día cero. Requiere suscripción para la entrega de un veredicto en tiempo real, caso contrario, se entrega en las actualizaciones diarias o semanales de cada servicio, URL-filtering o Threat Prevention Requiere suscripción.	**Si cumple** FortiSandbox Cloud realiza análisis dinámico para identificar malware de día cero, el veredicto es enviado a todos los clientes Fortinet con la suscripción de sandbox. Requiere suscripción.	**Si cumple** ThreatCloud con SandBlast Threat Emulation y SandBlast Threat Extraction son los encargados del análisis de amenazas de día cero. Requiere suscripción.
Políticas de NAT	**Si cumple** Permite reglas de NAT, que enmascaran la red interna en una dirección IP pública.	**Si cumple** Permite políticas de NAT, PAT, DNAT. No requiere de suscripción.	**Si cumple** Permite de políticas de NAT, PAT, DNAT. No requiere de suscripción.	**Si cumple** Permite de políticas de NAT, PAT, DNAT. No requiere de suscripción.

Reenvío de paquetes basado en políticas	**Si cumple parcial** Realiza el reenvío de paquetes, pero en base a marcado de tráfico mas no de políticas.	**Si cumple** Policy Base Forwarding puede especificar el reenvío de tráfico en base a direcciones, usuarios o aplicaciones (Palo Alto Networks, 2020f). No requiere de suscripción.	**Si cumple parcial** Policy Routing permite el reenvío de tráfico basado en direccionamiento y puerto (Fortinet, 2020f) No requiere de suscripción.	**Si cumple** Policy Base Routing permite el reenvío de tráfico basado en direccionamiento, interfaz y puerto (Check Point, 2019). No requiere de suscripción.
VPN site to site	**Si cumple** Tiene la capacidad de realizar VPN bajo protocolos como PPTP, SSTP, L2TP e IPSec.	**Si cumple** Tiene la capacidad de realizar túneles IPSec y es compatible con los dispositivos que soporten IPSec (Palo Alto Networks, 2020h). No requiere de suscripción.	**Si cumple** Tiene la capacidad de realizar túneles IPSec entre soluciones AWS, Azure, Cisco y FortiGate (Fortinet, 2020c). No requiere de suscripción.	**Si cumple** IPSec VPN es el modulo que permite la conexión entre sucursales. No requiere de suscripción si la conexión es entre equipos Check Points, requiere de suscripción para equipos de terceros (Check Point, 2020e).
VPN client to site	**Si cumple** Utiliza los clientes de los dispositivos Windows y MacOS para realizar la	**Si cumple** El agente de Palo Alto, Global Protect, permite una conexión remota en base a usuarios registrados en el	**Si cumple** FortiClient es el agente para la conexión remota basada en usuarios a la red interna de la empresa (Fortinet, 2020b).	**Si cumple** Mobile Access es el modulo que permite la conexión remota de usuarios a la red de

	conexión VPN, depende del sistema operativo del usuario.	directorio activo o en el NGFW. No requiere de suscripción.	Requiere de suscripción.	la empresa (Check Point, 2020h). Requiere suscripción.
Prevención pérdida/fuga datos	**No cumple**	**Si cumple** DLP utiliza técnicas de análisis de contenido para detectar, clasificar, supervisar y proteger los datos sensibles de forma coherente, independientemente de dónde residan y se transfieran. Requiere suscripción. File blocking es el complemento de la solución, filtrando el tráfico por tipo de archivo. No requiere de suscripción.	**Si cumple** File filter permite el paso de archivos basado en el tipo, hace inspección a nivel HTTP y FTP. (Fortinet, 2020a). Requiere suscripción.	**Si cumple** DLP es el modulo encargado de evitar las fugas de datos involuntarias al capturar los datos protegidos antes de que salgan de la red interna. (Check Point, 2020d). Requiere suscripción.

Fuente: (Mikrotik, 2020), (Palo Alto Networks, 2019), (Palo Alto Networks, 2020f), (Palo Alto Networks, 2020h), (Fortinet, 2020b), (Fortinet, 2020c), (Fortinet, 2020a), (Fortinet, 2020d), (Fortinet, 2020f), (Check Point, 2020c) (Check Point, 2020d), (Check Point, 2020f), (Check Point, 2020e), (Check Point, 2020h).

2.4.2 Selección de metodología de seguridad perimetral

Para la selección de metodología seguridad perimetral, se realiza un análisis comparativo de funcionalidades de acuerdo a la información recopilada en la Tabla 2-6. A continuación, se detallan los aspectos más relevantes para realizar el análisis:

Mikrotik

- Mikrotik es la solución actual que tiene la empresa, su arquitectura no está basada en zonas y tampoco utiliza el modelo zero-trust, además no cuenta con los módulos de prevención de amenazas como antivirus, antispyware, IPS, DLP.
- Al no ser una solución de seguridad perimetral se lo descarta de la selección y el análisis se enfoca en las tres marcas líderes para el reemplazo del equipo de seguridad perimetral actual.

Palo Alto Networks

- Su arquitectura es zonal y cumple con el modelo zero-trust.
- Permite la creación de VPN site to site y VPN client to site, sin la necesidad de una suscripción.
- Puede realizar reenvío de paquetes basado en aplicaciones, direcciones IP, puertos y usuarios.
- Nació como firewall de aplicaciones, lo que significa que su motor de categorización de aplicaciones siempre está activado y viene embebido sin necesidad de una suscripción adicional.
- La solución de prevención contra amenazas que incluye antivirus, antispyware, IPS, se soportan bajo una misma suscripción.
- La solución de prevención de pérdida/fuga de datos se soporta bajo una suscripción y permite el análisis de contenido de los archivos mas no solo el análisis de tipo de archivo.
- La solución de sandboxing se soporta bajo una suscripción si se requiere veredictos en tiempo real, caso contrario, Wildfire hace el análisis correspondiente de todos los archivos y el veredicto es actualizado en las bases de cada motor de prevención de amenazas con las actualizaciones diarias o semanales que Palo Alto Networks realiza.

- Para la puesta en producción del equipo, se requeriría apenas cuatro suscripciones: URL-Filtering, Threat Prevention, Data Loose Prevention y Wildfire.

Fortinet

- Su arquitectura es zonal y cumple con el modelo zero-trust.
- Puede realizar reenvío de paquetes basado en direcciones IP y puertos.
- Permite la creación de VPN site to site sin suscripción y solo es compatible con soluciones AWS, Azure, Cisco y Fortinet. Las VPN client to site, requieren de suscripción.
- Los módulos de application control y web-filtering son suscripciones independientes.
- Cada una de las soluciones de prevención de amenazas requieren de una suscripción independiente para su activación.
- El módulo de file-filter orientado a DLP, hace análisis únicamente del tipo de archivo y bajo los protocolos HTTP y FTP, este módulo se activa con la suscripción de web-filtering, pero no cubre con las necesidades de análisis de contenido de archivos sensibles.
- La solución de sandboxing requiere de una suscripción y solo los equipos que tengan esta suscripción pueden gozar de los beneficios del análisis de amenazas de día cero que ofrece el FortiSandbox.
- Para la puesta en producción del equipo, se requeriría de seis suscripciones: FortiClient, Application Control, Web-Filtering, Antivirus, IPS y FortiSandbox.

Check Point

- Su arquitectura es zonal y cumple con el modelo zero-trust.
- Puede realizar reenvío de paquetes basado en interfaces, direcciones IP y puertos.
- Permite la creación de VPN site to site sin suscripción entre equipos Check Point, para la integración con terceros se requiere de suscripción. Las VPN client to site, requieren de suscripción.
- Los módulos de application control y url-filtering son suscripciones independientes.

- Cada una de las soluciones de prevención de amenazas requieren de una suscripción independiente para su activación.
- El módulo de DLP orientado a Deep Loos Prevention, el análisis de contenido de los archivos y de tipo de archivo evitando que la información salga de la red interna sin autorización, este módulo requiere de suscripción.
- La solución de sandboxing requiere de una suscripción y permite no solo el análisis de amenazas de día cero sino también el análisis de contenido para la reconstrucción de archivos y entrega de documentos desinfectados.
- Para la puesta en producción del equipo, se requeriría de siete suscripciones: Mobile Remote Access, Application Control, URL-Filtering, Antivirus, IPS, DLP y ThreatCloud.

Después del análisis realizado, se determina que la metodología de seguridad perimetral actual debe ser reemplazada ya que no cumple con las necesidades de la empresa y con los requerimientos para mitigar los riesgos potenciales de ataques cibernéticos.

En base al análisis comparativo entre las tres marcas líderes del cuadrante de Gartner (Gartner, 2020) se concluye que la metodología de seguridad que emplea Palo Alto Networks permite cubrir todas las necesidades de la empresa y ofrece las mejores características para enfrentar los riesgos y amenazas cibernéticas, además de requerir menor cantidad de suscripciones para su funcionamiento lo que representa una mayor beneficio con menor inversión.

CAPÍTULO 3: MODELO DE POLÍTICAS DE SEGURIDAD

La definición del modelo y la metodología de seguridad perimetral se complementa con la aplicación de políticas de seguridad de una empresa. En este capítulo se realiza el análisis de la documentación que la empresa AKEA S.A dispone actualmente referente a políticas de seguridad, con el fin de realizar una propuesta de mejora la cual debe permitir la disminución de los riesgos encontrados en conjunto con la metodología de seguridad perimetral seleccionada en el capítulo anterior. El análisis se basa en las recomendaciones de la norma ISO/IEC 27001 y en las mejores prácticas de controles indicados en la norma ISO/IEC 27002.

3.1 ANÁLISIS DE LAS POLÍTICAS DE SEGURIDAD ACTUALES

En el Anexo A se encuentra el documento completo de políticas de seguridad que AKEA S.A dispone al momento del levantamiento de información. Los ingenieros del departamento técnico elaboraron el documento en base a los requerimientos de la empresa. El gerente técnico aprobó dicho documento y fue quien autorizó por escrito el uso de esta información para el presente análisis como se describe en el Anexo B.

3.1.1 Aplicabilidad de las políticas de seguridad actuales

Se realiza el análisis de aplicabilidad de las políticas de seguridad actuales en base a la medición de su nivel de cumplimiento. Este análisis utiliza tres niveles de cumplimiento, los cuales se detallan en la Tabla 3-1.

Además, se añade un nivel neutro para aquellas políticas que no se aplican a la seguridad perimetral, pero que se mencionan en el documento de la empresa.

Tabla 3-1 Niveles de cumplimiento

NIVEL	COLOR	DETALLE
Si cumple		La metodología de seguridad perimetral y la arquitectura permiten la aplicación de la política de seguridad propuesta y se lleva a cabo los controles de seguridad en los sistemas de información.
Cumple parcialmente		La metodología de seguridad perimetral y la arquitectura permiten en parte la aplicación de la política de seguridad propuesta, sin embargo no cumple con todos los controles de seguridad en los sistemas de información.

No cumple		La metodología de seguridad perimetral y la arquitectura no permiten la aplicación de la política de seguridad propuesta y no se lleva a cabo los controles de seguridad en los sistemas de información.
Neutro		No aplica para seguridad perimetral

En la Tabla 3-2 se presenta el análisis realizado el cual tiene como finalidad determinar si la metodología de seguridad perimetral y la arquitectura de red que la empresa dispone actualmente, puede cumplir con los parámetros requeridos por las políticas de seguridad presentadas en el Anexo A.

Tabla 3-2 Análisis de aplicabilidad de políticas de seguridad actuales

POLÍTICA	NIVEL	ANÁLISIS
3. CONSIDERACIONES		
3.1 Políticas de seguridad física En esta política se cuenta con seis subitems que determinan los lineamientos para los accesos físicos tanto a la empresa como a la infraestructura de red.		Esta fuera del alcance del análisis ya que no corresponde a las metodologías de seguridad perimetral de la información.
3.2 Protección física En esta política se cuenta con dos subitems que determinan los lineamientos para la protección de las conexiones física tanto a nivel de cableado estructurado como a nivel de cableado eléctrico.		Esta fuera del alcance del análisis ya que no corresponde a las metodologías de seguridad perimetral de la información.
3.3 Instalaciones de equipo En esta política se determinan los lineamientos para la instalación de los equipos de cómputo en el rack de comunicaciones de acuerdo a las normativas de seguridad.		Esta fuera del alcance del análisis ya que no corresponde a las metodologías de seguridad perimetral de la información.

3.4 Control		
3.4.1 Se debe llevar un control total y sistematizado de los recursos de cómputo y licenciamiento. Inventariado en una mesa de ayuda o en herramientas de uso más común como Microsoft Excel.		Esta fuera del alcance del análisis ya que no corresponde a las metodologías de seguridad perimetral de la información.
3.4.2 Los encargados del área de tecnología son los responsables de organizar al personal de mantenimiento preventivo y correctivo de los equipos de cómputo.		Esta fuera del alcance del análisis ya que no corresponde a las metodologías de seguridad perimetral de la información.
3.4.3 El área administrativa deberá reportar al departamento de tecnología cuando un usuario deje de laborar o de tener una relación con la empresa con el fin de retirarle las credenciales de ingreso a los recursos y supervisar la correcta devolución de los equipos y recursos asignados al usuario.		El departamento técnico realiza la creación y eliminación de usuarios según lo indique el departamento de recursos humanos, sin embargo, estos accesos son a nivel de correo electrónico y sistema contable, más no a nivel de uso de recursos empresariales. La metodología de seguridad perimetral actual no soporta control de accesos por usuario.
3.5 Respaldos		
3.5.1 Los servidores de hosting estarán alojados en Godaddy y su DNS en NIC.EC.		Esta fuera del alcance del análisis ya que no corresponde a las metodologías de seguridad perimetral de la información.
3.5.2 Para reforzar la seguridad de la información, los usuarios deberán hacer respaldos de la información de sus discos duros en las unidades de almacenamiento asignadas por la empresa en la nube Microsoft OneDrive.		AKEA S.A cuenta con el servicio de Microsoft OneDrive que permite la sincronización de archivos en la nube para respaldo de información en caso de daño físico del equipo. La metodología de seguridad perimetral actual permite el paso sin restricción ni control de ancho de banda de este tipo de tráfico.

3.5.3 El departamento técnico obtendrá respaldos periódicamente de los equipos de comunicaciones tales como routers, switches.		Esta fuera del alcance del análisis ya que no corresponde a las metodologías de seguridad perimetral de la información.
3.6 Recursos de los usuarios		
3.6.1 Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de la empresa. El correo electrónico no deberá ser usado para envío masivo de materiales de uso no institucional. La información confidencial de la empresa, de clientes y proveedores, debe mantenerse como tal y no debe ser divulgada a terceros .		La metodología de seguridad perimetral actual no realiza ningún tipo de control de uso de recursos informáticos, por lo que no se asegura el uso inadecuado de los mismos. A pesar de contar con un documento de confidencialidad, la arquitectura actual no presenta un control de extracción de información debido a que no soporta DLP.
3.6.2 Queda prohibido inspeccionar, copiar o almacenar programas de cómputo o aplicaciones adquiridas por la empresa, para tal efecto todos los usuarios deberán firmar un documento donde se comprometan, bajo su responsabilidad, a no usar programas que violen la ley de derechos de autor.		Esta fuera del alcance del análisis ya que no corresponde a las metodologías de seguridad perimetral de la información.
4. EXPOSICIÓN DE LAS POLÍTICAS		
4.1 Red		
4.1.1 No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de la empresa.		El metodología de seguridad perimetral actual no realiza ningún tipo de control de uso de recursos informáticos, por lo que no se asegura el uso inadecuado de los mismos.

4.1.2 Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la empresa y se usarán exclusivamente para actividades relacionadas con la labor asignada.		Las cuentas de ingreso son responsabilidad del personal, y depende de ellos su uso en las labores empresariales. La metodología de seguridad perimetral actual no soporta control de accesos por usuario.
4.1.3 Cuando se detecte un uso no aceptable, se cancelará la cuenta temporal o permanentemente al usuario dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.		La metodología de seguridad perimetral actual no soporta control de accesos por usuario por lo que no se puede registrar un uso no aceptable, sin embargo, los encargados de cada sistema pueden solicitar la cancelación de una cuenta en base a sospechas de mal uso.
4.2 Servidores		
4.2.1 La instalación y/o configuración de todo servidor será responsabilidad del departamento técnico. Durante la configuración de los servidores el personal de técnico debe efectuar las actividades apropiadas para el uso de recursos y de la red, principalmente restricción de directorios y permisos. Los servicios a través de la red e Internet deberán funcionar 24 horas del día los 365 días del año y ser monitoreados por el personal de técnico. Los servicios hacia Internet sólo podrán proveerse a través de los servidores autorizados por el departamento técnico.		Únicamente el departamento técnico cuenta con las claves de acceso a los dispositivos de red y a los servicios virtualizados, sin embargo, la red de administración de dispositivos no está separada de la red de usuarios, y se considera una vulnerabilidad, ya que las claves se pueden romper. Además, los servicios hacia Internet están publicados en base a puertos y no aplicaciones ya que la metodología de seguridad perimetral actual no lo soporta.

4.2.2 La cuenta de correo electrónico será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada. La longitud mínima de las contraseñas será igual o superior a ocho caracteres.		La arquitectura actual cuenta con el servicio de Office365 para la creación de cuentas de correo electrónico que cumplen con el requerimiento de la política de seguridad de la empresa
4.3 Recursos de computo		
4.3.1 El departamento técnico debe mantener configuradas políticas de seguridad de firewall a fin de proteger a los usuarios. El departamento de técnico es el único autorizado para monitorear constantemente el tráfico, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios.		Las políticas de seguridad actuales no son restrictivas y no cuentan con módulos de prevención contra ataques. Además, a pesar de que solo el departamento técnico cuenta con la clave de acceso al sistema de monitoreo, la administración de este dispositivo no está separado de la red de usuarios y se podría romper la clave de seguridad.
4.3.2 Los ingenieros de soporte técnico podrán ingresar de forma remota a computadoras para la solución de problemas. Deben auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, o permisos extra que pongan en riesgo la seguridad de la información.		No existe un sistema de control en la arquitectura actual que evite que los usuarios instalen cualquier tipo de software o que almacenen archivos no autorizados en las laptops y PCS de la empresa. Por lo tanto, el uso de software para acceso remoto no está limitado al departamento técnico.

4.3.3 Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.		Esta fuera del alcance del análisis ya que no corresponde a las metodologías de seguridad perimetral de la información.
4.4 Uso de Servicios de Red		
En esta política se cuenta con dos subitems que determinan los lineamientos referente al uso de servicios de red los cuales están determinados por gerencia tanto para usuarios internos, externos o invitados, así como el manejo de contraseñas de acceso.		Por disposición de gerencia, no se tiene restricciones de navegación. Solo los ingenieros de soporte realizan el registro de los dispositivos que tienen acceso a la red empresarial, mediante políticas de acceso basados en MAC ADDRESS. Solo los ingenieros de soporte realizan la configuración de la red inalámbrica para los dispositivos de los usuarios de la empresa. A nivel de usuarios externos, se tiene segmentada la red, esta red no tiene acceso a los servicios internos empresariales, y hace uso del servicio de internet del ISP secundario.
4.5 Antivirus		
4.5.1 Todos los equipos de cómputo de la empresa deberán tener instalada una solución Antivirus. Periódicamente se hará el rastreo en los equipos y se realizará la actualización de las firmas de antivirus o similar, proporcionadas por el fabricante.		Del levantamiento de información se validó que la mayoría de dispositivos utilizan Windows como sistema operativo y como solución de Antivirus, utilizan la solución propia de Windows que es Defender. Sin embargo, se presenta una limitante ya que la metodología de seguridad perimetral no cuenta con un módulo de Antivirus para la prevención de ataques.
4.6 Seguridad perimetral		
4.6.1 La solución de seguridad perimetral debe ser controlada con un firewall por Hardware y/o		Esta es la política más relevante relacionada a la metodología de seguridad perimetral, sin embargo, la solución actual de la empresa no

Software que se encargue de controlar el flujo de datos. El departamento técnico establecerá las reglas en el firewall necesarias para bloquear o permitir el flujo de datos entrante y saliente. El firewall debe controlar los ataques de DoS y controlar también el número de conexiones que se están produciendo. Controlar las aplicaciones que acceden a Internet para impedir la ejecución de programas maliciosos que puedan enviar información interna al exterior.		cumple con los requerimientos de la política, ya que no cuenta con módulos de prevención de ataques de denegación de servicio o de código malicioso, además de no ser un firewall de aplicación sino más bien basado en puertos.
4.7 Redes privadas virtuales (VPN)		
4.7.1 La matriz de la empresa ubicada en la ciudad de Quito tendrá comunicación con la sucursal ubicada en la ciudad de Guayaquil, mediante telefonía IP. Dicha comunicación estará protegida mediante una Red Privada Virtual implementada por el departamento técnico, con lo cual se garantizará la privacidad de la información.		La metodología de seguridad perimetral actual permite la conexión a través de VPN site to site entre las sucursales y la matriz, aplicando protocolos de encripción y tunelización IPSec.
4.8 Conectividad a Internet		
4.8.1 La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. El acceso a Internet desde las oficinas se restringe por medio del sistema de seguridad con firewall incorporado.		La metodología de seguridad perimetral actual no cuenta con políticas de restricción de navegación en Internet, ni para usuarios empresariales ni para usuarios externos. Debido a la falta de control en las aplicaciones o software permitido para la instalación,

Está permitido el acceso remoto en caso en el que los funcionarios del departamento técnico se encuentran brindando soporte en sitio, o cuando un funcionario se encuentra efectuando Teletrabajo.		cualquier usuario puede tener acceso mediante conexión remota a la red de la empresa.
4.9 Red inalámbrica (WIFI) en oficinas		
4.9.1 El departamento técnico es el encargado de la administración de usuarios en la red inalámbrica. El acceso a la red inalámbrica de la empresa serán otorgados según criterio de las gerencias y del rol que este desempeña.		Para el acceso a través de la red de usuarios únicamente los dispositivos autorizados por gerencia, pueden registrarse en el firewall mediante el control por MAC ADDRESS. Para los usuarios externos, se genera un usuario y clave temporal que se debe registrar en el portal cautivo configurado para la red inalámbrica de invitados.
4.10 Acceso a invitados en oficinas		
4.10.1 La red inalámbrica de invitados no tendrán acceso a la red de la empresa ni a ningún recurso de uso privado. La red inalámbrica es de tipo Portal Cautivo y se tendrá una lista de usuarios invitados con tiempo controlado de acceso.		La arquitectura actual permite el acceso a usuarios invitados a través de un portal cautivo, el departamento técnico genera un usuario y clave temporal para el registro en el portal cautivo, esta red no tiene acceso a los servicios internos de la empresa y utiliza el servicio de internet del ISP secundario.
4.11 Seguridad en el manejo de información de los clientes		
4.11.1 La información confidencial entregada por los clientes que pudiera llegar a conocimiento del personal, en razón de su relación con la compañía AKEA S.A. debe mantenerse como tal y no debe ser divulgada a terceros por ninguna razón ni circunstancia.		La empresa cuenta con un documento de confidencialidad que obliga a no divulgar la información de los clientes de la empresa, este documento aplica multas sumamente estrictas. La arquitectura actual no cuenta con un sistema de control de fuga de información ni de extracción de información por medios digitales externos como USB o CD.

5 PLAN DE CONTINGENCIA		
En esta política se determinan los lineamientos en caso de pérdida de información por daños físicos de los equipos o servidores.		Esta fuera del alcance del análisis ya que no corresponde a las metodologías de seguridad perimetral de la información.
6 CERTIFICACIONES		
En esta política se determinan los requerimientos del personal técnico para poder realizar sus funciones en la empresa y en los proyectos con los clientes.		Esta fuera del alcance del análisis ya que no corresponde a las metodologías de seguridad perimetral de la información.

El documento de políticas de seguridad actual cuenta con 36 políticas. De acuerdo al análisis realizado, 17 políticas no son aplicables al análisis de la metodología de seguridad perimetral. De las 19 políticas restantes se ha determinado que la metodología de seguridad perimetral actual cumple completamente con el 31%, el 32% se cumple parcialmente y el 37% no cumple con las políticas de la empresa por las limitantes de la arquitectura y de la metodología de seguridad perimetral, como se muestra en la Figura 3-1.

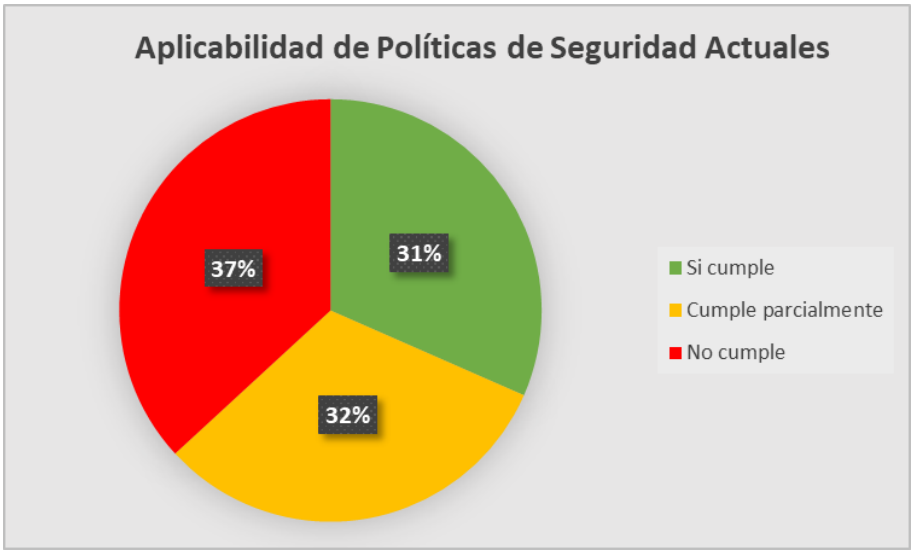


Figura 3-1 Aplicabilidad de las políticas de seguridad actuales

3.2 SELECCIÓN DE CONTROLES PARA SEGURIDAD PERIMETRAL

Del análisis realizado anteriormente se pudo identificar que la metodología de seguridad actual es ineficiente y la empresa se encuentra en riesgo de ataques tanto externos como internos. Por lo tanto, es necesario seleccionar los controles que permitan mitigar los riesgos y que sean aplicables con la metodología de seguridad perimetral seleccionada.

3.2.1 Selección de controles

Este análisis se lo realiza en base a las recomendaciones y controles presentados en la norma ISO/IEC 27002 la cual cuenta con 14 dominios, 35 objetivos de control y 114 controles de seguridad los cuales se listan a continuación en la Tabla 3-3.

Tabla 3-3 Controles de seguridad de la información de la norma ISO/IEC 27002

Sección	Controles de Seguridad de la Información
A5	**Políticas de seguridad de la información**
A5.1	**Directrices de gestión de la seguridad de la información**
A5.1.1	Políticas para la seguridad de la información
A5.1.2	Revisión de las políticas para la seguridad de la información
A6	**Organización de la seguridad de la información**
A6.1	**Organización interna**
A6.1.1	Roles y responsabilidades en seguridad de la información
A6.1.2	Segregación de tareas
A6.1.3	Contacto con las autoridades
A6.1.4	Contacto con grupos de interés especial
A6.1.5	Seguridad de la información en la gestión de proyectos
A6.2	**Los dispositivos móviles y el teletrabajo**
A6.2.1	Política de dispositivos móviles
A6.2.2	Teletrabajo
A7	**Seguridad relativa a los recursos humanos**
A7.1	**Antes del empleo**
A7.1.1	Investigación de antecedentes
A7.1.2	Términos y condiciones del empleo
A7.2	**Durante el empleo**
A7.2.1	Responsabilidades de gestión

A7.2.2	Concienciación, educación y capacitación en seguridad de la información
A7.2.3	Proceso disciplinario
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**
A7.3.1	Responsabilidades ante la finalización o cambio
A8	**Gestión de activos**
A8.1	**Responsabilidad sobre los activos**
A8.1.1	Inventario de activos
A8.1.2	Propiedad de los activos
A8.1.3	Uso aceptable de los activos
A8.1.4	Devolución de activos
A8.2	**Clasificación de la información**
A8.2.1	Clasificación de la información
A8.2.2	Etiquetado de la información
A8.2.3	Manipulado de la información
A8.3	**Manipulación de los soportes**
A8.3.1	Gestión de soportes extraíbles
A8.3.2	Eliminación de soportes
A8.3.3	Soportes físicos en tránsito
A9	**Control de acceso**
A9.1	**Requisitos de negocio para el control de acceso**
A9.1.1	Política de control de acceso
A9.1.2	Acceso a las redes y a los servicios de red
A9.2	**Gestión de acceso de usuario**
A9.2.1	Registro y baja de usuario
A9.2.2	Provisión de acceso de usuario
A9.2.3	Gestión de privilegios de acceso
A9.2.4	Gestión de la información secreta de autenticación de los usuarios
A9.2.5	Revisión de los derechos de acceso de usuario
A9.2.6	Retirada o reasignación de los derechos de acceso
A9.3	**Responsabilidades del usuario**
A9.3.1	Uso de la información secreta de autenticación
A9.4	**Control de acceso a sistemas y aplicaciones**

A9.4.1	Restricción del acceso a la información
A9.4.2	Procedimientos seguros de inicio de sesión
A9.4.3	Sistema de gestión de contraseñas
A9.4.4	Uso de utilidades con privilegios del sistema
A9.4.5	Control de acceso al código fuente de los programas
A10	**Criptografía**
A10.1	**Controles criptográficos**
A10.1.1	Política de uso de los controles criptográficos
A10.1.2	Gestión de claves
A11	**Seguridad física y del entorno**
A11.1	**Áreas seguras**
A11.1.1	Perímetro de seguridad física
A11.1.2	Controles físicos de entrada
A11.1.3	Seguridad de oficinas, despachos y recursos
A11.1.4	Protección contra las amenazas externas y ambientales
A11.1.5	El trabajo en áreas seguras
A11.1.6	Áreas de carga y descarga
A11.2	**Seguridad de los equipos**
A11.2.1	Emplazamiento y protección de equipos
A11.2.2	Instalaciones de suministro
A11.2.3	Seguridad del cableado
A11.2.4	Mantenimiento de los equipos
A11.2.5	Retirada de materiales propiedad de la empresa
A11.2.6	Seguridad de los equipos fuera de las instalaciones
A11.2.7	Reutilización o eliminación segura de equipos
A11.2.8	Equipo de usuario desatendido
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia
A12	**Seguridad de las operaciones**
A12.1	**Procedimientos y responsabilidades operacionales**
A12.1.1	Documentación de procedimientos operacionales
A12.1.2	Gestión de cambios
A12.1.3	Gestión de capacidades

A12.1.4	Separación de los recursos de desarrollo, prueba y operación
A12.2	**Protección contra el software malicioso (malware)**
A12.2.1	Controles contra el código malicioso
A12.3	**Copias de seguridad**
A12.3.1	Copias de seguridad de la información
A12.4	**Registros y supervisión**
A12.4.1	Registro de eventos
A12.4.2	Protección de la información del registro
A12.4.3	Registros de administración y operación
A12.4.4	Sincronización del reloj
A12.5	**Control del software en explotación**
A12.5.1	Instalación del software en explotación
A12.6	**Gestión de la vulnerabilidad técnica**
A12.6.1	Gestión de las vulnerabilidades técnicas
A12.6.2	Restricción en la instalación de software
A12.7	**Consideraciones sobre la auditoria de sistemas de información**
A12.7.1	Controles de auditoría de sistemas de información
A13	**Seguridad de las comunicaciones**
A13.1	**Gestión de la seguridad de las redes**
A13.1.1	Controles de red
A13.1.2	Seguridad de los servicios de red
A13.1.3	Segregación en redes
A13.2	**Intercambio de información**
A13.2.1	Políticas y procedimientos de intercambio de información
A13.2.2	Acuerdos de intercambio de información
A13.2.3	Mensajería electrónica
A13.2.4	Acuerdos de confidencialidad o no revelación
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**
A14.1	**Requisitos de seguridad en los sistemas de información**
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas
A14.1.3	Protección de las transacciones de servicios de aplicaciones

A14.2	**Seguridad en el desarrollo y en los procesos de soporte**
A14.2.1	Política de desarrollo seguro
A14.2.2	Procedimiento de control de cambios en sistemas
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
A14.2.4	Restricciones a los cambios en los paquetes de software
A14.2.5	Principios de ingeniería de sistemas seguros
A14.2.6	Entorno de desarrollo seguro
A14.2.7	Externalización del desarrollo de software
A14.2.8	Pruebas funcionales de seguridad de sistemas
A14.2.9	Pruebas de aceptación de sistemas
A14.3	**Datos de prueba**
A14.3.1	Protección de los datos de prueba
A15	**Relación con proveedores**
A15.1	**Seguridad en las relaciones con proveedores**
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores
A15.1.2	Requisitos de seguridad en contratos con terceros
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones
A15.2	**Gestión de la provisión de servicios del proveedor**
A15.2.1	Control y revisión de la provisión de servicios del proveedor
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor
A16	**Gestión de incidentes de seguridad de la información**
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**
A16.1.1	Responsabilidades y procedimientos
A16.1.2	Notificación de los eventos de seguridad de la información
A16.1.3	Notificación de puntos débiles de la seguridad
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información
A16.1.5	Respuesta a incidentes de seguridad de la información
A16.1.6	Aprendizaje de los incidentes de seguridad de la información
A16.1.7	Recopilación de evidencias
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**
A17.1	**Continuidad de la seguridad de la información**
A17.1.1	Planificación de la continuidad de la seguridad de la información

A17.1.2	Implementar la continuidad de la seguridad de la información
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
A17.2	**Redundancias**
A17.2.1	Disponibilidad de los recursos de tratamiento de la información
A18	**Cumplimiento**
A18.1	**Cumplimiento de los requisitos legales y contractuales**
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales
A18.1.2	Derechos de Propiedad Intelectual (DPI)
A18.1.3	Protección de los registros de la organización
A18.1.4	Protección y privacidad de la información de carácter personal
A18.1.5	Regulación de los controles criptográficos
A18.2	**Revisiones de la seguridad de la información**
A18.2.1	Revisión independiente de la seguridad de la información
A18.2.2	Cumplimiento de las políticas y normas de seguridad
A18.2.3	Comprobación del cumplimiento técnico

Fuente: (ISO/IEC, 2013)

No todos los controles presentes en la norma ISO/IEC 27002 hacen referencia a seguridad perimetral, por lo cual se seleccionan los controles adecuados que permiten generar una propuesta de políticas de seguridad complementadas y aplicadas por la metodología de seguridad perimetral seleccionada en el capítulo anterior, con el fin de superar el porcentaje de no cumplimiento y de cumplimiento parcial que presenta la solución de seguridad actual.

Tabla 3-4 Selección de controles de seguridad de la norma ISO/IEC 27002

SECCIÓN	CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	OBJETIVO
A5	**Políticas de seguridad de la información**	
A5.1	**Directrices de gestión de la seguridad de la información**	Resaltar la importancia de un documento de políticas de seguridad, y su constante revisión.
A5.1.1	Políticas para la seguridad de la información	
A5.1.2	Revisión de las políticas para la seguridad de la información	
A6	**Organización de la seguridad de la información**	
A6.1	**Organización interna**	

A6.1.1	Roles y responsabilidades en seguridad de la información	Definir los roles y responsabilidades del personal de la empresa.
A6.2	**Los dispositivos móviles y el teletrabajo**	Definir las políticas de acceso de dispositivos móviles y remotos.
A6.2.1	Política de dispositivos móviles	
A6.2.2	Teletrabajo	
A8	**Gestión de activos**	
A8.2	**Clasificación de la información**	Asegurar que la información reciba una apropiada protección de acuerdo con su nivel de importancia.
A8.2.1	Clasificación de la información	
A8.2.2	Etiquetado de la información	
A8.2.3	Manipulado de la información	
A9	**Control de acceso**	
A9.1	**Requisitos de negocio para el control de acceso**	Definir las políticas de acceso a la información y a los servicios de la empresa
A9.1.1	Política de control de acceso	
A9.1.2	Acceso a las redes y a los servicios de red	
A9.2	**Gestión de acceso de usuario**	Garantizar que los usuarios autorizados puedan accedes a los servicios que les corresponde.
A9.2.1	Registro y baja de usuario	
A9.2.2	Provisión de acceso de usuario	
A9.2.3	Gestión de privilegios de acceso	
A10	**Criptografía**	
A10.1	**Controles criptográficos**	Garantizar la integridad autenticidad y la confidencialidad de la información.
A10.1.1	Política de uso de los controles criptográficos	
A10.1.2	Gestión de claves	
A12	**Seguridad de las operaciones**	
A12.1	**Procedimientos y responsabilidades operacionales**	Gestionar el uso de los servicios que atraviesan el sistema de seguridad perimetral.
A12.1.3	Gestión de capacidades	

A12.2	**Protección contra el software malicioso (malware)**	Definir las capacidades del sistema de seguridad perimetral frente a malware.
A12.2.1	Controles contra el código malicioso	
A12.5	**Control del software en explotación**	Definir las capacidades del sistema de seguridad perimetral para detectar y prevenir explotación de vulnerabilidades.
A12.5.1	Instalación del software en explotación	
A13	**Seguridad de las comunicaciones**	
A13.1	**Gestión de la seguridad de las redes**	Definir la arquitectura de red y los controles que aseguren la protección de la información
A13.1.1	Controles de red	
A13.1.2	Seguridad de los servicios de red	
A13.1.3	Segregación en redes	
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	
A14.1	**Requisitos de seguridad en los sistemas de información**	Definir los requisitos de seguridad de servicios publicados en Internet
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	

3.3 PROPUESTA DE POLITICAS DE SEGURIDAD

3.3.1 Políticas de Seguridad en base a los controles seleccionados

De acuerdo a los controles seleccionados y al levantamiento de información, se redacta la propuesta de políticas de seguridad que mejorarán las políticas actuales, además, la propuesta está alineada con las recomendaciones expuestas en la norma ISO/IEC 27002 (ISO/IEC, 2013).

Tabla 3-5 Propuesta de políticas de seguridad referentes a seguridad perimetral

	CONTROLES DE SEGURIDAD DE LA INFORMACIÓN
A5	**Políticas de seguridad de la información**
A5.1	**Directrices de gestión de la seguridad de la información**
A5.1.1	Políticas para la seguridad de la información

Se propone que la gerencia general en conjunto con la gerencia técnica deberá elaborar un documento de Políticas de Seguridad de Información en el cual se defina claramente las políticas de acceso, las políticas de uso de los recursos, los privilegios de usuarios y las técnicas de protección de la información. Este documento deberá ser socializado en un tiempo prudente y estar disponible para todo el personal que labore en la empresa.	
A5.1.2	Revisión de las políticas para la seguridad de la información
Se propone que las políticas de seguridad de la información deberán ser revisadas constantemente por la gerencia general y la gerencia técnica de manera semestral o en caso de un cambio sustancial en la empresa, con el fin de validar su aplicación y en caso de ser necesario actualizarse, cambiarse o eliminarse de acuerdo a los requerimientos actuales de la empresa.	
A6	**Organización de la seguridad de la información**
A6.1	**Organización interna**
A6.1.1	Roles y responsabilidades en seguridad de la información
Se propone la definición de los roles y responsabilidades de cada departamento con el fin de determinar los privilegios de acceso del personal de la empresa a los diferentes servicios existentes, así como también los privilegios de acceso para el personal externos. El departamento de recursos humanos deberá informar a la gerencia general y a la gerencia técnica el ingreso o salida de personal a la empresa, con el fin de gestionar los permisos de acceso y uso de recursos empresariales. Únicamente la gerencia general y la gerencia técnica podrán autorizar el acceso a la red a los dispositivos tanto del personal que labore en la empresa como al personal externo. Únicamente el departamento técnico tendrá la autorización de generar los accesos solicitados por gerencia bajo las políticas de acceso y uso de recursos que defina la gerencia. Únicamente el personal del departamento técnico tendrá la autorización de administrar y operar los dispositivos de la infraestructura de red y en caso de requerirse el apoyo de un proveedor externo, se le otorgará el acceso previa autorización de gerencia y con la supervisión del personal del departamento técnico. El personal de toda la empresa deberá ser responsable de guardar de manera confidencial las credenciales de acceso otorgadas por el departamento técnico. El uso de estas credenciales será de responsabilidad exclusiva de cada persona que labore en la empresa. Todo el personal que labore en la empresa deberá firmar un acuerdo de confidencialidad, el cual deberá detallar que toda información tanto de clientes, proveedores y de la misma empresa es de carácter confidencial de acuerdo a los niveles que se presenta en la clasificación de información.	

A6.2	**Los dispositivos móviles y el teletrabajo**
A6.2.1	Política de dispositivos móviles

Se propone que únicamente los dispositivos móviles del tipo laptop que pertenezcan al inventario de la empresa podrán tener acceso a los recursos en base a las políticas de control por usuarios.

Con respecto a dispositivos móviles del tipo smartphone y tablet personales, únicamente la gerencia técnica tendrá la potestad de autorizar su conexión a la red con el uso del aplicativo para reconocimiento de políticas de control por usuario.

Para dispositivos móviles de personal externo se propone que esta conexión deberá ser temporal y a través de la red de invitados la cual no deberá tener acceso a los recursos internos de la empresa.

Todos los dispositivos móviles contarán con la protección y prevención de ataques provista por el sistema de seguridad perimetral.

A6.2.2	Teletrabajo

Se propone que el acceso remoto a la red de la empresa con fines de teletrabajo deberá ser otorgado con previa autorización de la gerencia general y la gerencia técnica, mediante el uso de un agente VPN que permitirá una conexión segura y encriptada, este acceso será exclusivo para el personal que labore en la empresa y únicamente el personal del departamento técnico tendrá la autorización de instalar y configurar el agente en los dispositivos del personal.

La confidencialidad de las credenciales de acceso único serán responsabilidad de cada usuario y en caso de detectarse un uso inadecuado se procederá con la inhabilitación temporal o permanente del acceso remoto.

Una vez que el usuario disponga de la conexión remota segura y encriptada, el usuario contará con el acceso a los recursos empresariales con los privilegios asignados por la gerencia mediante el control de accesos por usuario, así como las protección y prevención que ofrece el sistema de seguridad perimetral.

A8	**Gestión de activos**
A8.2	**Clasificación de la información**
A8.2.1	Clasificación de la información

Se propone que la información que maneja la empresa deberá ser clasificada en base a niveles de confidencialidad, disponibilidad y riesgo. Los cuatro niveles correspondientes podrían ser los siguientes:

- Nivel bajo: su divulgación o pérdida no causa daños.
- Nivel medio: su divulgación o pérdida causa un impacto menor a la operación de la empresa.
- Nivel alto: su divulgación o pérdida causa un impacto significativo a la operación de la empresa.

• Nivel crítico: su divulgación o pérdida causa un impacto grave y pone en riesgo la supervivencia de la empresa.	
A8.2.2	Etiquetado de la información
Se propone que la información deberá ser etiquetada de acuerdo a los niveles de clasificación con el fin de determinar las políticas de acceso, uso y almacenamiento en sus correspondientes repositorios. La información que maneja la empresa podría etiquetarse de la siguiente manera. • Nivel bajo: Información profesional del personal de la empresa, de proveedores y contratistas. • Nivel medio: Información comercial de clientes. • Nivel alto: Información contable y financiera de la empresa, información presupuestaria de clientes y procesos de adjudicación. • Nivel crítico: Información técnica confidencial de cliente, respaldos de configuración de equipos	
A8.2.3	Manipulado de la información
Se propone que el acceso al tipo de información de cada nivel, deberá estar restringido de acuerdo a las políticas de control de accesos definidos por las gerencias. Todo el personal de la empresa deberá hacer uso de los medios empresariales para el almacenamiento de la información y únicamente su compartición estará permitida a través del correo institucional, en el caso actual, mediante las herramientas que ofrece Microsoft Office365.	
A9	**Control de acceso**
A9.1	**Requisitos de negocio para el control de acceso**
A9.1.1	Política de control de acceso
Se propone la definición de políticas de acceso basadas en los roles y las responsabilidades de cada departamento utilizando la premisa "Todo está generalmente prohibido a menos que se permita expresamente." Únicamente el personal del departamento técnico, así como gerencia tendrá acceso a la información confidencial recopilada de los clientes de la empresa ya sea en levantamientos de información previos a la ejecución de un proyecto o a la información confidencial recopilada durante el tiempo de contrato de servicios. Únicamente el personal del departamento de contabilidad y financiero tendrá autorización de acceso al servicio contable de la empresa, mediante credenciales propias del sistema. El departamento de contabilidad y financiero deberá presentar los reportes necesarios que gerencia requiera para los análisis semanales, mensuales o anuales. Únicamente el departamento de recursos humanos y gerencia tendrán acceso a la documentación profesional de todo el personal que labore en la empresa, así como de los proveedores y contratistas.	

Únicamente el personal del departamento comercial tendrá acceso a la documentación comercial y presupuestaria de los clientes que maneje cada asesor.

El personal externo tendrá únicamente acceso al servicio de Internet mediante el ISP secundario con políticas de navegación restrictivas definidas por gerencia.

Todo el personal de la empresa tendrá acceso a Internet mediante balanceo de carga entre el ISP principal y el secundario únicamente utilizando sus dispositivos empresariales, las políticas de navegación serán mediante perfiles restrictivos, los cuales podrían ser los siguientes:

- Departamento técnico: Sin restricción a excepción de contenido adulto y categorías de riesgo.
- Gerencia: Sin restricción a excepción de contenido adulto, acceso remoto y categorías de riesgo.
- Departamento comercial: Sin restricción a excepción de contenido adulto, acceso remoto, entretenimiento, streaming y categorías de riesgo.
- General: Sin restricción a excepción de contenido adulto, acceso remoto, entretenimiento, streaming, redes sociales y categorías de riesgo.

A9.1.2	Acceso a las redes y a los servicios de red

Se propone que los accesos a la red y a sus servicios deberá ser autorizados por la gerencia general y gerencia técnica y deberá ser monitoreada por el departamento técnicos.

El acceso a los recursos empresariales será exclusivo del personal de la empresa, en base a las políticas de control de accesos por departamento.

El acceso a los recursos empresariales por parte del personal de la empresa deberá ser a través de cableado si se dispone de puntos de red o a través de la red WiFi empresarial, la cual deberá ser configurada por el departamento técnico.

Únicamente el personal de la empresa contará con credenciales, las mismas que le darán acceso dependiendo de los privilegios otorgados por gerencia, así como el acceso remoto a la red mediante el agente VPN, previa autorización de la gerencia técnica.

El acceso a los recursos empresariales para personal externo estará restringido, únicamente la gerencia técnica tendrá la potestad de autorizar el acceso a personal externo con la supervisión del personal del departamento técnico o el departamento en cuestión del soporte.

El acceso personal externo deberá ser a través de la red inalámbrica para invitados, la cual permitirá una conexión temporal mediante un portal cautivo para hacer uso únicamente del servicio de Internet.

A9.2	**Gestión de acceso de usuario**
A9.2.1	Registro y baja de usuario

Se propone que el proceso de registro de usuarios deberá ser en conjunto con el departamento de recursos humanos, la gerencia general, la gerencia técnica y el departamento técnico.

El personal de recursos humanos deberá informar por correo electrónico a la gerencia general y a la gerencia técnica cuando se requiera del registro de un nuevo usuario para la empresa. La gerencia general y la gerencia técnica enviará mediante correo electrónico al departamento de recursos humanos y al departamento técnico, su respuesta con los permisos de accesos y los privilegios dependiendo del departamento al cual se integre el nuevo personal. El departamento técnico será el único encargado de realizar el registro de usuarios en los sistemas correspondientes, sea correo electrónico, sistema contable y sistema de seguridad perimetral para los permisos de acceso. Para el proceso de dar de baja a un usuario se deberá enviar un correo electrónico por parte del departamento de recursos humanos hacia el departamento técnico y las gerencias indicando el usuario y los permisos que se deberán eliminar; la revocación de los permisos de acceso y navegación deberá ser ejecutada de manera inmediata por parte del departamento técnico.	
A9.2.2	Provisión de acceso de usuario
Se propone que ningún usuario deberá tener acceso a la red y sus servicios sin previa autorización formal por parte de las gerencias. Los requerimientos de accesos deberán ser enviados por correo electrónico a la gerencia general y gerencia técnica, posterior al análisis, se recibirá un correo eléctrico de respuesta con los permisos y privilegios otorgados por gerencia hacia el departamento técnico para la configuración de los mismos. El departamento técnico deberá hacer una revisión periódica de su sistema de control de usuarios para la depuración de los mismos y el registro de posibles anomalías. Para el sistema contable, se propone una revisión periódica con el proveedor del servicio, para la depuración de usuarios propios del sistema.	
A9.2.3	Gestión de privilegios de acceso
Se propone que los privilegios de accesos deberán ser en base a las funciones de cada departamento definidas por las gerencias. En caso de requerir un cambio en los permisos de acceso o navegación, se deberá realizar la solicitud formal mediante correo electrónico a la gerencia de su departamento y a la gerencia técnica. En la solicitud se deberá indicar los accesos requeridos y el motivo por el cual es necesario el cambio, la gerencia técnica lo analizará en conjunto con la gerencia general y se enviará una respuesta por correo electrónico al solicitante y al departamento técnico para ejecutar o no el cambio solicitado. El departamento técnico deberá llevar un registro de las políticas aplicables a cada usuario y de los cambios solicitados, aprobados o rechazados.	
A10	**Criptografía**

A10.1	**Controles criptográficos**
A10.1.1	Política de uso de los controles criptográficos
Se propone el uso de controles criptográficos especialmente para acceso remoto y los servicios publicados en Internet de la empresa. El departamento técnico estará a cargo de la ejecución de los procesos de encripción tanto para acceso remoto como para los servicios de la empresa. En orientación con mantener la confidencialidad, integridad y autenticidad de la información, todo el personal que adquiera la autorización para acceso remoto mediante el agente VPN deberá solicitar al departamento técnico la instalación de los certificados del sistema de seguridad perimetral para encriptar la comunicación entre el agente VPN de la laptop y la red de la empresa. Las conexiones remotas que no cuenten con el certificado instalado en sus dispositivos, no podrán tener acceso a los servicios de la empresa. Respecto a los servicios publicados en Internet de la empresa deberán contar con un dominio DNS y su respectivo registro, además del uso de certificados firmados por una entidad certificadora.	
A10.1.2	Gestión de claves
Se propone que todos los certificados y sus llaves deberán tener un tiempo máximo de expiración de dos años. El departamento técnico deberá realizar los procesos de renovación tanto para el personal como para los servicios publicados en Internet de la empresa.	
A12	**Seguridad de las operaciones**
A12.1	**Procedimientos y responsabilidades operacionales**
A12.1.3	Gestión de capacidades
Se propone que el departamento técnico deberá realizar un monitoreo proactivo del uso de enlace principal de salida a Internet, con el fin de evitar cuellos de botella que afecten a las aplicaciones críticas de la empresa, como son el correo electrónico, la mesa de ayuda, conexiones VPN, el acceso al portal de compras públicas y el respaldo de la información en sincronismo con Microsoft Office365. El departamento técnico deberá realizar las configuraciones necesarias para restringir el uso de ancho de banda para aplicaciones como video streaming, estas políticas asegurarán un máximo de 4Mbps para aplicaciones que no son relevantes a la empresa, cuando estas son permitidas por los permisos de acceso otorgados por gerencia. El departamento técnico deberá realizar las configuraciones necesarias para limitar las actualizaciones de sistemas operativos a un máximo de 4Mbps en horarios laborales. A pesar de que la sincronización de información de manera segura con Microsoft Office365 al igual que las actualizaciones de sistema operativo son servicios críticos, estos deben ser limitados a un	

máximo de 4Mbps en horario laboral, ya que podría congestionar el ancho de banda si el sincronismos es para archivos a la actualización es superior a 1GB de transferencia.	
A12.2	**Protección contra el software malicioso (malware)**
A12.2.1	Controles contra el código malicioso
Se propone la implementación de controles de detección y prevención contra malware, así como la capacitación al personal de la empresa para el uso apropiado del sistema operativo y de Internet. El departamento técnico deberá configurar los perfiles de seguridad que permitan la detección y prevención de malware oculto en websites o aplicaciones conocidas o sospechosos para la protección de todo el personal que se conecte a la red de la empresa. El departamento técnico deberá configurar el sistema de seguridad perimetral para que tenga la capacidad de detectar en tiempo real amenazas de malware de día cero y permita la aplicación de controles de manera automatizada e inmediata.	
A12.5	**Control del software en explotación**
A12.5.1	Instalación del software en explotación
Se propone que únicamente el departamento técnico tendrá acceso a descargas de archivos ejecutables o modificaciones de sistema operativo, con el fin de analizar si el software requerido presenta información de vulnerabilidades o malware reportado previo a su instalación. Todos los dispositivos de la empresa deberán estar actualizados con los parches necesarios para disminuir los riesgos de explotación por vulnerabilidades. La arquitectura de red deberá tener la capacidad de separar a los dispositivos con versiones de software o sistema operativo obsoletos que por alguna razón se mantengan en la empresa, sin embargo, se deberá realizar el plan de reemplazo para disminuir este riesgo de seguridad.	
A13	**Seguridad de las comunicaciones**
A13.1	**Gestión de la seguridad de las redes**
A13.1.1	Controles de red
Se propone que únicamente el departamento técnico deberá tener el acceso para la administración de los dispositivos de red y seguridad, sin embargo, los cambios a realizarse deberán ser aprobados previamente por la gerencia técnica. La conexión a la red mediante cableado y WiFi empresarial será exclusiva de los usuarios de la empresa mediante el aplicativo de control de accesos por usuarios, el cual permitirá ejecutar los permisos de accesos y navegación definidos por gerencia. El departamento técnico deberá ser el único conocedor de las credenciales de acceso a la red WiFi empresarial.	

El personal de la empresa deberá estar autenticado con las credenciales otorgadas por el departamento técnico para poder acceder a los recursos de la empresa.	
A13.1.2	Seguridad de los servicios de red
Se propone que el sistema de seguridad perimetral deberá asegurar todas las conexiones entrantes y salientes de la red mediante mecanismos de control de acceso, restricciones de navegación y técnicas de prevención contra ataques que incluyan malware, phishing, virus, exploits etc.	
A13.1.3	Segregación en redes
Se propone que el sistema de seguridad perimetral deberá tener la capacidad de controles por zonas para permitir la segmentación de redes dependiendo del nivel de confianza (Internet, servidores, desmilitarizada, usuarios, invitados, desarrollo). La zona de usuarios podrá ser segmentada lógicamente de acuerdo a los diferentes departamentos que operan en la empresa (gerencias, técnicos, comercial, recursos humanos, general). El sistema de seguridad perimetral deberá hacer las funciones de Gateway de cada red y definirá las políticas de acceso tanto por redes como por usuarios.	
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**
A14.1	**Requisitos de seguridad en los sistemas de información**
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas
Se propone las políticas de seguridad referentes a los servicios publicados en Internet como son la página web y la mesa de ayuda. Los servicios estarán publicados mediante un control de políticas en base a aplicaciones y perfiles de seguridad a través del sistema de seguridad perimetral. El departamento técnico será el encargado de realizar los procesos para generación de certificados para el tráfico seguro de los servicios en Internet. La página web deberá ser de acceso público y únicamente informativa, los cambios a realizarse en el código HTML serán responsabilidad exclusiva del proveedor del sitio web de acuerdo a las solicitudes de las gerencias. El servicio de mesa de ayuda deberá ser de uso exclusivo de los clientes para lo cual el departamento deberá generar las credenciales de acceso para el reporte de incidentes o soportes en la mesa de ayuda. Toda la información recopilada por la mesa de ayuda será de acceso exclusivo del departamento técnico y de las gerencias.	

CAPÍTULO 4: REDISEÑO DE LA ARQUITECTURA DE RED Y SEGURIDAD PERIMETRAL

En este capítulo se presenta la propuesta de rediseño de la arquitectura de red y de seguridad perimetral en base a la definición de la metodología de seguridad perimetral escogida y de la propuesta de políticas de seguridad para la empresa AKEA S.A

4.1 PROPUESTA DE REESTRUCTURACIÓN DE LA RED

Después del levantamiento de información realizado, se identificó ciertas falencias de la red al no tener una estructura organizada de acuerdo a las funciones o servicios. Por lo tanto, se propone una reorganización de la red y la inclusión de algunos servicios que permiten mejorar el control en base a las políticas de seguridad.

4.1.1 Segmentación de la red

La segmentación de redes en una empresa es de vital importancia para poder mantener un control de acceso hacia los diferentes servicios. Para este escenario, se realiza la propuesta de segmentación de redes en base a los servicios que representan, sin embargo, las políticas de control de accesos se plantean realizar en base a usuarios. En la Tabla 4-1 se presenta la propuesta de segmentación de red:

Tabla 4-1 Segmentación de redes según su función

DESCRIPCION	SERVICIO	RED	FUNCION
RED INTERNET	ISP-Principal	NA	Esta red es entregada por el proveedor de servicio. Se tiene contratado 40Mbps de servicio de Internet y la asignación de una IP publica estática para la publicación de servicios.
	ISP-Secundario	NA	Esta red es entregada por el proveedor de servicio. Se tiene contratado 20Mbps de servicio de Internet y la asignación de una IP publica estática para la publicación de servicios.

RED LAN	Administración	192.168.1.0/24	Red exclusiva para la administración de dispositivos de red como Switch, Wireless, Firewall, etc.
	Usuarios	192.168.2.0/24	Red exclusiva para el personal que labora en la empresa.
	Invitados	192.168.3.0/24	Red exclusiva para personal externo que visita las instalaciones de la empresa. Conexión únicamente por Wireless.
	Wireless	192.168.4.0/24	Red exclusiva del servicio de Wireless para uso del personal interno de la empresa.
	Telefonía IP	192.168.5.0/25	Red exclusiva para el servicio de telefonía IP, pensado a futuro para comunicaciones unificadas y videoconferencia.
	Impresión	192.168.5.128/25	Red exclusiva para el servicio de impresión, que incluye impresoras, copiadoras, escáner y multifunción.
RED SERVIDORES	Servicios Internos	192.168.6.0/24	Red exclusiva para los servicios internos de la empresa tales como el servicio contable, la intranet, etc. Estos servicios son de uso interno y no deben ser publicados hacia Internet.
RED DMZ	Servicios Externos	192.168.7.0/24	Red exclusiva para los servicios externos de la empresa, es decir servicios que permiten su uso desde Internet, tales como la página web y la mesa de ayuda.

RED DESARROLLO	Desarrollo	192.168.8.0/24	Red exclusiva para ambientes de pruebas o desarrollos, para no afectar la continuidad del servicio de las redes en producción.

4.1.2 Categorización de usuarios

A nivel empresarial, es necesario contar con un sistema de control de usuarios; lo ideal sería disponer de un directorio activo a través del cual se pueda realizar el registro y activación de cuentas del personal que labora en la empresa. El uso de un directorio activo permite la centralización de configuraciones, ya que se puede realizar la configuración del correo electrónico, así como la extensión del servicio de telefonía IP para cada usuario, además de los privilegios de accesos a servicios compartidos y sobre el sistema operativo.

En este caso, la empresa no dispone de un directorio activo, por lo que se propone como alternativa el uso de la base de datos local del sistema de seguridad perimetral para la categorización de usuarios. Palo Alto Networks permite la creación de usuarios y grupos de usuarios de manera local y mediante el uso de su agente Global Protect configurado como gateway interno, el personal de la empresa se puede registrar con las credenciales asignadas para obtener los privilegios de acceso y navegación determinados para ese usuario.

El control en base a usuarios está orientado para el personal que labora en la empresa, por lo que se genera credenciales permanentes en la base de datos local, en la Tabla 4-2 se presenta la clasificación de usuarios según sus funciones, lo cual permitirá determinar los privilegios de cada usuario o grupo de usuarios.

Tabla 4-2 Clasificación de grupos de usuarios según su función

GRUPO USUARIOS	FUNCION
Gerencias	Personal de la empresa responsable del funcionamiento de cada departamento y de la toma de decisiones de la empresa.
Departamento Técnico	Personal especializado en soluciones tecnológicas, encargado de la administración y funcionamiento de la red de la empresa, así como de sus servicios. Departamento encargado del dimensionamiento e implementación de soluciones tecnológicas para los clientes de la empresa.

Departamento Contable	Personal especializado en el área contable y financiera que en conjunto con gerencia están encargados del flujo económico de la empresa
Departamento Comercial	Personal especializado en el área comercial encargado de la búsqueda de potenciales clientes, así como el mantenimiento de la relación comercial con clientes ya existentes.
Departamento Talento Humanos	Personal especializado en el área de talento humano encargado de la revisión de la experiencia laboral de futuros colaboradores, o contratistas, así como de mantener al personal de la empresa en un ambiente laboral aceptable para el cumplimiento de sus funciones.
Departamento Administrativo	Personal especializado en el área de administrativa para apoyo a las gerencias y demás departamentos, además se encuentra el personal de mensajería y de logística de la empresa

4.1.3 Parámetros de alta disponibilidad

Un factor importante a considerar es la disponibilidad de los servicios y cuanto afectaría a la producción de la empresa en caso de que uno de ellos faltase. Por lo tanto, se presenta los siguientes aspectos para cumplir con una arquitectura de alta disponibilidad:

- *ISP redundante:* AKEA S.A al ser una empresa orientada a las soluciones tecnológicas y al soporte de sus clientes, es indispensable que cuente con conectividad hacia Internet, por tal razón, se ha considerado el uso de dos ISP, NETLIFE como proveedor principal con 40Mbps de enlace y TVCABLE como proveedor secundario con 20Mbps de enlace. El enlace principal es de uso exclusivo de los usuarios de la empresa y de sus servicios, el enlace secundario es de uso compartido entre los usuarios de la empresa y los usuarios invitados con el fin de garantizar que el consumo de los usuarios invitados no congestione el enlace para los servicios empresariales.
- *Seguridad Perimetral*: se ha considerado que el equipamiento de seguridad perimetral debe garantizar la operatividad de la empresa es por esto que se propone una solución de equipamiento físicos en alta disponibilidad activo-pasivo. En esta modalidad, los equipos sincronizan en tiempo real las configuraciones que se realiza en el equipo activo hacia el pasivo. Por lo tanto, si llega a existir una falla del equipamiento activo, el pasivo

está listo para tomar el rol de activo y permitir la continuidad del servicio en cuestión de pocos segundos.

Esta transición de pasivo a activo es automática, una vez que se supere el tiempo configurado para el testeo entre los dispositivos, si el equipo pasivo no recibe una respuesta del equipo activo en un tiempo determinado (keepalive), este inmediatamente cambia su estado a activo y transfiere todas las sesiones del anterior equipo hacia él.

- *Respaldo de servicios*: para el tema de respaldos de servicio lo ideal es contar con una solución de respaldo automático como por ejemplo las soluciones de VeeamBackup, sobretodo de las máquinas virtuales que ofrecen servicio tanto interno como externo, pero en este caso, no se dispone de esta solución en la empresa, se propone que el departamento técnico realice respaldos manuales cada mes de las máquinas virtuales y manejar ese repositorio sincronizado con la nube de Microsoft OneDrive.
- *Respaldo de información*: la disponibilidad de la información que maneja cada usuario es indispensable, y en la actualidad las soluciones de almacenamiento en la nube permiten que los usuarios no dependan de un solo dispositivo físico. AKEA S.A cuenta con la solución de Microsoft OneDrive para la sincronización segura y encriptada de sus archivos en la nube del proveedor, esta información está disponible para cada usuario desde cualquier punto de conexión a Internet.

4.1.4 Arquitectura de red propuesta

Considerando lo anteriormente expuesto, la arquitectura de red propuesta varía sustancialmente relacionada con la arquitectura actual de la empresa. En la Figura 4-1 se puede identificar los nuevos parámetros considerados para que la empresa cuente con una arquitectura orientada al control de accesos y a la seguridad perimetral. Tomar en consideración que la red LAN esta segmentada en Vlans de usuarios, Vlan de invitados, Vlan de administración, Vlan de impresión y Vlan de telefonía IP.

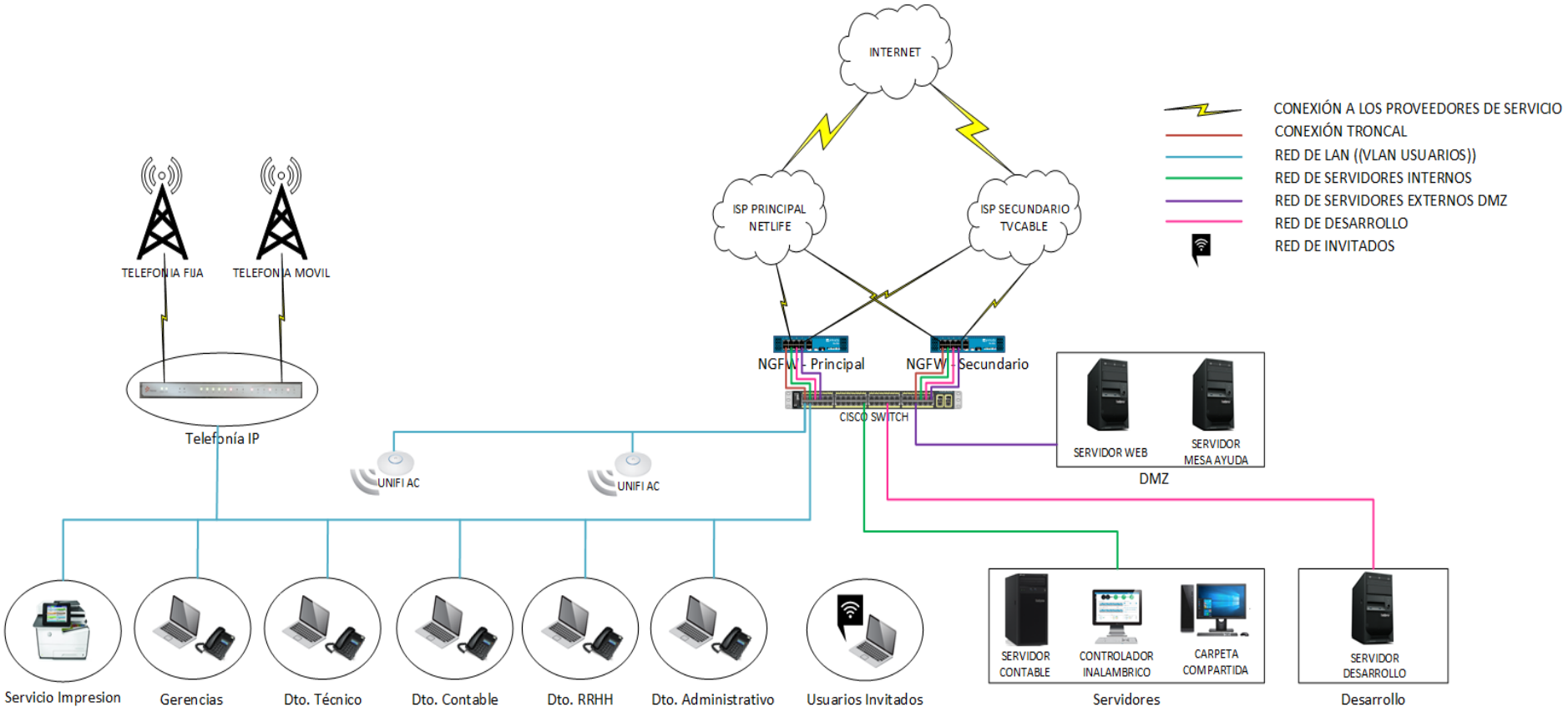


Figura 4-1 Arquitectura de red propuesta

4.2 EQUIPAMIENTO DE SEGURIDAD PERIMETRAL

4.2.1 Selección de equipamiento

Una vez determinada la arquitectura de red, se procede con la selección del equipamiento de seguridad perimetral que permita el correcto funcionamiento de la red y de sus políticas de seguridad. A continuación, en la Tabla 4-3, se presentan los parámetros que debe cumplir el equipamiento de seguridad perimetral y la selección del equipo que cumpla con los requerimientos en base a la tabla comparativa de los modelos de equipos que presenta Palo Alto Networks en el Anexo D (Palo Alto Networks, 2020g).

Tabla 4-3 Selección de la solución de seguridad perimetral

PARÁMETRO	REQUERIMIENTO	EQUIPAMIENTO SUGERIDO
Usuarios	Soportar hasta 100 usuarios	PA-220
Interfaces	8 interfaces de 10/100/1000 Mbps	PA-220
Administración	1 interfaz de 10/100/1000 Mbps	PA-220
Ancho de banda	100 Mbps con todas las funcionalidades	PA-220
Almacenamiento	32 GB	PA-220
VPN	VPN site to site y client to site	PA-220
App-ID	Capacidad de clasificación por aplicaciones	PA-220
User-ID	Capacidad de control por usuarios	PA-220
File-Blocking	Capacidad de control por tipo de archivos	PA-220
Data-Filtering	Capacidad de control en base a patrones de datos personalizados	PA-220
URL-Filtering	Capacidad de control en base a filtrado web	PA-220 (Suscripción)
Threat-Prevention	Capacidad de control de amenazas, vulnerabilidades, virus, exploits malware, comando y control.	PA-220 (Suscripción)
Wildfire	Capacidad de control de amenazas de día cero, análisis en la nube.	PA-220 (Suscripción)

Fuente: (Palo Alto Networks, 2020g)

El modelo PA-220, que se muestra en la Figura 4-2, es el modelo en hardware más pequeño y compacto que dispone Palo Alto Networks, sin embargo, cumple con las mismas

funcionalidades que los demás modelos ya que posee el mismo sistema operativo y su principio de Single Pass Parallel Processing (SP3).

Figura 4-2 Palo Alto Networks PA-220
Fuente: (Palo Alto Networks, 2020e)

Tiene la capacidad nativa de control de aplicaciones mediante inspección de capa 7, permite evitar la actividad maliciosa oculta en el tráfico cifrado y refuerza la seguridad para los usuarios en cualquier ubicación, en cualquier dispositivo, mientras adapta las políticas en respuesta a la actividad del usuario (Palo Alto Networks, 2020e).

4.2.2 Propuesta económica

Se solicitó una proforma referencial para la adquisición de la solución de seguridad perimetral, la cual se presenta en el Anexo E. Adicionalmente, se consideró un valor para la implementación de la solución y la reestructuración de la misma, a pesar de que se considera que la configuración la realizaría el personal capacitado del departamento técnico de la misma empresa.

La Tabla 4-4 presenta el resumen de los valores que se deben considerar para esta propuesta

Tabla 4-4 Propuesta económica

ÍTEM	CÓDIGO	DESCRIPCION	CANT.	VALOR UNITARIO	VALOR TOTAL
1	PA-220	NGFW PA-220 Hardware PAN OS 10	2	$ 710.22	$ 1420.44
2	LIC-3Y	Suscripciones por 3 años	2	$ 915.66	$ 1831.32
3	SUPP-3Y	Soporte de Fábrica por 3 años	2	$ 573.91	$ 1147.82
4	CONFIG-NGFW	Configuración y puesta en producción	2	$ 450.00	$ 900.00
				SUBTOTAL	$ 5299.58
				IVA	$ 635.95
				TOTAL	$ 5935.53

4.3 CONFIGURACION DE RED DEL EQUIPO DE SEGURIDAD PERIMETRAL

4.3.1 Configuración de interfaces y zonas de seguridad

Para poder acceder a las configuraciones del equipo de seguridad, se configura una dirección IP de administración la cual debe utilizar únicamente protocolos seguros para el acceso, tales como HTTPS y SSH como se muestra en la Figura 4-3.

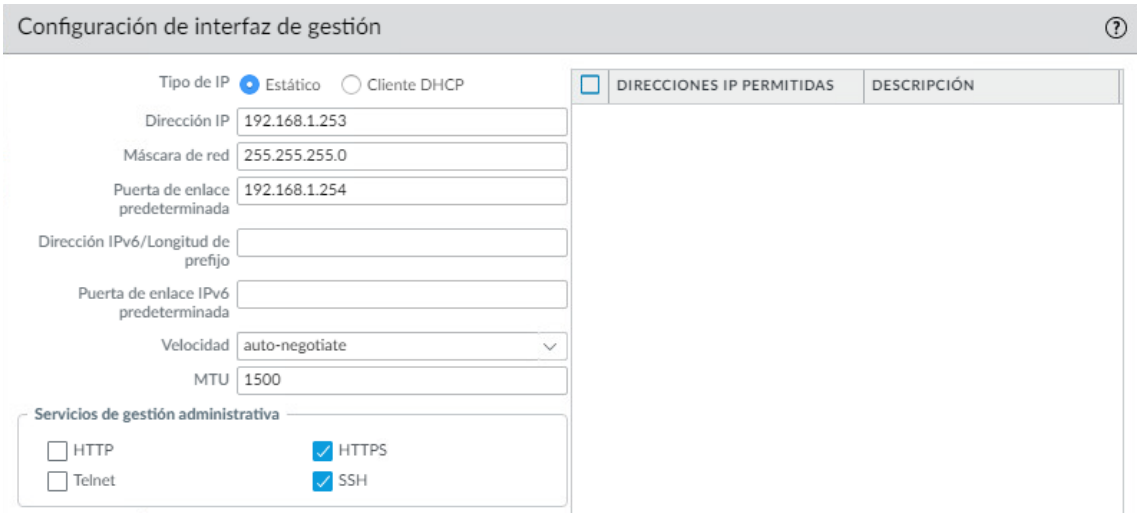


Figura 4-3 Configuración de interfaces de administración

A través de esta interfaz, Palo Alto Networks realiza las operaciones de gestión, como son verificaciones de nuevas actualizaciones de firmware, actualizaciones dinámicas de los servicios de seguridad (Antivirus, App-ID, URL-Filtering, etc.) así como la integración con el directorio activo en el caso de disponer de uno en la empresa.

Para las configuraciones de las interfaces de datos, se considera la reestructuración de red que se propuso anteriormente. Se debe tomar en cuenta que Palo Alto Networks además de considerar la segmentación de redes, utiliza el concepto de zonas de seguridad, una zona de seguridad puede contener diferentes interfaces físicas o virtuales.

En la Figura 4-4, se muestra las configuraciones de las interfaces y las zonas de seguridad de acuerdo a la redistribución de redes propuesta.

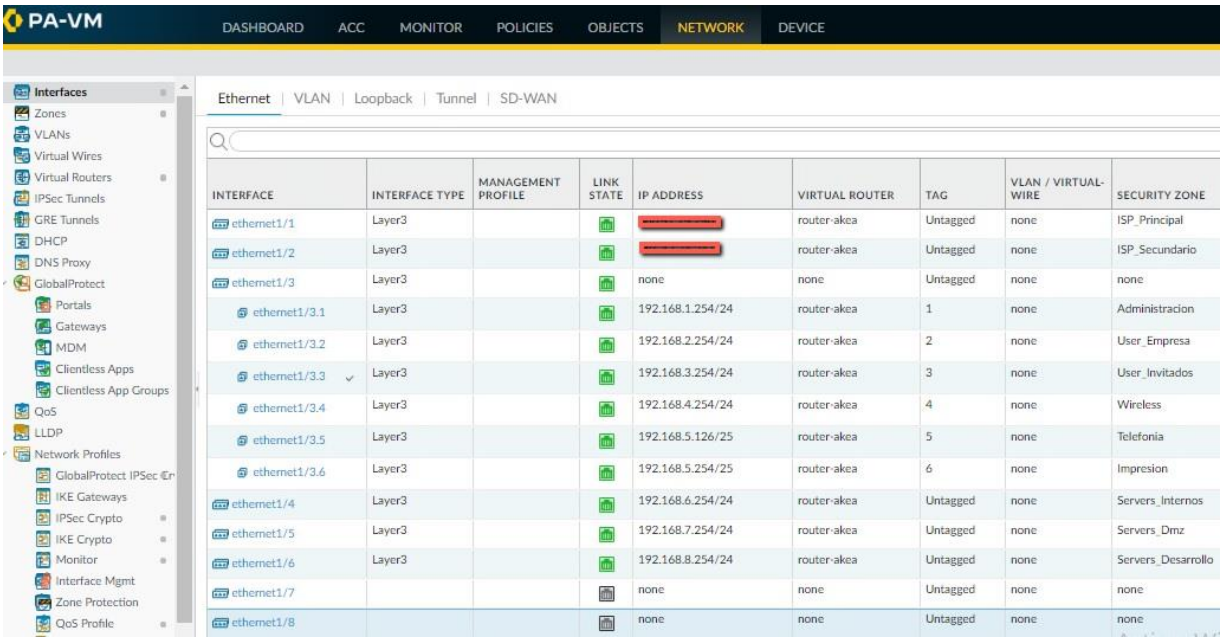


Figura 4-4 Configuración de interfaces y zonas de seguridad

Tomar en consideración que la interfaz ethernet 1/3 debe conectarse a un puerto troncal, para el tráfico de las Vlans de la red interna. Las redes de servidores se considera una conexión directa al NGFW.

4.3.2 Configuración de rutas

Para la interconexión de estas interfaces, los dispositivos de Palo Alto Networks requieren de la configuración de un router virtual como se muestra en la Figura 4-5, en la cual se configura las rutas ya sean estáticas o mediante protocolos dinámicos.

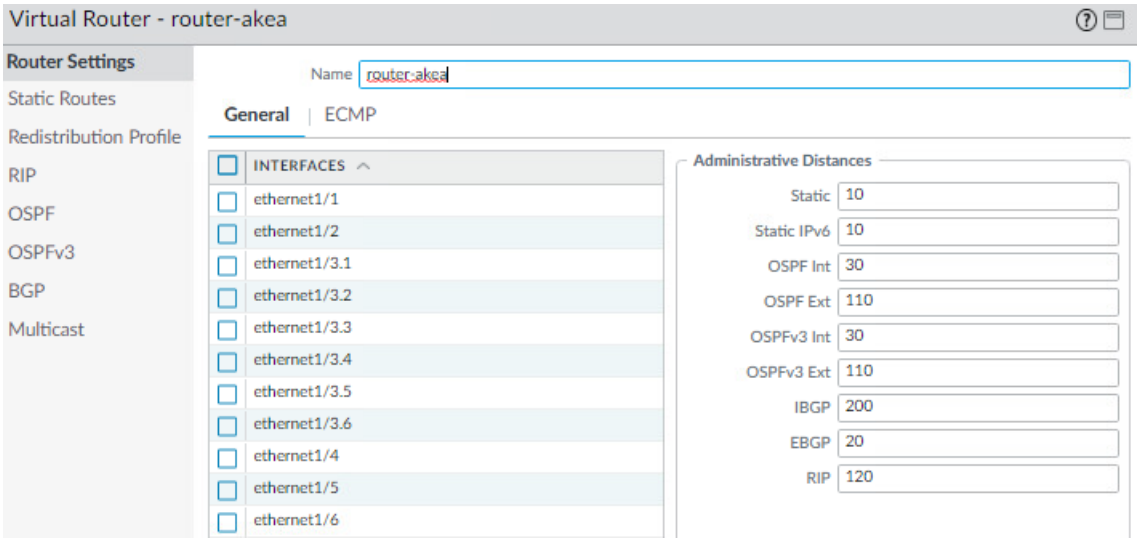


Figura 4-5 Creación del router virtual

En este caso, se utiliza enrutamiento estático con rutas por defecto de igual métrica para el balanceo de carga entre los dos ISPs mediante la habilitación de ECMP (Equal-cost multi-path routing) como se muestra en la Figura 4-7.

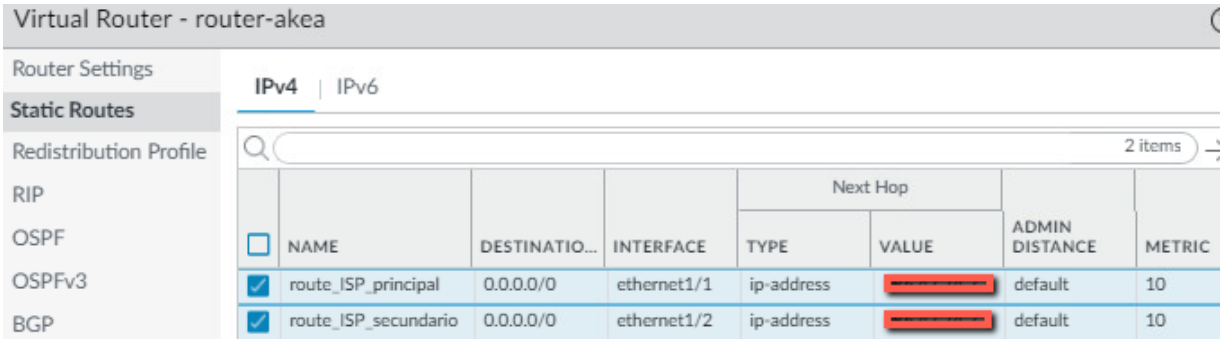


Figura 4-6 Configuración de rutas por defecto

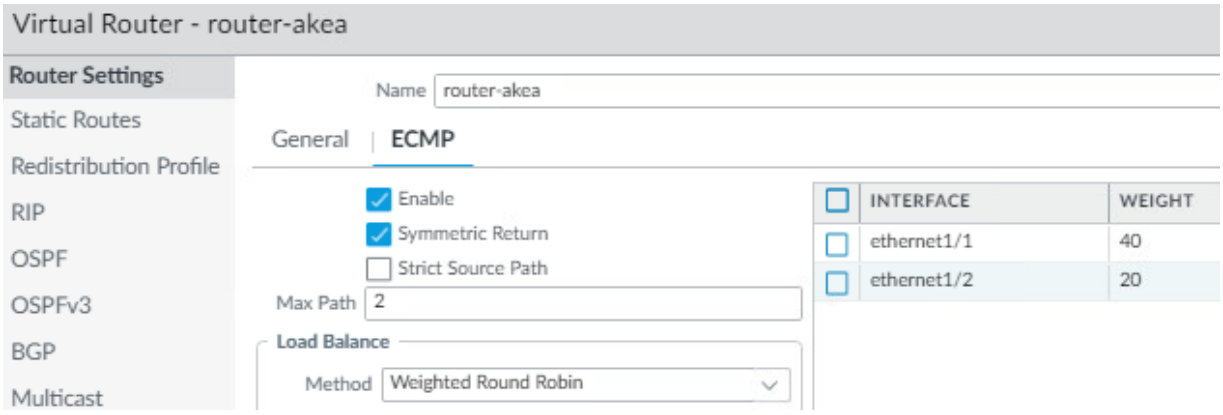


Figura 4-7 Habilitación de ECMP

Adicionalmente, se activa el monitoreo de enlaces con una prueba de disponibilidad para que en caso de falla el tráfico se envíe únicamente por el enlace disponible.

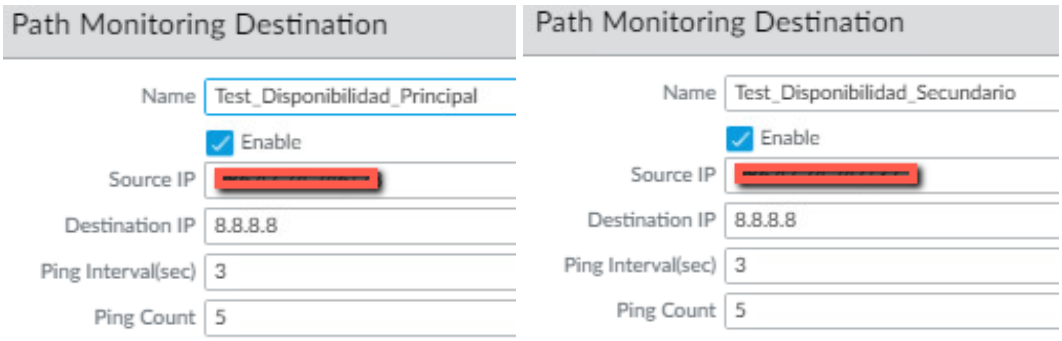


Figura 4-8 Monitoreo de enlaces

4.3.3 Configuración de políticas de NAT

Las configuraciones de NAT se requieren para que las redes internas puedan acceder a la red pública de Internet, la técnica que se utiliza es el enmascaramiento de las direcciones IPs internas en la dirección IP pública entregada por el ISP además del traslado de puertos de servicios a puertos aleatorios.

Como se indicó en las políticas de seguridad, únicamente el personal de la empresa, así como sus servicios utilizan el ISP principal y el ISP secundario, mientras que los usuarios invitados utilizan únicamente el ISP secundario. Para lograr este funcionamiento, se configuran dos políticas de NAT de origen, para el ISP principal y el ISP secundario como se muestra a la Figura 4-9:

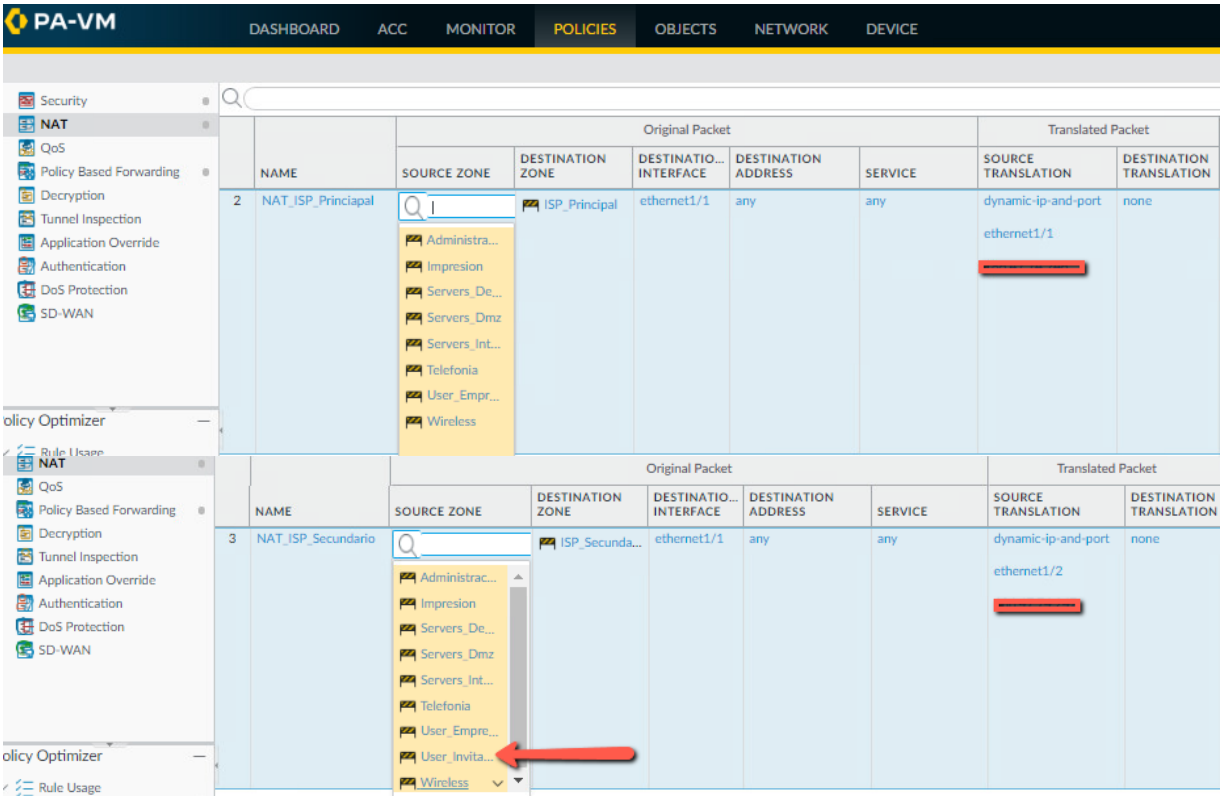


Figura 4-9 Políticas de NAT para uso de Internet

Para que los usuarios invitados no presenten intermitencias en el servicio de Internet por el balanceo de carga entre los proveedores de servicio; es necesario configurar una política de PBF (Policy Base Forwarding) para obligar que el tráfico proveniente de la red de invitados salga únicamente por la interfaz ethernet 1/2 del ISP secundario.

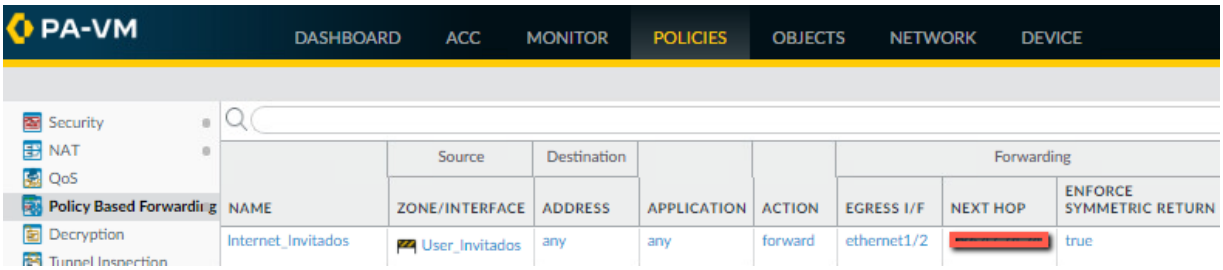


Figura 4-10 Políticas de PBF para la red de invitados

Finalmente, en las políticas de NAT se configura también la publicación de los servicios a través de la dirección IP pública entregada por el ISP principal. Esta técnica es conocida como DNAT (Destination Network Address Translation) y tiene como fin encaminar el tráfico solicitado a la dirección IP pública hacia el servidor interno correspondiente dependiendo del servicio/aplicación solicitado.

En la empresa se tiene publicado dos servicios web que se alojan en un mismo servidor, pero que usan diferentes puertos de servicio. El servidor web usa el puerto estándar 80, mientras que la mesa de ayuda utiliza el puerto 8080. La Figura 4-11 muestra las configuraciones de las políticas de DNAT para estos servicios.

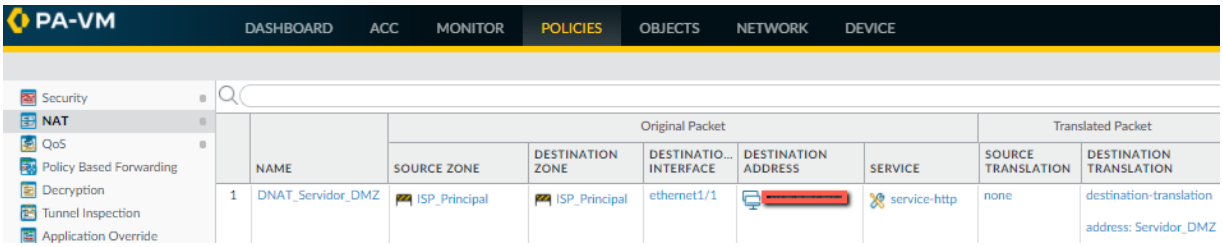


Figura 4-11 Políticas de DNAT para los servicios publicados

Como se muestra en la Figura 4-11, se utiliza el servicio service-http, el cual incluye los puertos 80 y 8080 y lo traslada al servidor interno.

4.3.4 Configuración de usuarios y grupos de usuarios

Como se mencionó anteriormente, la configuración de usuarios y grupos de usuarios para el control de políticas de seguridad, es ideal realizarlo a través de la integración con un Directorio Activo, sin embargo, en este caso se hace uso de la base de datos local que manejan los equipos de Palo Alto Networks. Se realiza la configuración de usuarios y grupos de usuarios de acuerdo a la redistribución propuesta de la red interna.

En la Figura 4-12 se presenta el ejemplo de creación de un usuario de la empresa, en la cual se genera las credenciales de ingreso que le otorgaran los privilegios de navegación y acceso.

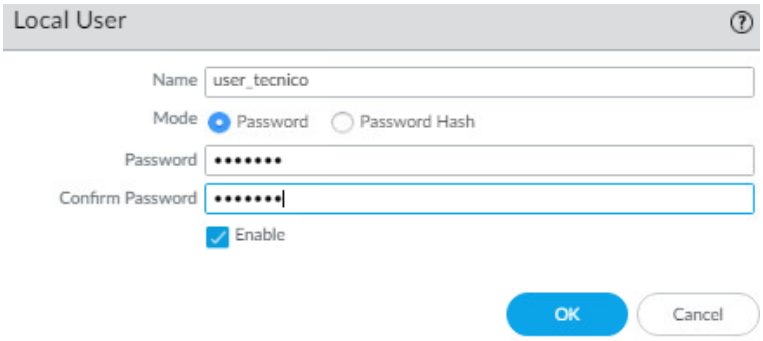


Figura 4-12 Creación de usuarios locales

La creación de grupos permite simplificar el control de las políticas de seguridad, en la Figura 4-13 se muestra los grupos y la asignación de usuarios, según la redistribución propuesta.

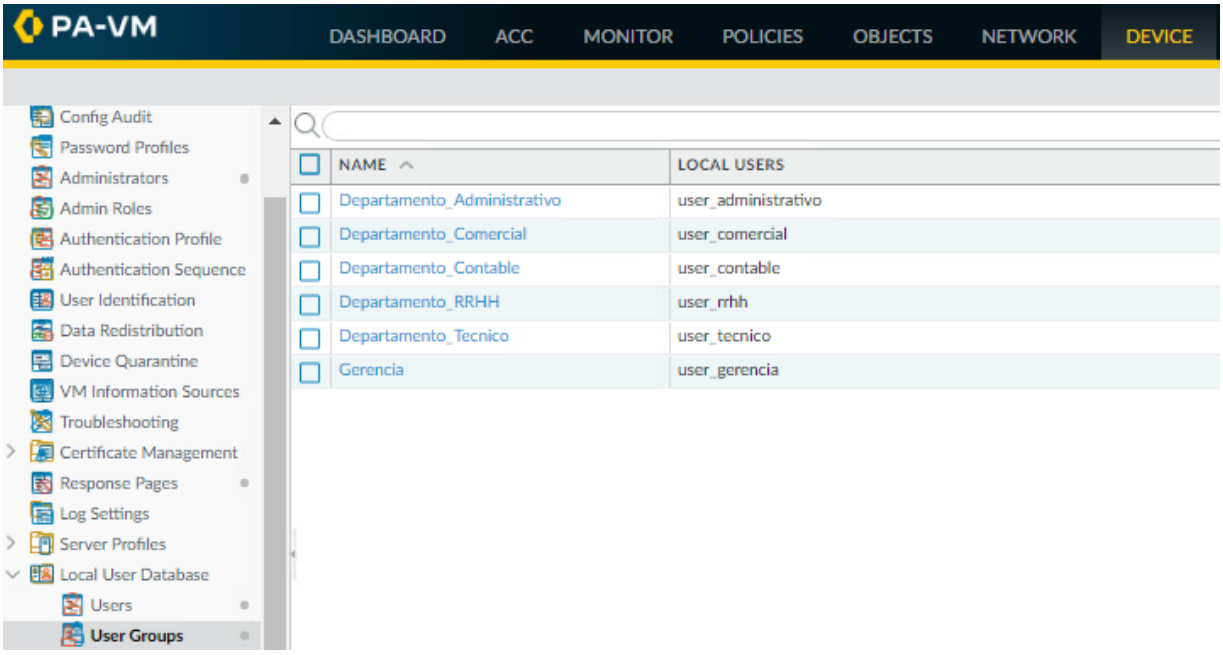


Figura 4-13 Configuración de grupos de usuarios locales

4.3.5 Configuración de agente Global Protect para identificación de usuarios

Cuando se utiliza una base de datos local, se requiere el apoyo de un agente que permita relacionar el usuario con la computadora que utilice. En este caso, Palo Alto Networks permite esta configuración mediante su agente Global Protect configurado como Gateway interno. La guía de configuración paso a paso se encuentra en (Palo Alto Networks, 2018).

La configuración de este agente requiere de un certificado y de un perfil SSL/TLS, el certificado se lo puede generar en Palo Alto Networks como muestra la y se necesita que la cadena de certificados se instale en la raíz de confianza de los equipos de los usuarios.

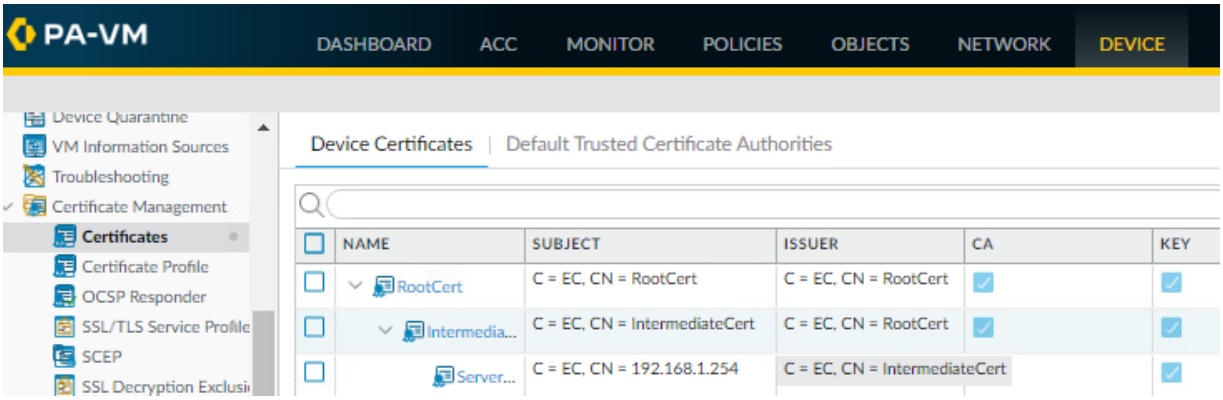


Figura 4-14 Creación de certificados

Se configura un perfil de autenticación indicando que solo los usuarios locales pueden registrarse con el agente Global Protect.

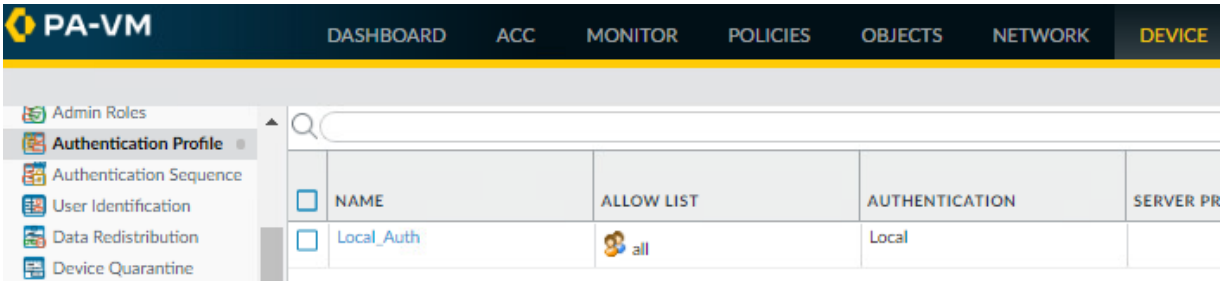


Figura 4-15 Perfil de autenticación

Global Protect requiere la configuración de un portal y de un Gateway en el cual se indica a través de que interfaz y dirección IP el agente registrará a los usuarios. En las Figura 4-16 y Figura 4-17 se muestra las configuraciones principales del Gateway en donde se selecciona el perfil de autenticación.

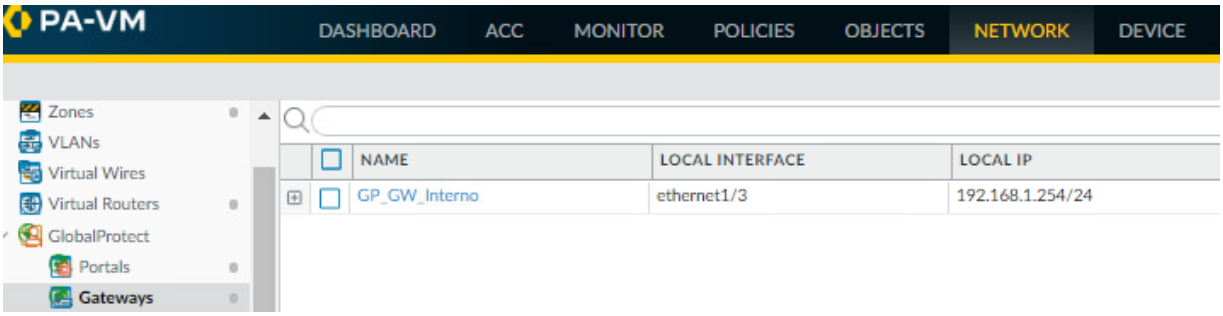


Figura 4-16 Configuración Gateway interno

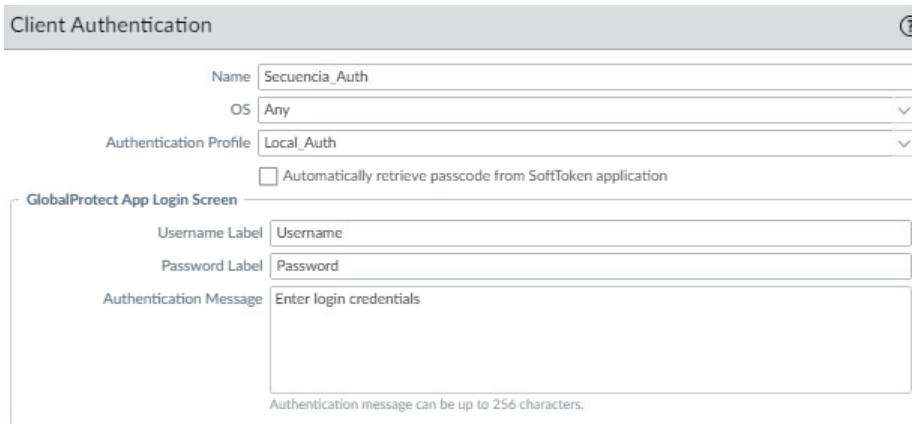


Figura 4-17 Configuración secuencia de autenticación

La configuración del portal implica los parámetros de funcionamiento del agente, se configura de tal manera que solamente el personal técnico tenga la capacidad de realizar cambios en el agente instalado en los equipos de los usuarios, con esto se evita que los usuarios cambien sus privilegios de accesos y navegación. En las Figura 4-18 y Figura 4-19 se muestran los parámetros de configuración del portal de Global Protect.

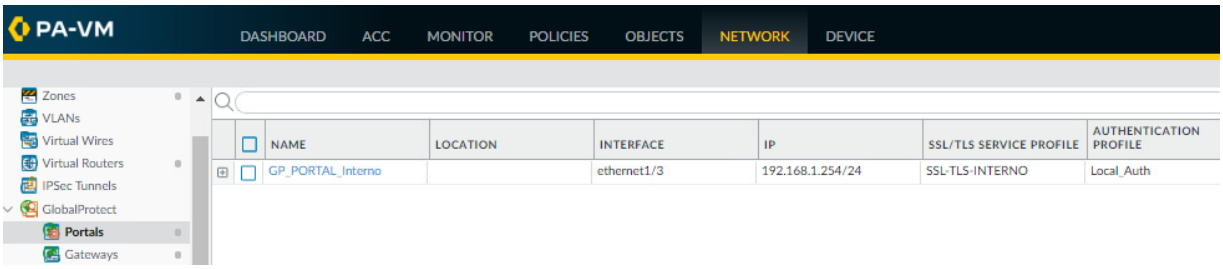


Figura 4-18 Configuración del portal interno

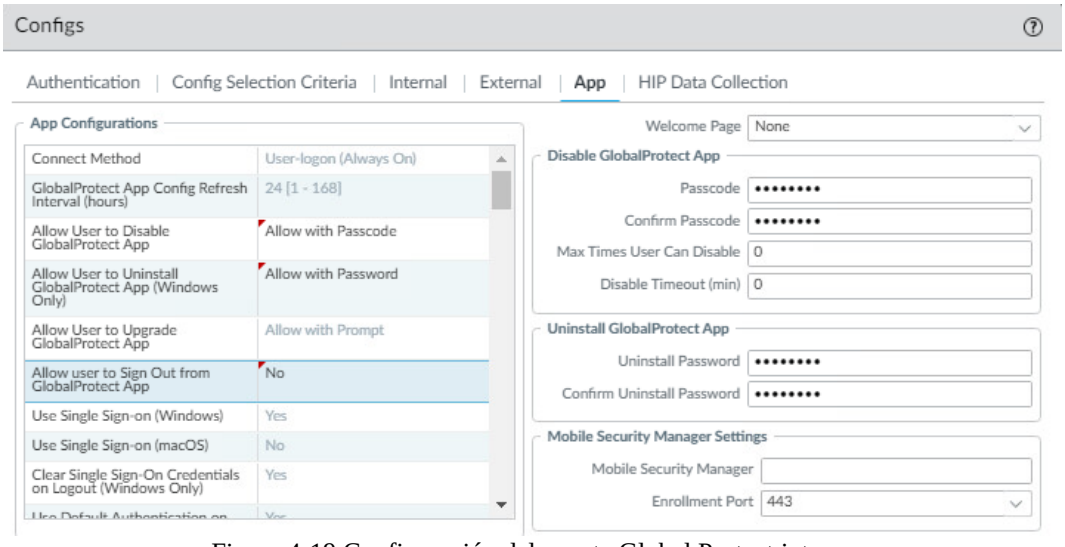


Figura 4-19 Configuración del agente Global Protect interno

A través del navegador web, se ingresa al portal interno con la dirección IP configurada, en esta sección únicamente los usuarios registrados podrán ingresar y descargar el instalador del agente de Global Protect.

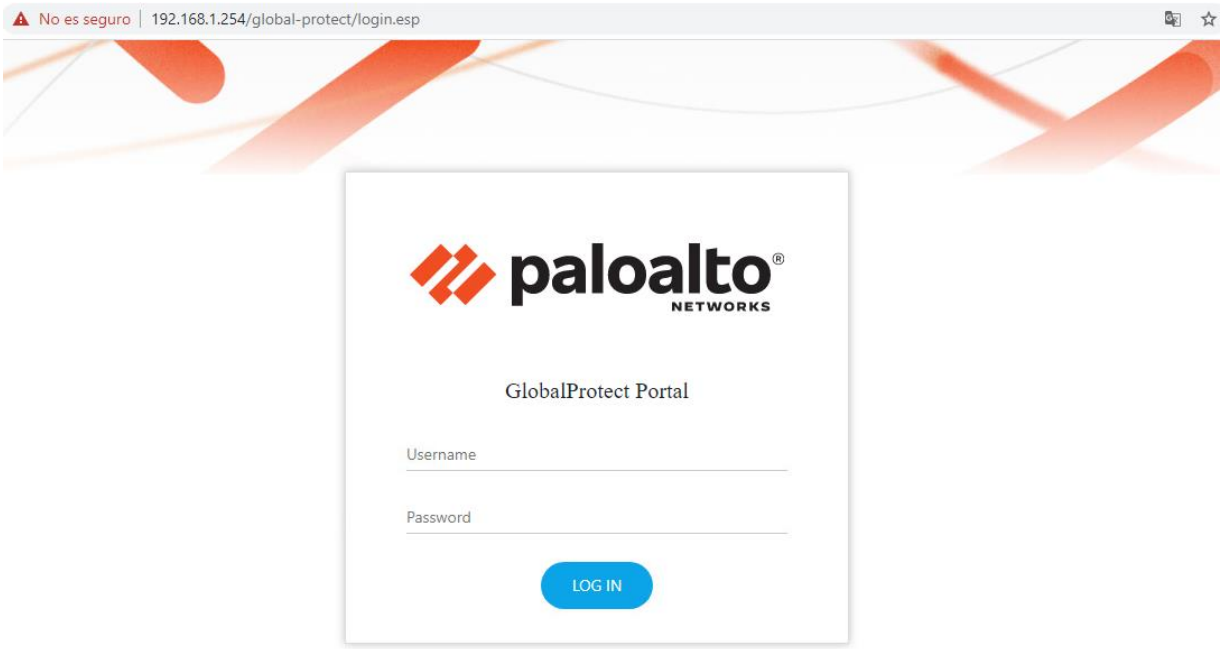


Figura 4-20 Ingreso a la interfaz web del agente Global Protect

Una vez instalado el agente, se debe configurar los parámetros del Gateway, como son la dirección IP y las credenciales del usuario como se muestra en la Figura 4-21.

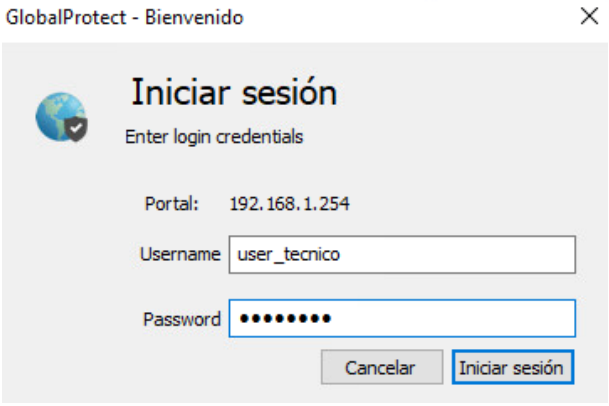


Figura 4-21 Inicio de sesión en el agente Global Protect

Si las credenciales son correctas, el agente indicará que está conectado a la red interna como muestra la Figura 4-22.

Figura 4-22 Mensaje de conexión exitosa a la red interna

Finalmente, de acuerdo a las políticas, únicamente el personal del departamento técnico puede realizar modificaciones en el agente, por lo que si el usuario quisiera cambiar sus privilegios el sistema le solicitará una contraseña de autorización como muestra la Figura 4-23.

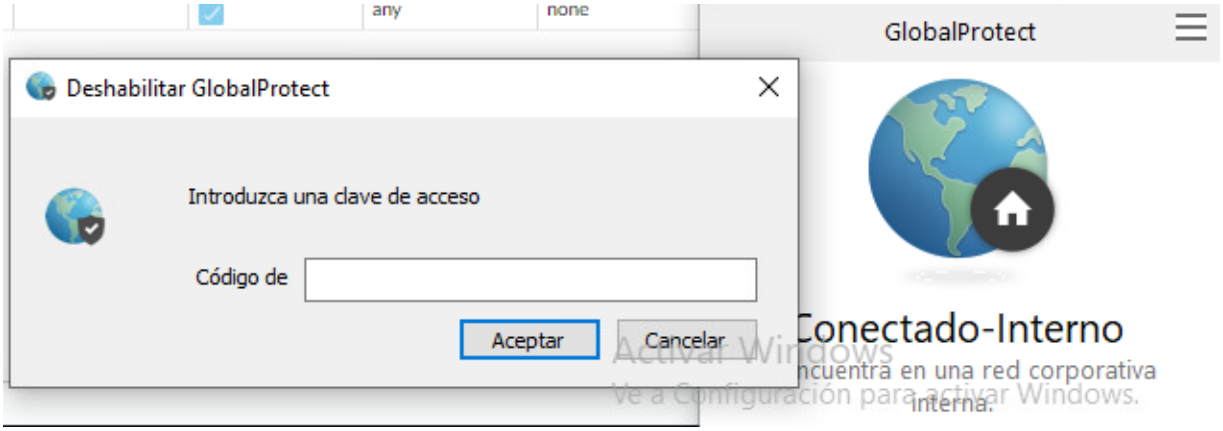


Figura 4-23 Solicitud de contraseña de autorización para modificar el agente

4.3.6 Configuración de VPN Client to Site para acceso remoto por teletrabajo

Para el acceso remoto de igual manera se requiere del agente Global Protect configurado mediante la interfaz que contiene la dirección IP pública a través de la cual los usuarios van a poder conectarse mediante un túnel IPSec VPN hacia la red interna, respetando los privilegios de acceso y de navegación que cada usuario dispone, como si estuviera conectado físicamente a la red. Estas configuraciones requieren de la creación de una interfaz VPN y una zona de seguridad como se muestra en la Figura 4-24.

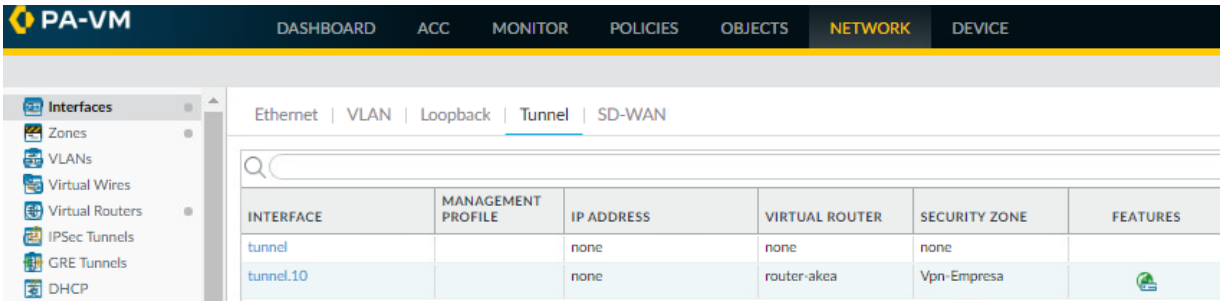


Figura 4-24 Creación de interfaz y zona de seguridad VPN

Al igual que la configuración de Gateway interno, para las conexiones de VPN client to site requiere de la configuración de un portal y de un Gateway. La diferencia principal es en la configuración de un túnel IPSec y las configuraciones de red de los clientes VPN como se muestra en las Figura 4-25 y Figura 4-26.

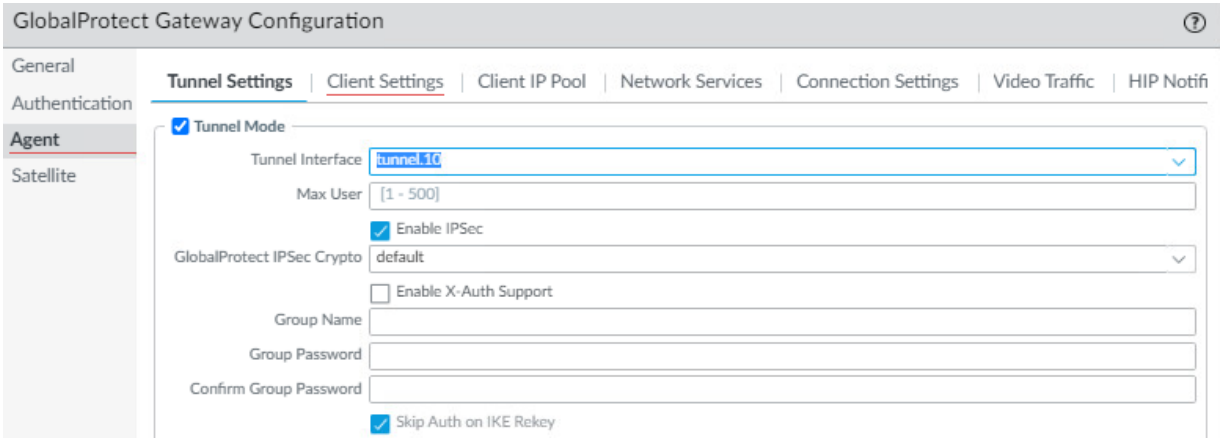


Figura 4-25 Configuración de túnel IPSec

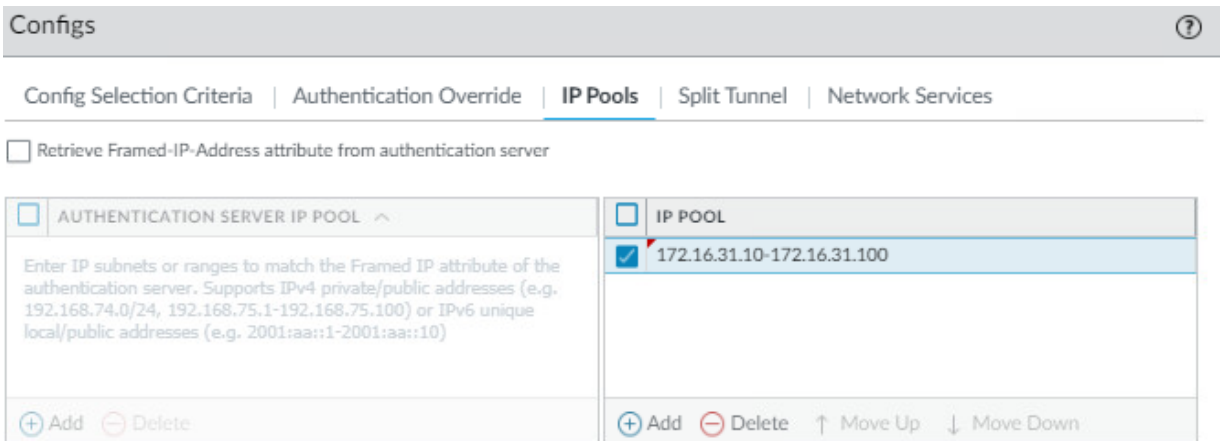


Figura 4-26 Configuración de pool de direcciones IP para clientes VPN

Para que los clientes se conecten a través de Internet, al igual que en el Gateway interno, en el navegador deben ingresar la dirección IP de la interfaz configurada como Gateway externo, y

así seguir el proceso de descarga del agente. Una vez descargado, el agente solicitará las credenciales de acceso que son las configuradas como usuarios locales, y permitirá el acceso y la navegación de acuerdo a los privilegios de cada usuario.

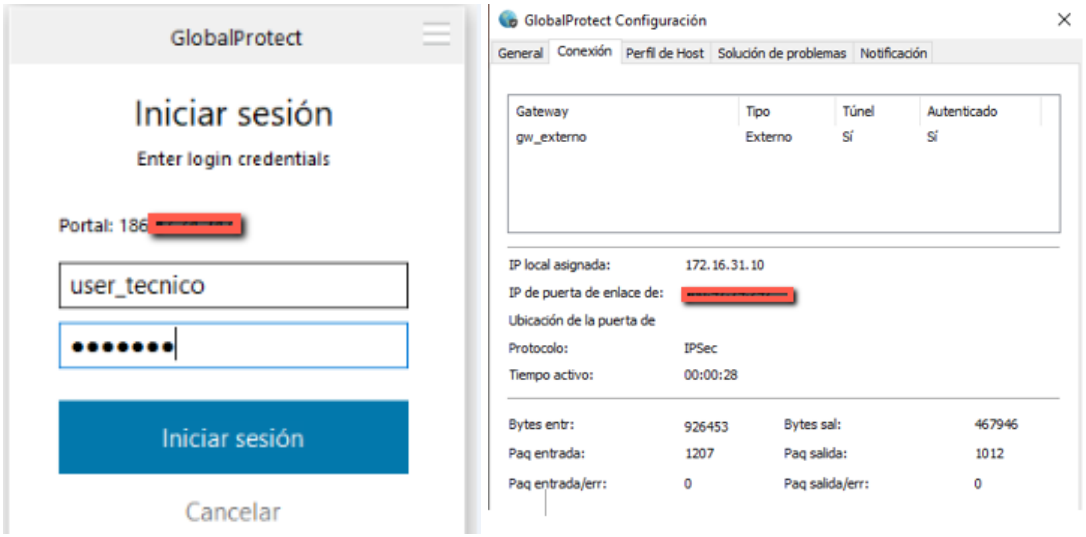


Figura 4-27 Parámetros de conexión del agente Global Protect externo

A diferencia del agente interno, los usuarios pueden deshabilitar el agente de Global Protect cuando lo deseen, ya que se considera que no deben estar conectados a la red interna en todo momento, sino solo cuando sea necesario. La Figura 4-28 muestra que únicamente para la desinstalación del agente se requiere una contraseña.

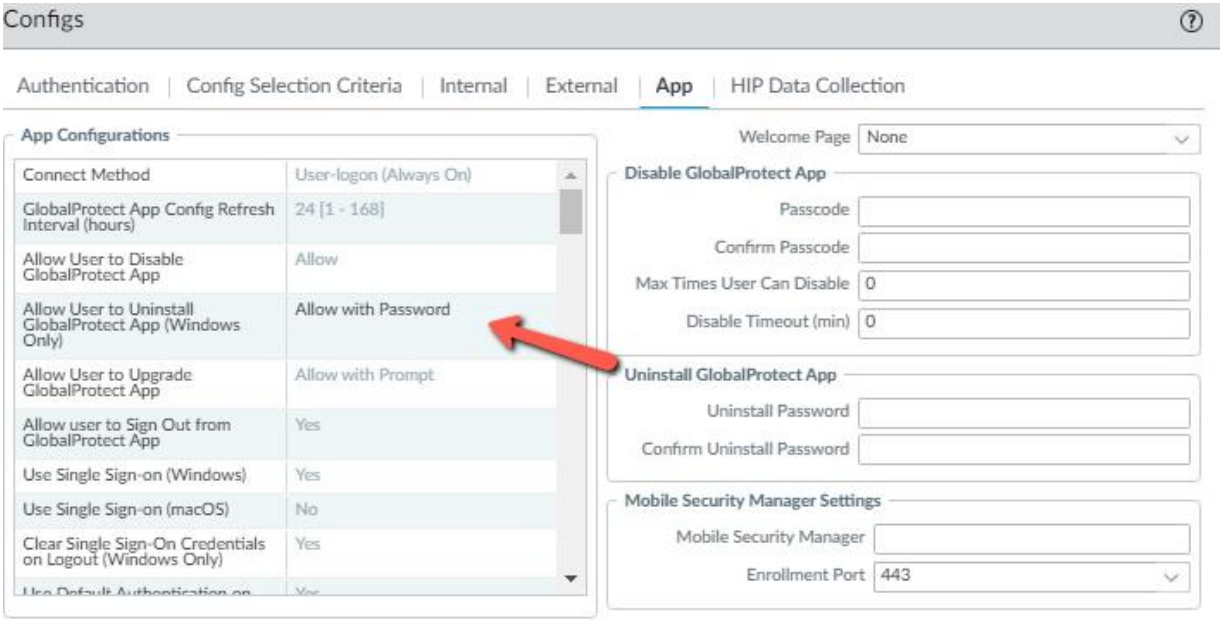


Figura 4-28 Configuración del agente Global Protect externo

4.4 CONFIGURACIÓN DE PERFILES DE SEGURIDAD

La definición de perfiles de seguridad permite realizar el análisis de vulnerabilidades, virus, exploits, o cualquier tipo de ataque al momento de que el trafico cruza el dispositivo de seguridad, este análisis se lo realiza antes de que el tráfico llegue a los dispositivos finales, por lo que, si alguna amenaza quisiera atravesar a red, esta será bloqueada de acuerdo a los perfiles de seguridad configurados, mitigando de esta forma el ciberataque.

Palo Alto Networks tiene predefinido algunos perfiles de seguridad por defecto que no son modificables, sin embargo, es importante realizar el análisis de cada uno de ellos para que se acoplen a las políticas de seguridad de cada empresa y poder alcanzar el objetivo que es reducir al máximo las amenazas cibernéticas. Los perfiles de seguridad se aplican a cada política con acción "permitir" sea política de acceso o de navegación.

4.4.1 Antivirus

El perfil de seguridad de Antivirus permite detectar y evitar que los virus, malware o ransomware se transfieran a través de siete protocolos: FTP, HTTP, HTTP2, IMAP, POP3, SMB y SMTP (Palo Alto Networks, 2020c). La Figura 4-29 muestra las acciones recomendadas que se debe configurar para detectar una amenaza dentro de los protocolos mencionados.

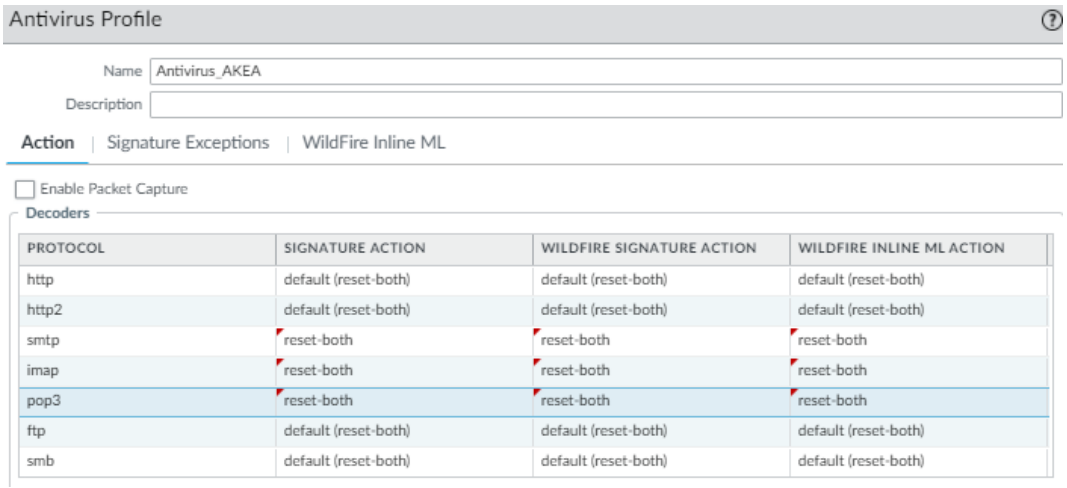


Figura 4-29 Perfil de Antivirus

El correo electrónico es una de las aplicaciones más utilizadas para la propagación de virus y malware, es por esto que se considera un perfil estricto de reseteo tanto de la conexión del cliente como del servidor, al momento de detectar una amenaza por medio de estos protocolos.

4.4.2 Anti-Spyware

El perfil de seguridad de Anti-Spyware permite detectar el tráfico de comando y control iniciado por un código malicioso que se ejecuta en un servidor o punto final y evitar que los sistemas comprometidos establezcan una conexión saliente desde la red interna (Palo Alto Networks, 2020c). La Figura 4-30 muestra las configuraciones de este perfil además, es recomendable habilitar la captura de paquetes (PCAP) para las amenazas consideradas críticas, altas o medias para facilitar el análisis y determinar los dispositivos que estén comprometidos.

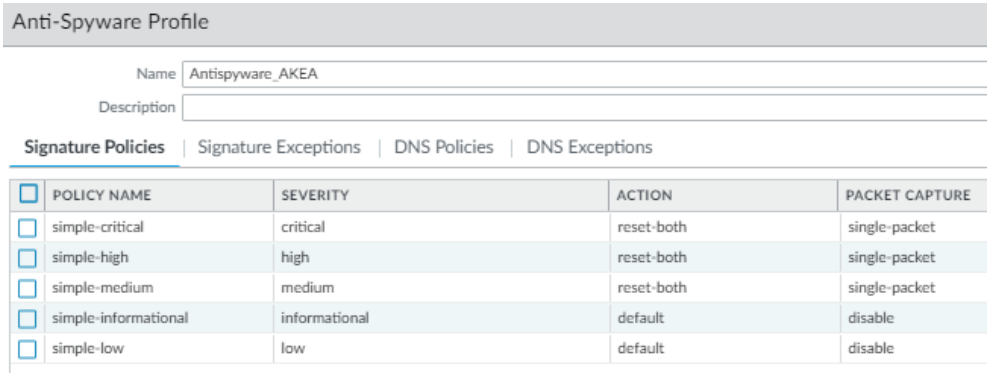


Figura 4-30 Perfil de Anti-Spyware

La configuración DNS sinkhole permite identificar dispositivos potencialmente comprometidos que intentan acceder a dominios sospechosos. Esta acción permite mantener una protección óptima y proporciona un mecanismo para ayudar a identificar los dispositivos comprometidos.

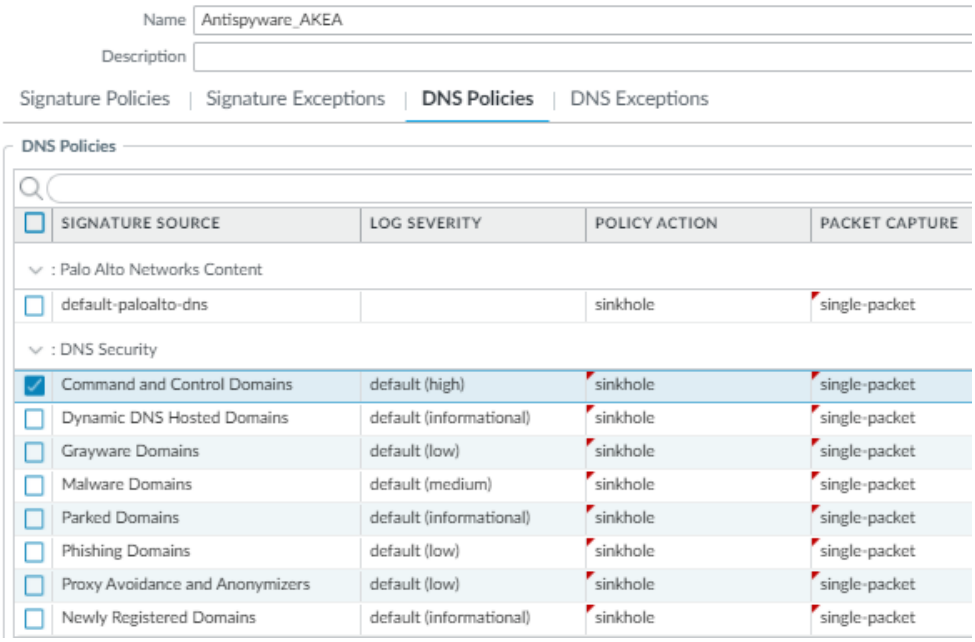
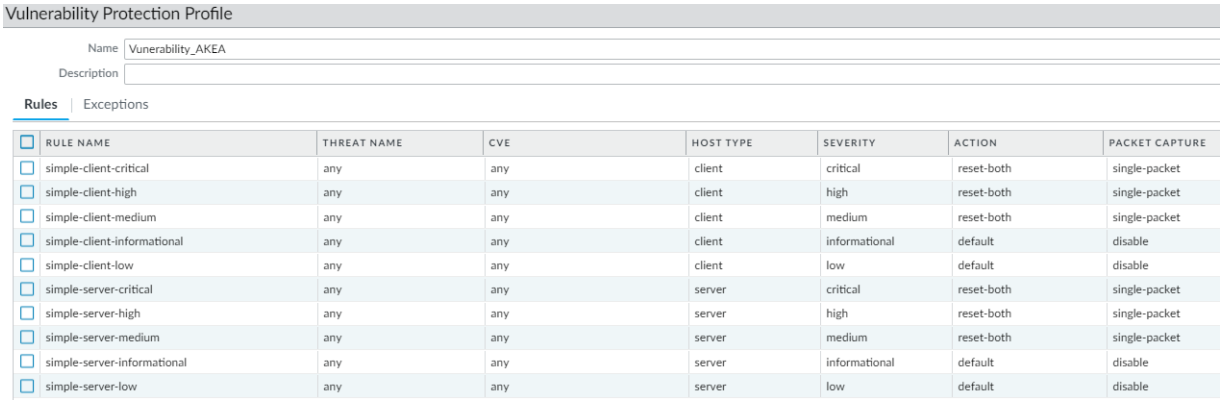


Figura 4-31 Políticas de DNS

4.4.3 Vulnerability Protection

Este perfil permite proteger la red contra ataques de desbordamientos de búfer, ejecución ilegal de código y otros exploits que aprovechan las vulnerabilidades del lado del cliente y del servidor. Este perfil también evita que un atacante use vulnerabilidades en los dispositivos internos para moverse lateralmente dentro de la red (Palo Alto Networks, 2020c).

El perfil estricto que viene predefinido en Palo Alto Networks tiene las acciones necesarias para cada nivel de amenaza. La Figura 4-32 muestra las configuraciones de este perfil, y de igual manera que el perfil anterior, se recomienda habilitar la captura de paquetes para el análisis y localización de las posibles fuentes del ataque.



RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
simple-client-critical	any	any	client	critical	reset-both	single-packet
simple-client-high	any	any	client	high	reset-both	single-packet
simple-client-medium	any	any	client	medium	reset-both	single-packet
simple-client-informational	any	any	client	informational	default	disable
simple-client-low	any	any	client	low	default	disable
simple-server-critical	any	any	server	critical	reset-both	single-packet
simple-server-high	any	any	server	high	reset-both	single-packet
simple-server-medium	any	any	server	medium	reset-both	single-packet
simple-server-informational	any	any	server	informational	default	disable
simple-server-low	any	any	server	low	default	disable

Figura 4-32 Perfil Vulnerability Protection

4.4.4 File Blocking

El perfil de seguridad File Blocking permite bloquear archivos que se incluyen comúnmente en campañas de ataque de malware y que no tienen un caso de uso real para la carga / descarga. El bloqueo de estos archivos reduce la superficie de ataque. Palo Alto Networks cuenta con un perfil estricto predefinido el cual bloquea archivos por lotes, DLL, archivos de clase Java, archivos de ayuda, accesos directos de Windows (.lnk), archivos BitTorrent, archivos .rar, archivos .tar, archivos rar cifrados y zip cifrados, archivos codificados de varios niveles (comprimidos hasta cuatro veces), archivos .hta y archivos Windows Portable Executable (PE), que incluyen .exe, .cpl, .dll, .ocx, .sys, .scr, .drv, .efi,. fon y archivos .pif. El perfil estricto predefinido alerta sobre todos los demás tipos de archivos para obtener visibilidad de otras transferencias de archivos para que pueda determinar si necesita realizar cambios en la política (Palo Alto Networks, 2020c).

Para este caso se utiliza dos perfiles. Un perfil general estricto para toda la empresa y un perfil que permita archivos de instalación de software que únicamente el departamento técnico debe tener acceso según se define en las políticas de seguridad propuestas.

NAME	RULE NAME	APPLICATIO...	FILE TYPES	DIRECTION	ACTION
FileBlocking_AKEA	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
	Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
	Log all other file types	any	any	both	alert
FileBlocking_Dpto_Tecnico	Block all risky file types	any	bat, cab, chm, class, cpl, dll, flash, hlp, hta, jar, Multi-Level-Encoding, ocx, pif, scr, torrent, vbe, wsf	both	block
	Block encrypted files	any	encrypted-rar, encrypted-zip	both	alert
	Log all other file types	any	any	both	alert

Figura 4-33 Perfil File Blocking

4.4.5 Wildfire Analysis

Los perfiles de seguridad anteriormente configurados, permiten reducir la superficie de ataque para amenazas conocidas, sin embargo, las amenazas desconocidas son cada vez más sofisticadas y a menudo pasan desapercibidas hasta mucho después de un ataque exitoso. Para protegerse de amenazas desconocidas, es necesario reenviar los archivos que circulan por la red en ambas direcciones a WildFire para su análisis (Palo Alto Networks, 2020c).

La Figura 4-34 muestra la configuración de este perfil, y se identifica que el análisis se lo realizará en la nube de WildFire, lo que permite hacer un análisis a nivel de machine learning, comportamiento y bare-metal.

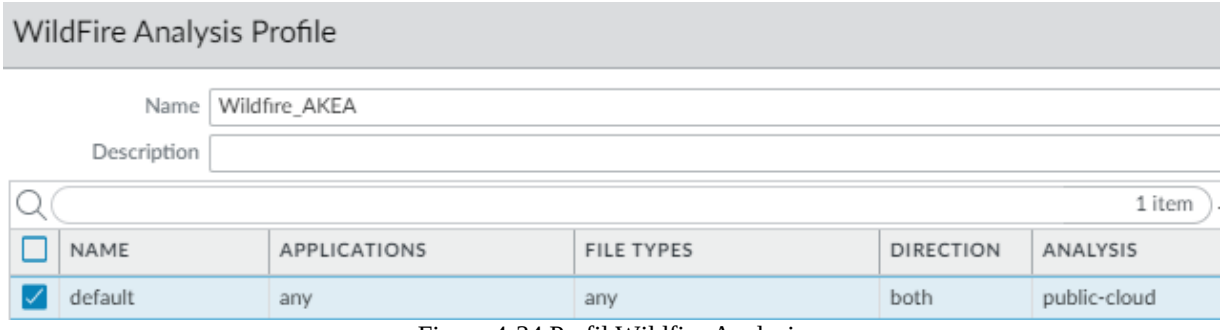


Figura 4-34 Perfil Wildfire Analysis

4.4.6 URL-Filtering

El perfil de URL-Filtering evita el acceso a contenido web de alto riesgo albergando malware o contenido de explotación. Palo Alto Networks recomienda el bloqueo todas las categorías de

URL peligrosas que incluyen comando y control, infracción de derechos de autor, DNS dinámico, extremismo, malware, phishing, proxy-avoidance-and-anonymizers, desconocido, dominio recién registrado, hacking, grayware y parked. El no bloquear estas categorías peligrosas pone en riesgo de infiltración de exploits, descarga de malware, actividad de comando y control y exfiltración de datos (Palo Alto Networks, 2020c).

Además de las categorías bloqueadas por seguridad, este perfil permite el bloqueo de contenido web dependiendo de las políticas de seguridad de la empresa. Por lo cual se genera 4 perfiles de seguridad de URL-Filtering según indica la Tabla 4-5:

Tabla 4-5 Descripción de perfiles de URL-Filtering

PERFIL URL	DETALLES
URL_Filtering_Gerencias	Bloquea todo lo recomendado por fábrica por seguridad Bloquea contenido adulto y de desnudez Permite todas las demás categorías
URL_Filtering_Dpto_Técnico	Bloquea todo lo recomendado por fábrica por seguridad Bloquea contenido adulto y de desnudez Permite todas las demás categorías
URL_Filtering_Dpto_Comercial	Bloquea todo lo recomendado por fábrica por seguridad Bloquea contenido adulto y de desnudez Boquea contenido de juegos, deportes y citas Bloquea contenido de streaming media Permite todas las demás categorías
URL_Filtering_AKEA	Bloquea todo lo recomendado por fábrica por seguridad Bloquea contenido adulto y de desnudez Boquea contenido de juegos, deportes y citas Bloquea contenido de multimedia y streaming Bloquea contenido de redes sociales y blogs Permite todas las demás categorías

La Figura 4-35 muestra la configuración de los perfiles de URL-Filtering de acuerdo a las políticas de seguridad propuestas.

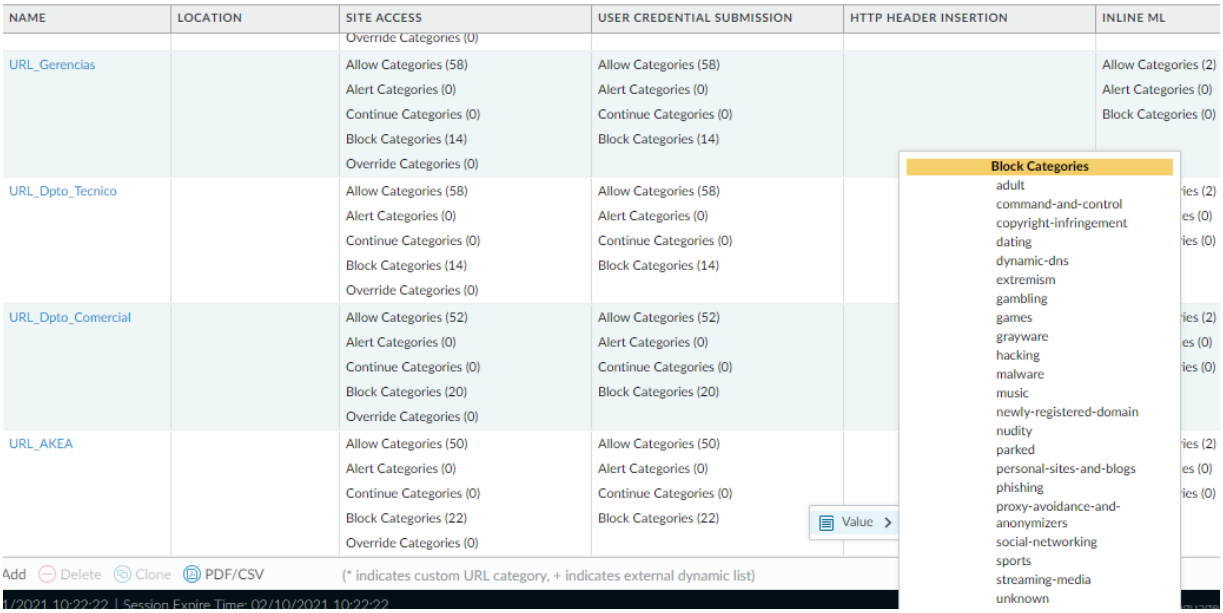


Figura 4-35 Perfiles de URL-Filtering

4.4.7 Application Filter

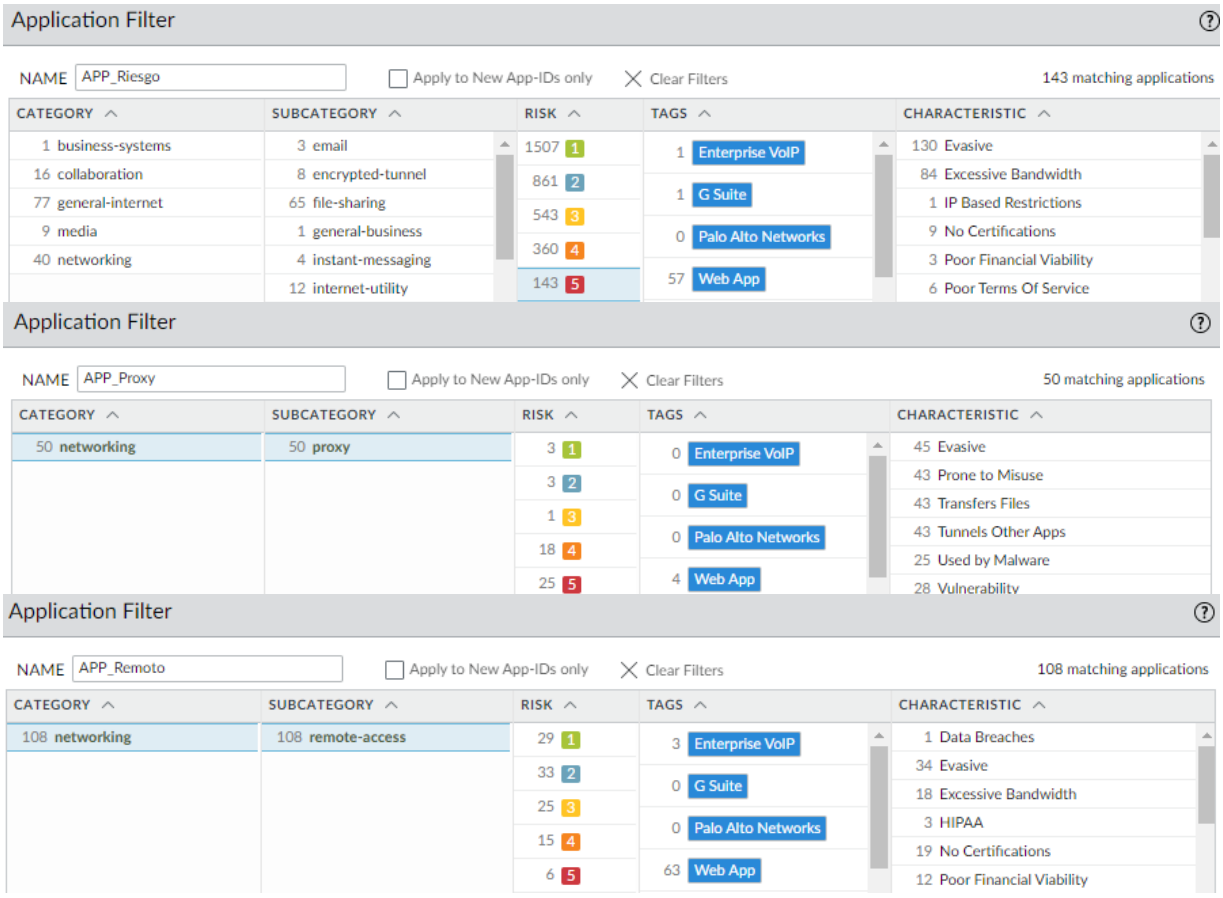
Application Filter permite la agrupación dinámica de aplicaciones basada en atributos como su categoría, tecnología o riesgo. De esta manera se puede controlar a que aplicaciones pueden acceder los usuarios y que aplicaciones el sistema de seguridad perimetral debe bloquear. En este caso, se considera siete filtros detallados en la Tabla 4-6:

Tabla 4-6 Descripción de los filtros de Aplicaciones dinámicas

APP-FILTER	DETALLES
APP_Riesgo	Al momento Palo Alto Networks registra 143 aplicaciones con categoría de alto riesgo. Se recomienda bloquear estas aplicaciones.
APP_Proxy	Al momento Palo Alto Networks registra 50 aplicaciones con funcionalidades de proxy, lo que puede inhabilitar las políticas de seguridad de la empresa. Se recomienda bloquear estas aplicaciones.
APP_Remoto	Al momento Palo Alto Networks registra 108 aplicaciones para acceso remoto. Se recomienda bloquear estas aplicaciones.
APP_ FileShare	Al momento Palo Alto Networks registra 351 aplicaciones para compartición de archivos, por política de seguridad, únicamente se debe utilizar los medios oficiales para la compartición de archivos. Se recomienda bloquear estas aplicaciones.

APP_Update	Al momento Palo Alto Networks registra 35 aplicaciones para actualizaciones de software. Se recomienda realizar un control de ancho de banda para estas aplicaciones.
APP_Multimedia	Al momento Palo Alto Networks registra 325 aplicaciones para multimedia. Se recomienda bloquear estas aplicaciones y conceder el acceso únicamente a los grupos que tengan la autorización de gerencia.
APP_Social_Networking	Al momento Palo Alto Networks registra 332 aplicaciones para multimedia. Se recomienda bloquear estas aplicaciones y conceder el acceso únicamente a los grupos que tengan la autorización de gerencia.

La Figura 4-36 muestra la configuración de cada uno de los filtros mencionados anteriormente, que van a ser utilizados en las políticas de navegación.



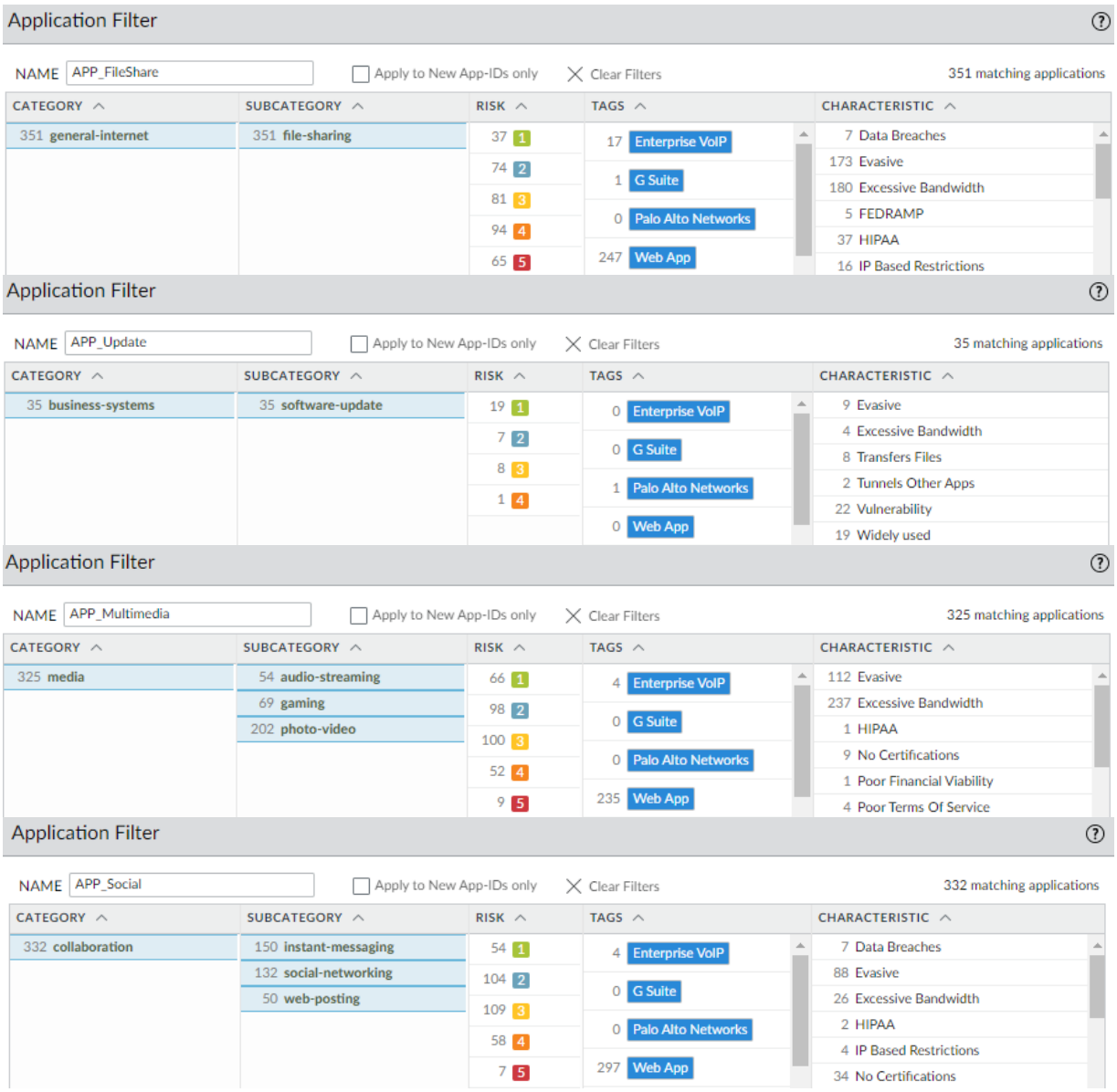


Figura 4-36 Configuración de filtros de aplicación dinámicas

4.5 CONFIGURACION DE POLÍTICAS DE ACCESO

Estas políticas definen los permisos de acceso que cada usuario o grupo de usuario debe tener a los servicios de la empresa, dependiendo de los privilegios definidos por gerencia. Estas políticas son secuenciales, es decir, dejará de analizar las demás políticas y procesará el tráfico de acuerdo la primera política que encuentre coincidencia. Hay que considerar que se debe aplicar los perfiles de seguridad en cada política con acción “permitir”.

4.5.1 Acceso al servicio de Global Protect Interno

Para poder hacer el control a nivel de usuarios, es necesario tener acceso a la dirección IP a través de la cual Global Protect actúa como Gateway interno. Este servicio se ofrece a través de la zona de seguridad de Administración, por lo que es necesario generar una política entre la zona de User_Empresa, Vpn_Empresa, Wireless_Empresa y la zona de Administración únicamente para la dirección IP del Gateway de Global Protect en con la aplicación web-browsing. La Figura 4-37 muestra la configuración de esta política incluyendo los perfiles de seguridad de Antivirus, Antispyware, Vulnerability Protection y Wildfire Analysis

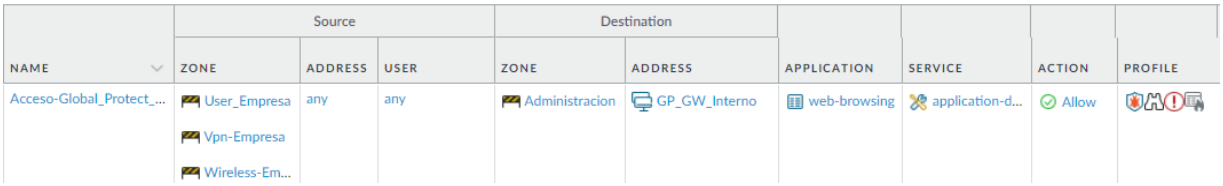


Figura 4-37 Política de acceso al Gateway interno de Global Protect

4.5.2 Acceso a la administración de dispositivos de red y servidores

De acuerdo a las políticas de seguridad propuestas, solo el personal del departamento técnico debe tener acceso a la gestión y configuración de dispositivos de red y la granja de servidores, por lo tanto, se genera una política de acceso para permitir estas conexiones. La Figura 4-38 muestra la política configurada para los permisos entre la zona de User_Empresa, Vpn_Empresa, Wireless_Empresa, el grupo de usuario Departamento_Tecnico y las zonas Administracion, Servers_Desarrollo, Servers_Dmz, Servers_Internos y Telefonía con los perfiles de seguridad de Antivirus, Antispyware, Vulnerability Protection y Wildfire Analysis.

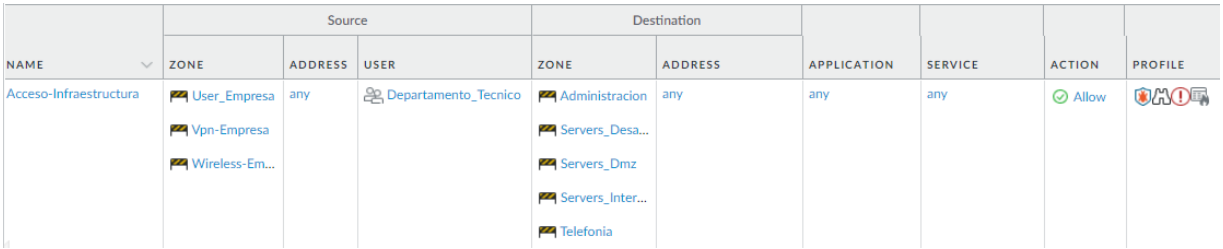


Figura 4-38 Política de acceso a la administración de dispositivos de red

Adicionalmente, se recomienda la creación de usuarios de administración para cada dispositivo de red, con el fin de mantener un registro por usuario de los cambios que se realicen a nivel de las configuraciones de los dispositivos.

Como ejemplo se realiza la configuración de usuarios administradores para el acceso a las configuraciones y monitoreo a través de la interfaz de management de Palo Alto Networks. Estos usuarios son los mismos que forman parte de la base de datos locales del grupo de Departamento_Tecnico. La Figura 4-39 muestra la configuración del perfil de autenticación para usuarios de administración del dispositivo PA-220 y la Figura 4-40 muestra la aplicación de este perfil en la creación de usuarios administradores.

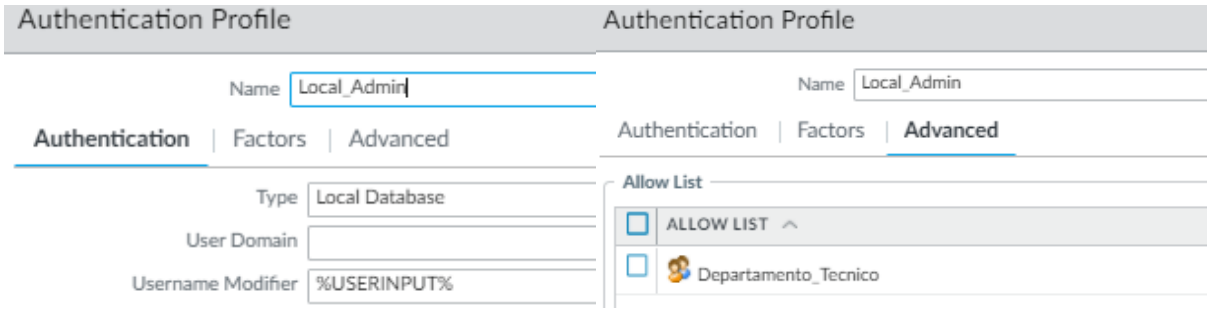


Figura 4-39 Perfil de autenticación de usuarios administradores del PA-220

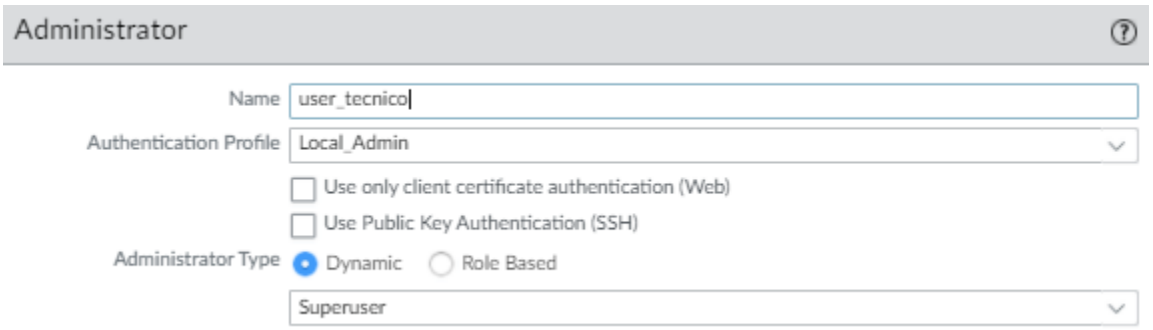


Figura 4-40 Usuario administrador con perfil de autenticación Local_Admin

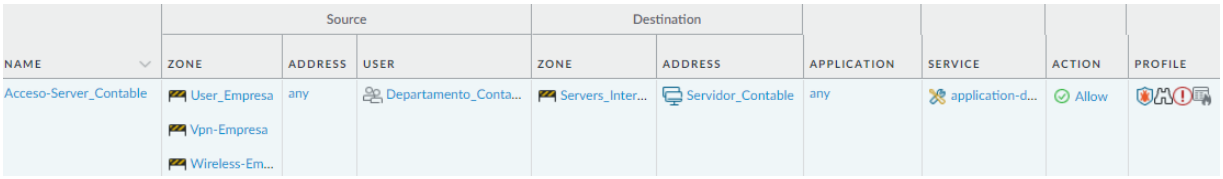
De esta manera se registra la actividad que realice el usuario en el equipamiento de seguridad perimetral como se muestra en la Figura 4-41.

RECEIVE TIME	ADMINISTRAT...	HOST	CLIENT	COMMA...	RESULT	CONFIGURATION PATH	FULL PATH	BEFORE CHANGE	AFTER CHANGE
01/15 07:13:58	user_tecnico	181.175.230....	Web	commit	Submitted				
01/15 07:13:32	user_tecnico	181.175.230....	Web	edit	Succeed...	vsys vsys1 rulebase security rules Acceso-Server_Repositorio service	/config/devices/... Server_Reposito...	service [any];	service [application-default];
01/15 07:13:25	user_tecnico	181.175.230....	Web	edit	Succeed...	vsys vsys1 rulebase security rules Acceso-Server_Contable service	/config/devices/... Server_Contable'...	service [any];	service [application-default];
01/12 18:58:59	user_tecnico	181.175.230....	Web	commit	Submitted				
01/12 18:58:31	user_tecnico	181.175.230....	Web	rename	Succeed...	vsys vsys1 rulebase security rules Acceso-Repositorio	/config/devices/... Repositorio']	Acceso-Repositorio 42aac60f-763d-4d89-bb24-574255369d94	Acceso-Server_Reposito... 42aac60f-763d-4d89-bb24-574255369d94
01/12 18:58:31	user_tecnico	181.175.230....	Web	edit	Succeed...	vsys vsys1 rulebase security rules Acceso-Repositorio	/config/devices/... Repositorio']	Acceso-Repositorio 42aac60f-763d-4d89-bb24-574255369d94 [ ]	Acceso-Repositorio 42aac60f-763d-4d89-bb24-574255369d94 [

Figura 4-41 Registro de actividad del usuario administrador user_tenico

4.5.3 Acceso al sistema contable

De acuerdo a las políticas de seguridad propuestas, solo el personal del departamento de contabilidad y financiero tienen autorización de acceso al servicio contable, por lo tanto, se genera una política de acceso para permitir estas conexiones. La Figura 4-42 muestra la política configurada para los permisos entre la zona de User_Empresa, Vpn_Empresa, Wireless_Empresa, el grupo de usuario Departamento_Contable y la zona Server_Internos únicamente al Servidor_Contable, además se configura los perfiles de seguridad de Antivirus, Antispyware, Vulnerability Protection y Wildfire Analysis.

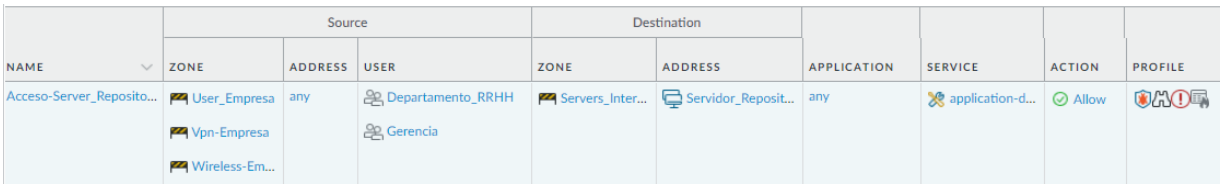


	Source			Destination					
NAME	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE
Acceso-Server_Contable	User_Empresa Vpn-Empresa Wireless-Em...	any	Departamento_Conta...	Servers_Inter...	Servidor_Contable	any	application-d...	Allow	

Figura 4-42 Política de acceso al servidor contable

4.5.4 Acceso al repositorio de información del personal de la empresa

De acuerdo a las políticas de seguridad propuestas, solo el personal del departamento de recursos humanos y gerencia tiene acceso a la documentación profesional del personal que labora en la empresa, así como de los proveedores y contratistas, información que se encuentra alojada en un repositorio en la granja de servidores internos. La Figura 4-43 muestra la política configurada para los permisos entre la zona de User_Empresa, Vpn_Empresa, Wireless_Empresa, el grupo de usuario Departamento_RRHH y Gerencia, y la zona Server_Internos únicamente al Servidor_Repositorio, además se configura los perfiles de seguridad de Antivirus, Antispyware, Vulnerability Protection y Wildfire Analysis.



	Source			Destination					
NAME	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE
Acceso-Server_Reposito...	User_Empresa Vpn-Empresa Wireless-Em...	any	Departamento_RRHH Gerencia	Servers_Inter...	Servidor_Reposit...	any	application-d...	Allow	

Figura 4-43 Política de acceso al servidor de repositorio de información

4.5.5 Acceso al servicio de impresión

De acuerdo a las políticas de seguridad propuestas, el acceso a los recursos de la empresa, como es el servicio de impresión, es exclusivo del personal que labora en la misma. La Figura 4-44 muestra la política configurada para los permisos entre la zona de User_Empresa,

Vpn_Empresa, Wireless_Empresa, que incluye todos los departamentos y el personal que labora en la empresa, y la zona Impresión; además se configura los perfiles de seguridad de Antivirus, Antispyware, Vulnerability Protection y Wildfire Analysis.

NAME	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE
Acceso-Impresion	User_Empresa Vpn-Empresa Wireless-Em...	any	any	Impresion	any	any	any	Allow	

Figura 4-44 Política de acceso al servicio de impresión

4.6 CONFIGURACION DE POLÍTICAS DE NAVEGACIÓN

Las políticas de navegación están definidas según las políticas de seguridad propuestas. Actualmente las políticas de seguridad no indican restricciones de ningún tipo para la navegación en Internet. Sin embargo, se recomienda las siguientes políticas de navegación para asegurar que los recursos de la empresa sean utilizados con fines acorde al giro de negocio.

4.6.1 Políticas de control de ancho de banda

La información de la empresa debe ser respaldada frecuentemente, por lo que la empresa cuenta con el servicio de OneDrive de la plataforma de Microsoft Office365, sin embargo, la sincronización de estos archivos puede llegar a saturar el enlace de Internet, de igual manera puede suceder con las actualizaciones de sistemas operativos necesarias para la disminución de riesgos de explotación de vulnerabilidades por lo que, se debe configurar una política de calidad de servicio (QoS) para limitar el tráfico a 4Mbps en el horario laboral.

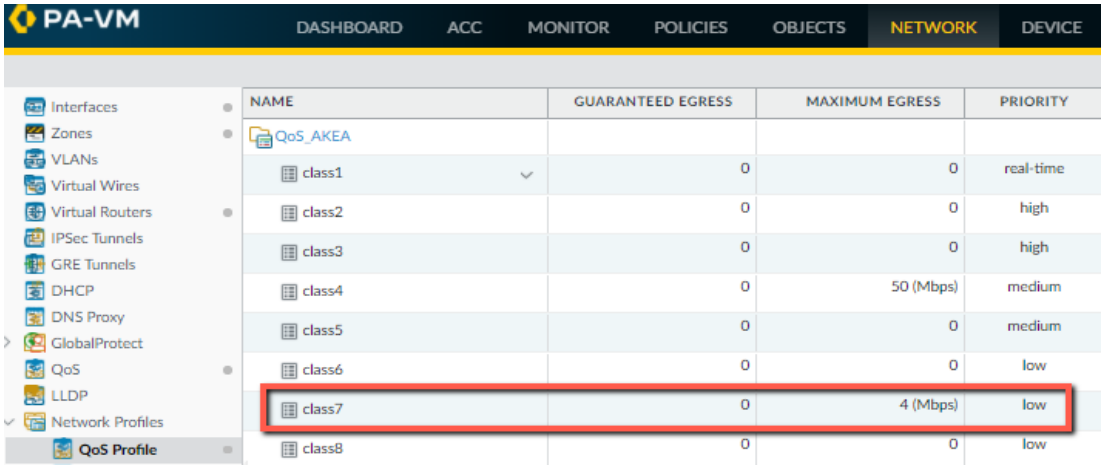


Figura 4-45 Perfil general de QoS

La Figura 4-45 muestra el perfil de QoS configurado, Palo Alto Networks maneja ocho clases para QoS. El tráfico general por defecto utiliza la clase 4, es por esto que se configura el ancho de banda total en esta clase. Además, se utiliza la clase 7 para la política de QoS de OneDrive y actualización de software, con 4Mbps según las políticas de seguridad propuestas.

El perfil de QoS se activa en la interfaz de salida a Internet, en este caso se configura únicamente para la interfaz ethernet 1/1 que es el enlace principal de la empresa.

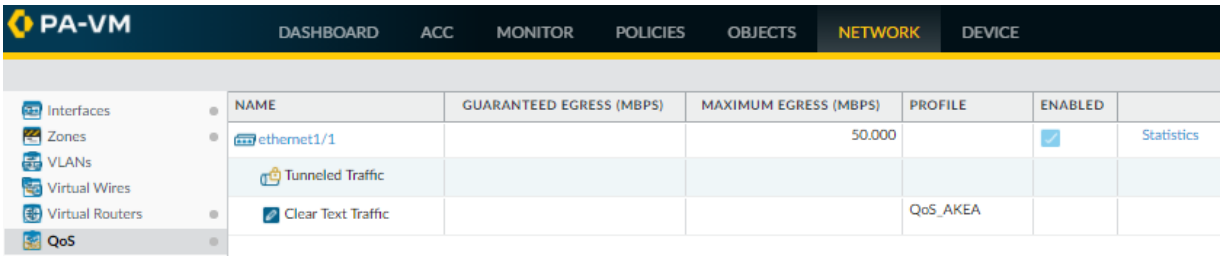


Figura 4-46 Aplicación de perfil QoS en la interfaz principal de Internet

De acuerdo a las políticas de seguridad propuestas, el perfil de QoS debe ser aplicado en horario laboral, por lo que se crea un horario de lunes a viernes de 8am.

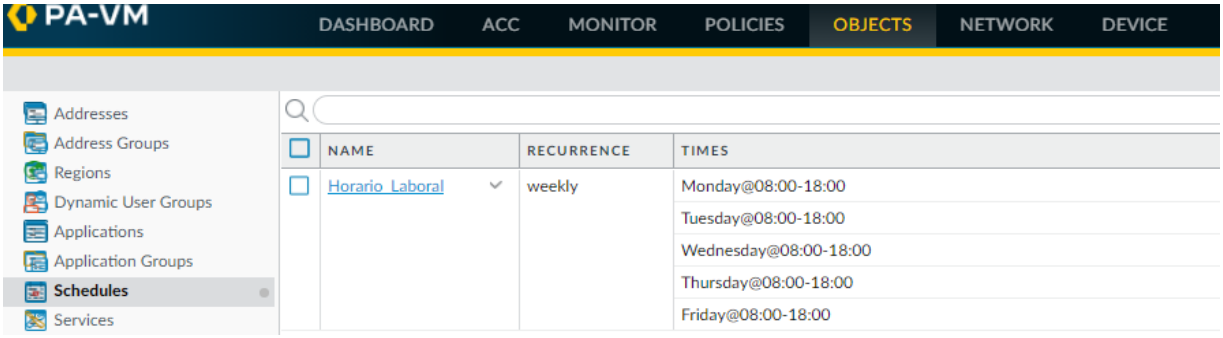


Figura 4-47 Creación de horario laboral

Se configura la política de QoS para Microsoft OneDrive y para las aplicaciones referentes a actualizaciones de software, esta política se aplica únicamente para los usuarios de la empresa, ya sea que se conecten a través de la red interna o a través de la VPN.

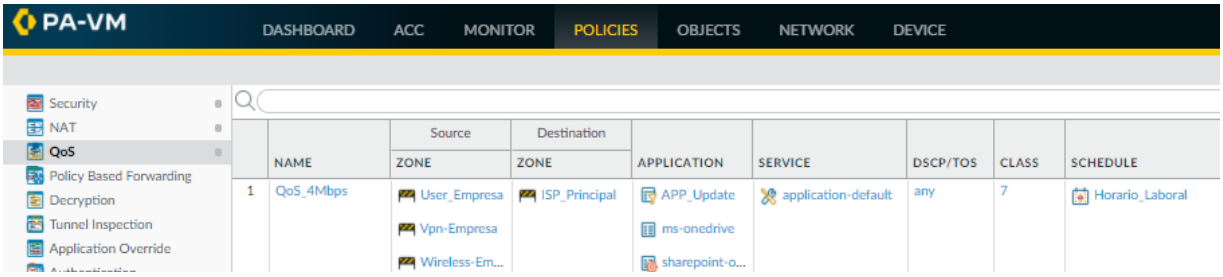


Figura 4-48 Política de QoS para 4Mbps

Finalmente, la Figura 4-49 muestra la configuración de la política de seguridad para estas aplicaciones, autorizando el trafico únicamente a los usuarios de la empresa, con los perfiles de seguridad de Antivirus, Antispyware, Vulnerability Protection y Wildfire Analysis.

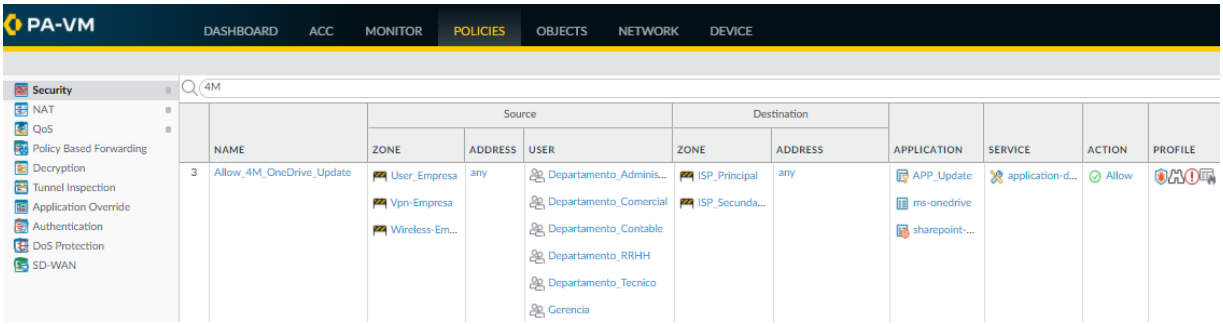


Figura 4-49 Política de seguridad para Microsoft OneDrive y Actualizaciones controladas

4.6.2 Políticas de servicios publicados

Para la publicación de los servicios de manera segura, es necesario identificar que aplicaciones utilizan para dar acceso externo únicamente a estas aplicaciones.

En el caso de la empresa, cuenta con dos servicios publicados que son la mesa de ayuda y la página web, los cuales utilizan la aplicación de web-browsing por los puertos 80 y 8080. La política de seguridad trabaja en conjunto con la política de DNAT creada anteriormente.

La Figura 4-50 muestra la configuración de la política de seguridad para controlar el acceso a los servicios publicados, además se aplican los perfiles de seguridad Antivirus, Antispyware, Vulnerability Protection y Wildfire Analysis.

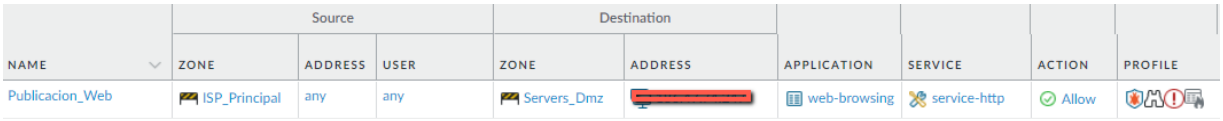


Figura 4-50 Política de seguridad para Publicación de Servicios Web

4.6.3 Políticas de bloqueo general

Se recomienda el bloque de ciertas aplicaciones que se consideran de alto riesgo y aquellas aplicaciones que permiten saltar las políticas de seguridad con la creación de túneles con aplicaciones de terceros, estas aplicaciones son conocidas como aplicaciones proxy. La Figura 4-51 muestra la configuración de la política de seguridad para el bloqueo de estas aplicaciones las cuales fueron definidas en los perfiles de seguridad como Application Filter.

NAME	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE
Block_APP_Riesgo	any	any	any	ISP_Principal ISP_Secundario	any	APP_Proxy APP_Riesgo	application-d...	Drop	none

Figura 4-51 Política de seguridad para bloqueo de aplicaciones de riesgo alto

Los usuarios solo tienen permitido el acceso a Microsoft OneDrive como repositorio y compartición de archivos, por lo tanto, se debe bloquear el acceso a cualquier otro repositorio como MegaUpload, GooglDrive, Dropbox entre otros. La Figura 4-52 muestra la política de seguridad configurada para cumplir con este requerimiento.

NAME	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION
Block_APP_FileShare	any	any	any	ISP_Principal ISP_Secundario	any	APP_FileSha...	application-d...	Drop

Figura 4-52 Política de seguridad para bloqueo de aplicaciones repositorio en la nube

Además, se considera el bloqueo de ciertas aplicaciones de acuerdo a las políticas de seguridad propuestas como son las aplicaciones de acceso remoto.

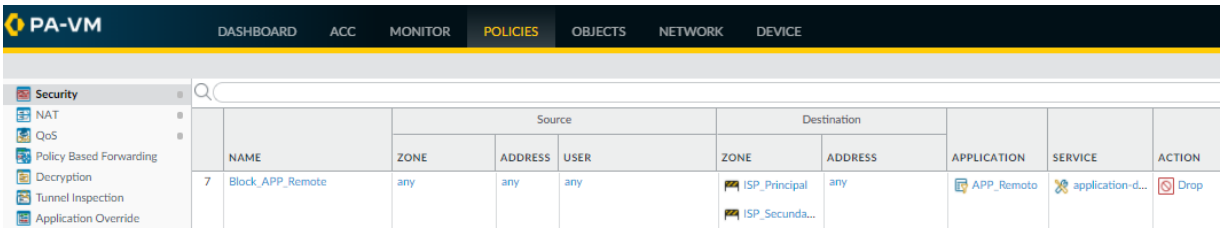


Figura 4-53 Política de seguridad para bloqueo de aplicaciones acceso remoto

Finalmente, se definen políticas de bloqueo para ciertas aplicaciones que no tienen relación con el giro de negocio y consumen recursos de la empresa, a las cuales se dará acceso únicamente bajo autorización de gerencia. La Figura 4-54 muestra las dos políticas de seguridad configuradas para cumplir con este requerimiento.

NAME	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION
Block_APP_Social_Netw...	any	any	any	ISP_Principal ISP_Secundario	any	APP_Social	application-d...	Drop
Block_APP_Multimedia	any	any	any	ISP_Principal ISP_Secundario	any	APP_Multim...	application-d...	Drop

Figura 4-54 Política de seguridad para bloqueo de multimedia y redes sociales

4.6.4 Políticas de navegación para los Servicios

Para la granja de servidores, la red de telefonía, la red de impresión y la red de administración se considera una navegación básica aplicando los bloqueos generales y los perfiles de seguridad de Antivirus, Antispyware, Vunerability Protection, File Blocking, Wildfire Analysis y el perfil de URL_Filtering URL_AKEA. La Figura 4-55 muestra la configuración de esta política.

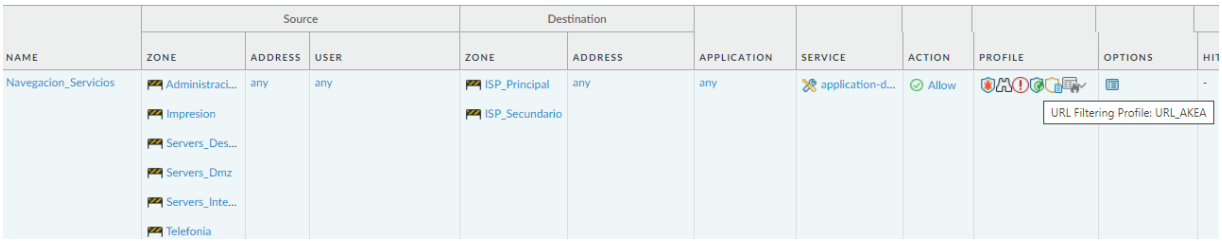


Figura 4-55 Política de seguridad para la navegación de las redes de servicio

4.6.5 Políticas de navegación para las Gerencias

Para los usuarios de Gerencia, se considera una navegación de perfil alto, se aplican los bloqueos generales a excepción de multimedia y de redes sociales, y se aplican los perfiles de seguridad de Antivirus, Antispyware, Vunerability Protection, File Blocking, Wildfire Analysis y el perfil de URL_Filtering URL_Gerencia. La Figura 4-56 y la Figura 4-57 muestran la configuración de estas políticas.

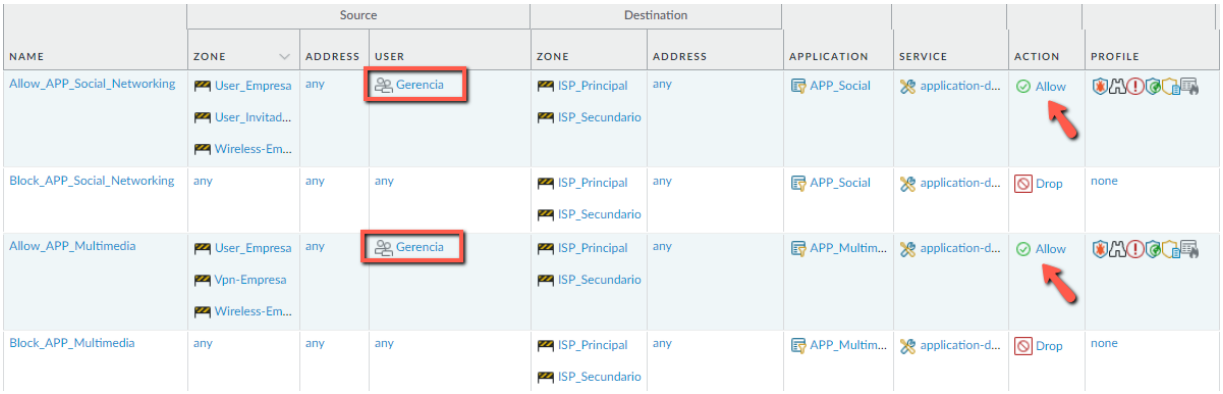


Figura 4-56 Política de seguridad para permitir multimedia y redes sociales a las Gerencias

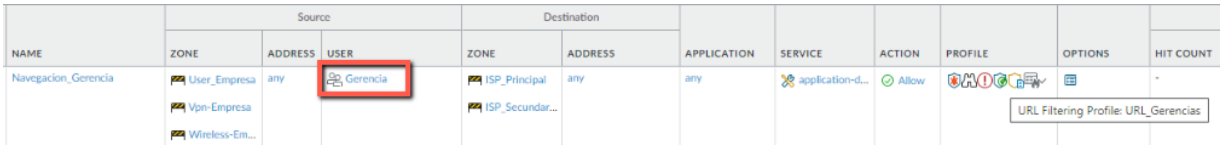


Figura 4-57 Política de seguridad para la navegación de usuarios de Gerencia

4.6.6 Políticas de navegación para el Departamento Técnico

Para los usuarios del Departamento Técnico, se considera una navegación de perfil alto, se aplican los bloqueos generales a excepción de multimedia y de redes sociales; y también se da acceso a las aplicaciones de acceso remoto. Además, se aplican los perfiles de seguridad de Antivirus, Antispyware, Vunerability Protection, Wildfire Analysis y los perfiles de URL_Filtering y File_Blocking propios del Departamento Técnico. La Figura 4-58 y la Figura 4-59 muestran la configuración de estas políticas.

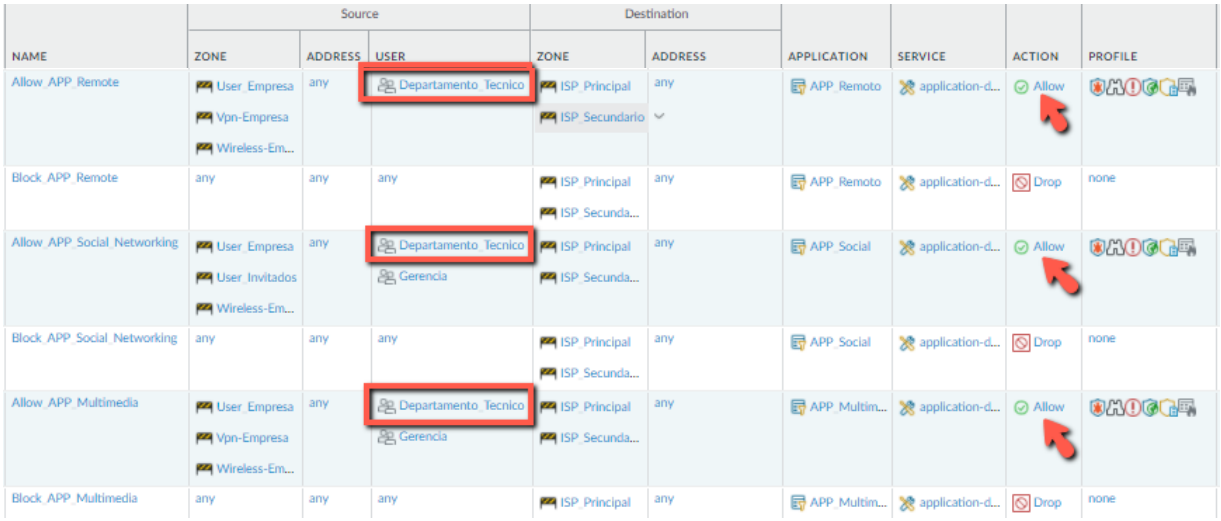


Figura 4-58 Política de seguridad para permitir acceso remoto, redes sociales y multimedia al Departamento Técnico

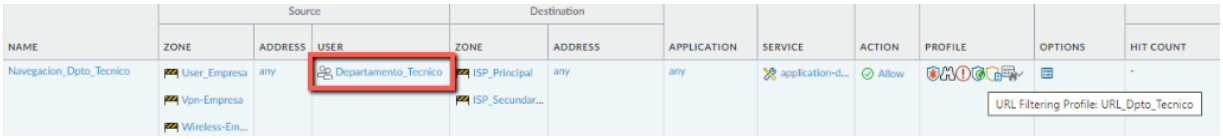


Figura 4-59 Política de seguridad para la navegación del Departamento Técnico

4.6.7 Políticas de navegación para el Departamento Comercial

Para los usuarios del departamento comercial, se considera una navegación de perfil medio, se aplican los bloqueos generales a excepción de redes sociales, por el contacto con los clientes. Se aplican los perfiles de seguridad de Antivirus, Antispyware, Vunerability Protection, File_Blocking, Wildfire Analysis y los perfiles de URL_Filtering propios del Departamento Comercial. La Figura 4-60 y la Figura 4-61 muestran la configuración de estas políticas.

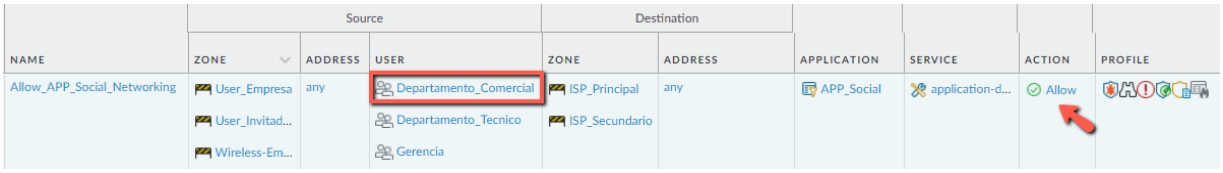


Figura 4-60 Política de seguridad para permitir redes sociales al Departamento Comercial

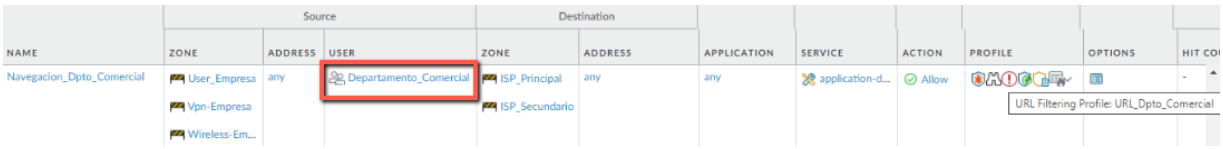


Figura 4-61 Política de seguridad para la navegación del Departamento Comercial

4.6.8 Políticas de navegación para los demás Departamentos

Para los usuarios de los demás departamentos, se considera una navegación de perfil bajo, se aplican los bloqueos generales y los perfiles de seguridad de Antivirus, Antispyware, Vunerability Protection, File_Blocking, Wildfire Analysis y los perfiles de URL_Filtering configurado como URL_AKEA. La Figura 4-62 muestran la configuración de estas políticas.

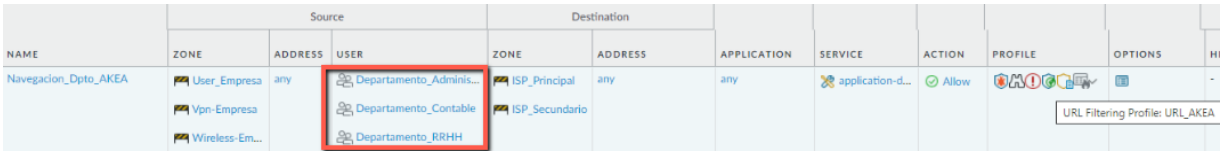


Figura 4-62 Política de seguridad para la navegación para los demás departamentos

4.6.9 Políticas de navegación para los Usuarios Invitados

Para los usuarios Invitados se considera una navegación de perfil bajo, se aplican los bloqueos generales y los perfiles de seguridad de Antivirus, Antispyware, Vunerability Protection, File_Blocking, Wildfire Analysis y los perfiles de URL_Filtering configurado como URL_AKEA. Además, se permite solo la navegación a través del ISP secundario. La Figura 4-63 muestran la configuración de estas políticas.

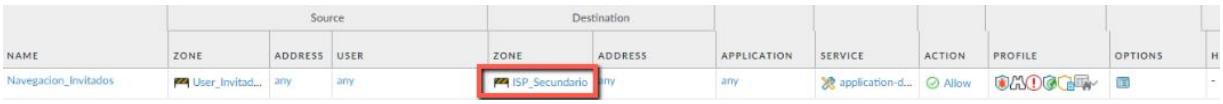


Figura 4-63 Política de seguridad para la navegación de usuarios invitados

4.6.10 Políticas de navegación por defecto

No se configura una política de navegación por defecto, es decir, si un usuario quiere navegar y no está declarado dentro de las redes empresariales, no podrá tener acceso a Internet. De esta manera se tendrá un control de uso de este recurso.

CAPÍTULO 5: EVALUACIÓN DE LA ARQUITECTURA Y POLÍTICAS DE SEGURIDAD.

Este capítulo se enfoca en la evaluación de la metodología de seguridad y las políticas de seguridad propuestas, mediante el uso de recursos virtuales para la simulación de la arquitectura empresarial y la generación de tráfico para el análisis.

Gracias a la facilidad que Palo Alto Networks presenta, es posible utilizar una de sus versiones virtuales conocidas como VM-Series para la configuración y simulación de la metodología de seguridad perimetral en un entorno de la nube.

Tomando en cuenta las limitantes de la virtualización y de los recursos en el gestor de la nube asignados para este laboratorio, se considera el siguiente esquema presentado en la Figura 5-1, para el análisis y evaluación.

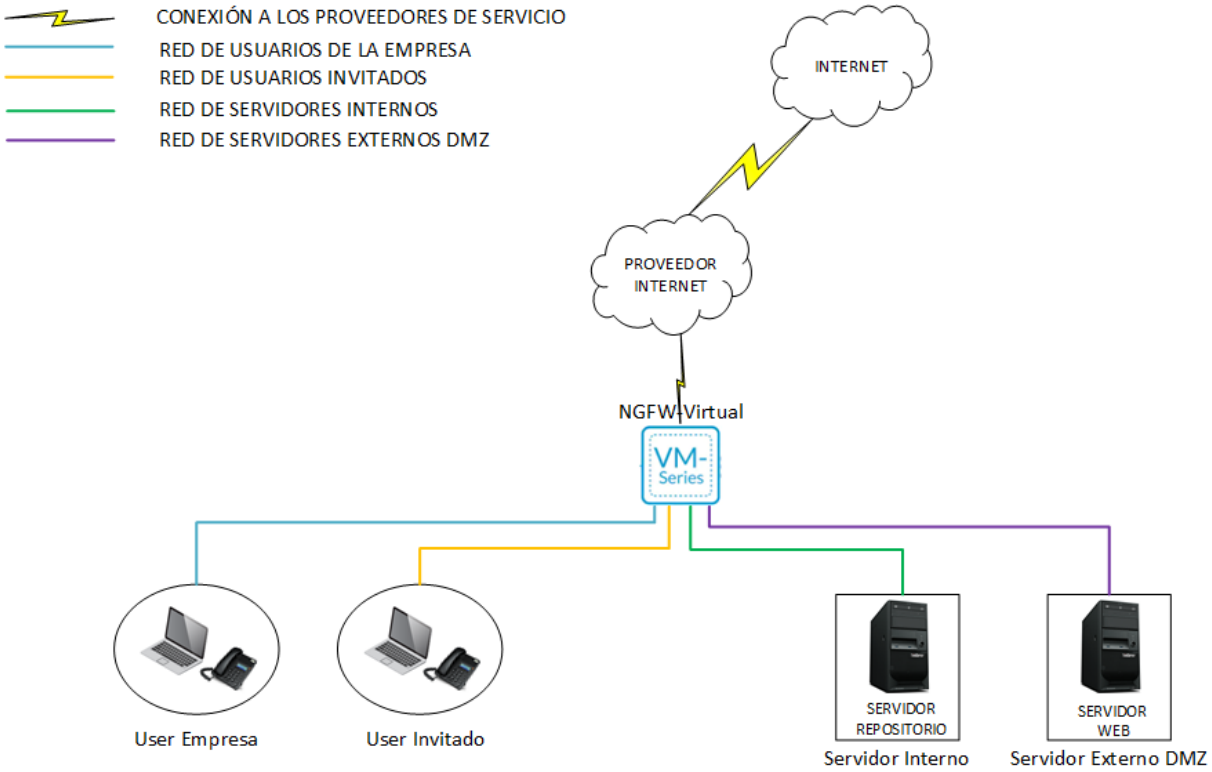


Figura 5-1 Esquema de conexión para la evaluación de políticas de seguridad

5.1 EVALUACIÓN DE LA METODOLOGÍA DE SEGURIDAD EN BASE A LAS MEJORES PRÁCTICAS DE CONFIGURACIÓN.

Palo Alto Networks, permite la importación de configuraciones de un dispositivo a otro, sea virtual o físico, mediante la exportación de un archivo html. Esto facilita las configuraciones en ambientes de laboratorio que posteriormente pueden ser utilizados ya con equipamiento físico.

Para la evaluación de las configuraciones de políticas en la metodología de seguridad perimetral, se considera el análisis de tráfico entre las diferentes zonas, tomando en cuenta que el ambiente virtual no permite presentar el esquema completo con todas las zonas e interfaces propuestas en la reestructuración de la arquitectura actual.

Se considera siete zonas para el laboratorio, las cuales se presenta en la Figura 5-2. Sin embargo, la aplicación de políticas de seguridad y de acceso son las propuestas en el capítulo anterior.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1	Layer3	Profile_GP		186.47.74.247/28	router-akea	Untagged	none	ISP_Principal
ethernet1/2	Layer3	Profile_GP		192.168.1.254/24	router-akea	Untagged	none	Administracion
ethernet1/3	Layer3			192.168.2.254/24	router-akea	Untagged	none	User_Empresa
ethernet1/4	Layer3			192.168.6.254/24	router-akea	Untagged	none	Servers_Internos
ethernet1/5	Layer3			192.168.7.254/24	router-akea	Untagged	none	Servers_Dmz
ethernet1/6	Layer3			192.168.8.254/24	router-akea	Untagged	none	User_Invitados

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE
tunnel		none	none	none
tunnel.10		none	router-akea	Vpn-Empresa

Figura 5-2 Interfaces y Zonas

Las pruebas realizadas para la generación de tráfico que atraviese la solución de seguridad perimetral se presentan en la Tabla 5-1, las cuales aplican las políticas de acceso, navegación y perfiles de seguridad propuestas.

Tabla 5-1 Pruebas para la generación de tráfico

ZONA ORIGEN	ZONA DESTINO	DETALLES DE PRUEBA
User_Invitado	ISP_Principal	Generar tráfico hacia Internet desde la PC conectada a la interfaz eth1/6. La navegación del usuario invitado es limitado.
User_Invitado	Administracion	Generar tráfico hacia la red de Administración, el usuario invitado no debe tener acceso a esta red.

User_Invitado	Servers_Internos	Generar tráfico hacia la red de Servers_Internos, el usuario invitado no debe tener acceso a esta red.
User_Invitado	Servers_Dmz	Generar tráfico mediante hacia la red de Servers_Dmz, el usuario invitado no debe tener acceso a esta red.
User_Invitado	User_Empresa	Generar tráfico hacia la red de usuarios internos, el usuario invitado no debe tener acceso a esta red.
User_Empresa	ISP_Principal	Generar tráfico hacia Internet desde la PC conectada a la interfaz eth1/3. La navegación de los usuarios empresariales depende del departamento a que pertenezca mediante control de usuario es limitado. Se prueba navegación para user_tecnico, user_comercial y user_rrhh.
User_Empresa	Administracion	Generar tráfico hacia la red de Administracion, solo los usuarios del Departamento técnico deben tener acceso.
User_Empresa	Servers_Internos	Generar tráfico hacia la red de Servers_Internos, solo los usuarios del Departamento técnico deben tener acceso a todos los servers. Dependiendo del departamento se tiene acceso a los servidores internos por ejemplo al Repositorio solo accede el Departamento recursos humanos.
User_Empresa	Servers_Dmz	Generar tráfico hacia la red de Servers_Internos, solo los usuarios del Departamento técnico deben tener acceso.
Vpn_Empresa	ISP_Principal	Generar tráfico mediante una conexión con el cliente VPN de Global Protect desde una PC fuera de la organización. La navegación debe ser de acuerdo a los perfiles de cada usuario y departamento como si estuviera conectado desde la red interna.
Vpn_Empresa	Administracion	Generar tráfico hacia la red de Administracion, solo los usuarios del Departamento técnico deben tener acceso.
Vpn_Empresa	Servers_Internos	Generar tráfico hacia la red de Servers_Internos, solo los usuarios del Departamento técnico deben tener acceso a todos los servers. Dependiendo del departamento se tiene acceso a los servidores internos por ejemplo al Repositorio solo accede el Departamento recursos humanos.

Vpn_Empresa	Servers_Dmz	Generar tráfico hacia la red de Servers_Internos, solo los usuarios del Departamento técnico deben tener acceso.
Servers_Interno	ISP_Principal	Generar tráfico hacia Internet desde el server conectado a la interfaz eth1/4, la navegación de los servidores es limitada.
Servers_Dmz	ISP_Principal	Generar tráfico hacia Internet desde el server conectado a la interfaz eth1/5, la navegación de los servidores es limitada.
ISP_Principal	Servers_Dmz	Generar tráfico desde Internet para consumir los servicios publicados en la DMZ.

Luego de la generación de tráfico entre zonas, se procede exportar de la solución de seguridad perimetral un archivo de soporte llamado tech_support, el cual es cargado en la página de Palo Alto Networks para generar un BPA (Best Practice Assessment).

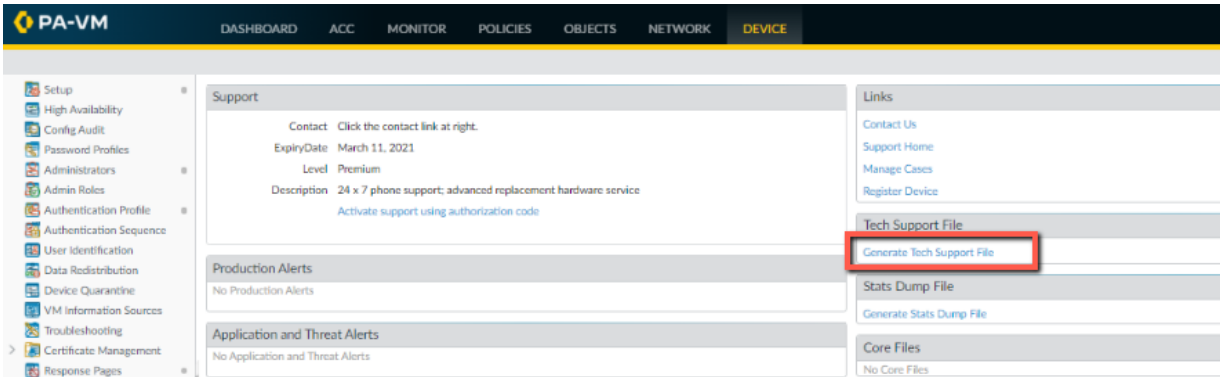


Figura 5-3 Generación de archivo tech_support

Un BPA permite determinar el estado actual de las configuraciones y la aplicación de políticas de seguridad, presenta una guía para mejorar el rendimiento de la solución perimetral, identifica los posibles riesgos y las configuraciones faltantes para alcanzar una adopción completa a las funcionalidades como Next Generation Firewall (Palo Alto Networks, 2020a).

Para generar este tipo de informe se requiere de una cuenta de soporte en Palo Alto Networks. Los archivos que se generan son tres, un informe ejecutivo en pdf con los resultados del BPA, un archivo xlsx con la guía para mejorar el rendimiento de la solución y un archivo xml, que presenta gráficamente los mapas de calor de adopción y una guía interactiva para la aplicación de las mejores prácticas de configuración.

A continuación, se presentan los resultados más relevantes del BPA generado, el informe completo se encuentra en el Anexo F.

La Figura 5-4 muestra el porcentaje de adopción de la solución propuesta, en comparación con las mejores prácticas de configuración y también en relación con el tipo de industria, en este caso, se hace referencia a la industria de servicios de Telecomunicaciones.

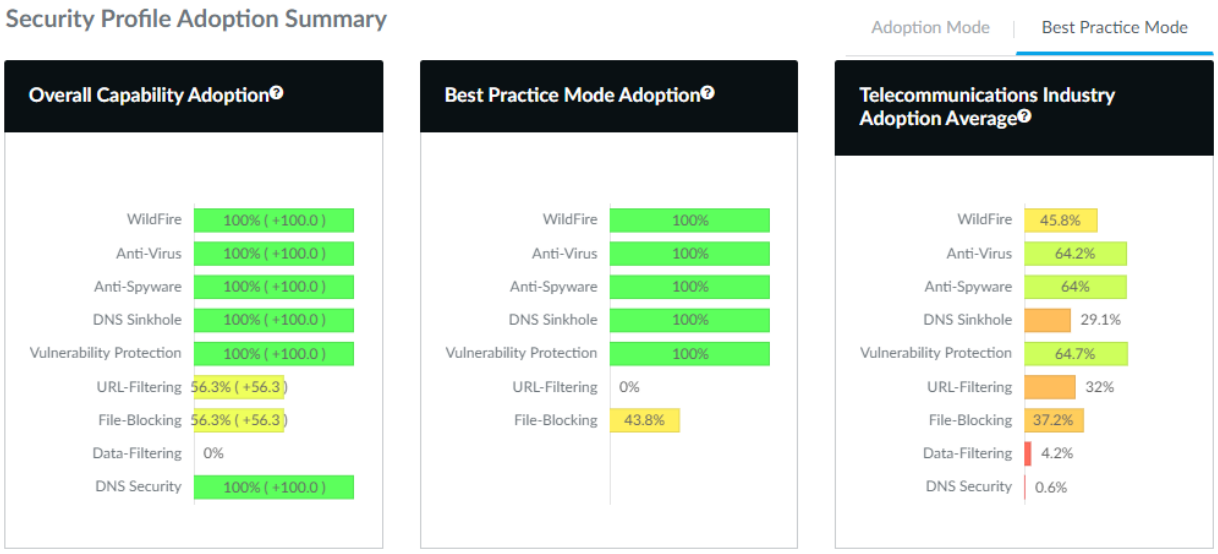


Figura 5-4 Resumen de Adopción
Fuente: (Palo Alto Networks, 2021)

A pesar de que se tiene un alto porcentaje de adopción con relación a las mejores prácticas de configuración, existen políticas y perfiles que podrían ser analizados para mejorar la adopción con referente a la industria de las telecomunicaciones, esto se lo puede realizar con el uso del archivo en Excel y la guía interactiva que entrega el BPA.

Un tema importante a considerar es la adopción a políticas con controles en base a usuarios, lo cual permite un mejor control de accesos, a pesar de esta integración el BPA presenta un 68.8% de adopción en este tema, esto es debido a que Palo Alto Networks siempre va a considerar una mejor opción la integración con usuarios de directorio activo para mejor autenticación.

Además, como se muestra en la Figura 5-5, se presenta una adopción a políticas basadas en aplicación, sin embargo, su porcentaje aún es bajo, esto se puede ir mejorando con análisis de tráfico para la configuración de políticas con aplicaciones específicas. También, se tiene un porcentaje alto en el control de políticas por servicio debido a que se identifican las aplicaciones

para puertos específicos o por defecto, por ejemplo, la aplicación ssh por su puerto por defecto 22 es el único tráfico ssh que se permite.

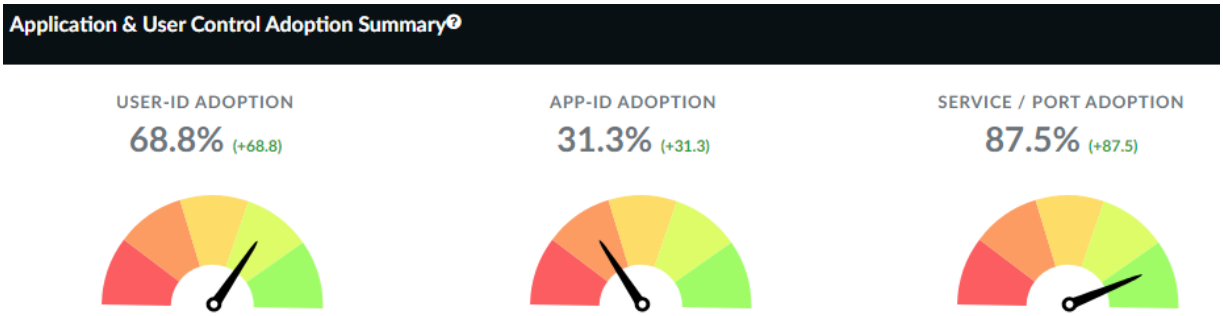
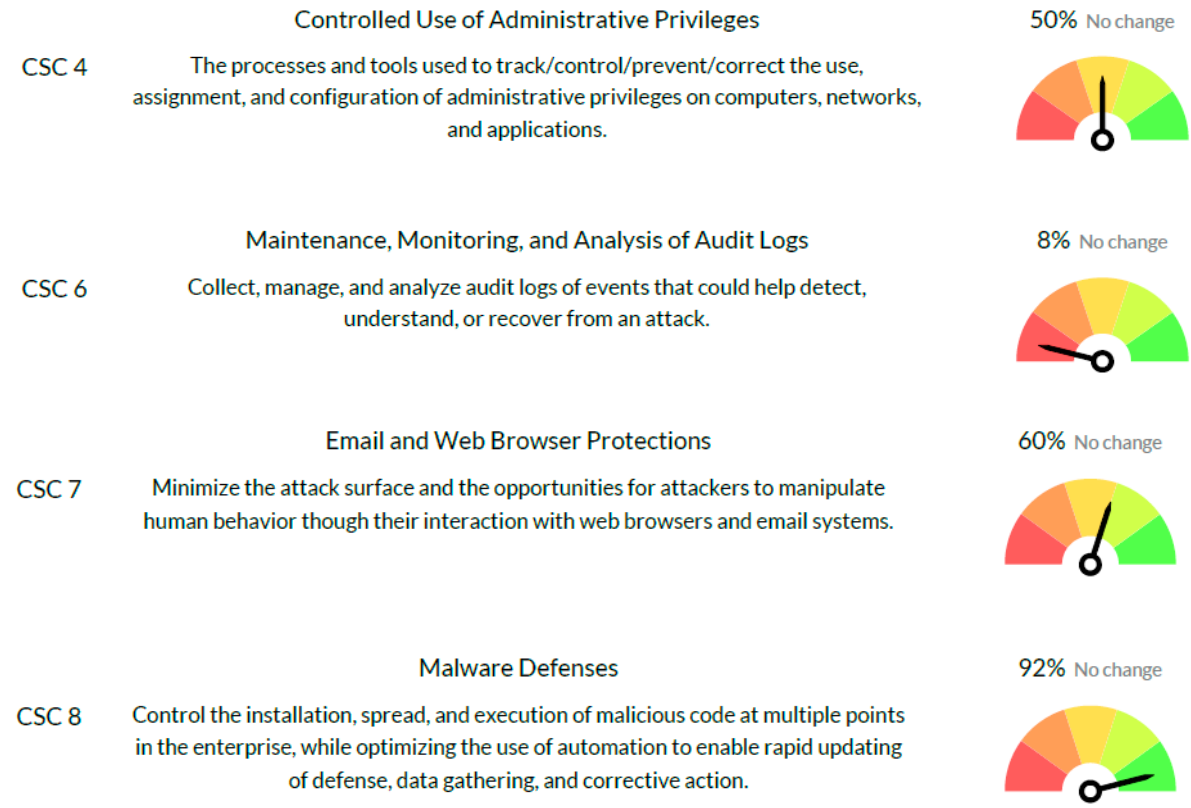


Figura 5-5 Adopción de APP-ID y USER-ID
Fuente: (Palo Alto Networks, 2021)

Finalmente, en la Figura 5-6 se presenta los resultados referentes a las configuraciones de controles de seguridad critica, a nivel de protección los porcentajes son altos, sin embargo, se tiene un bajo porcentaje a nivel de monitoreo y auditoria de logs, esto se debe principalmente porque los logs se almacenan en el mismo dispositivo y no se ha configurado su envío hacia un correlacionador de eventos.



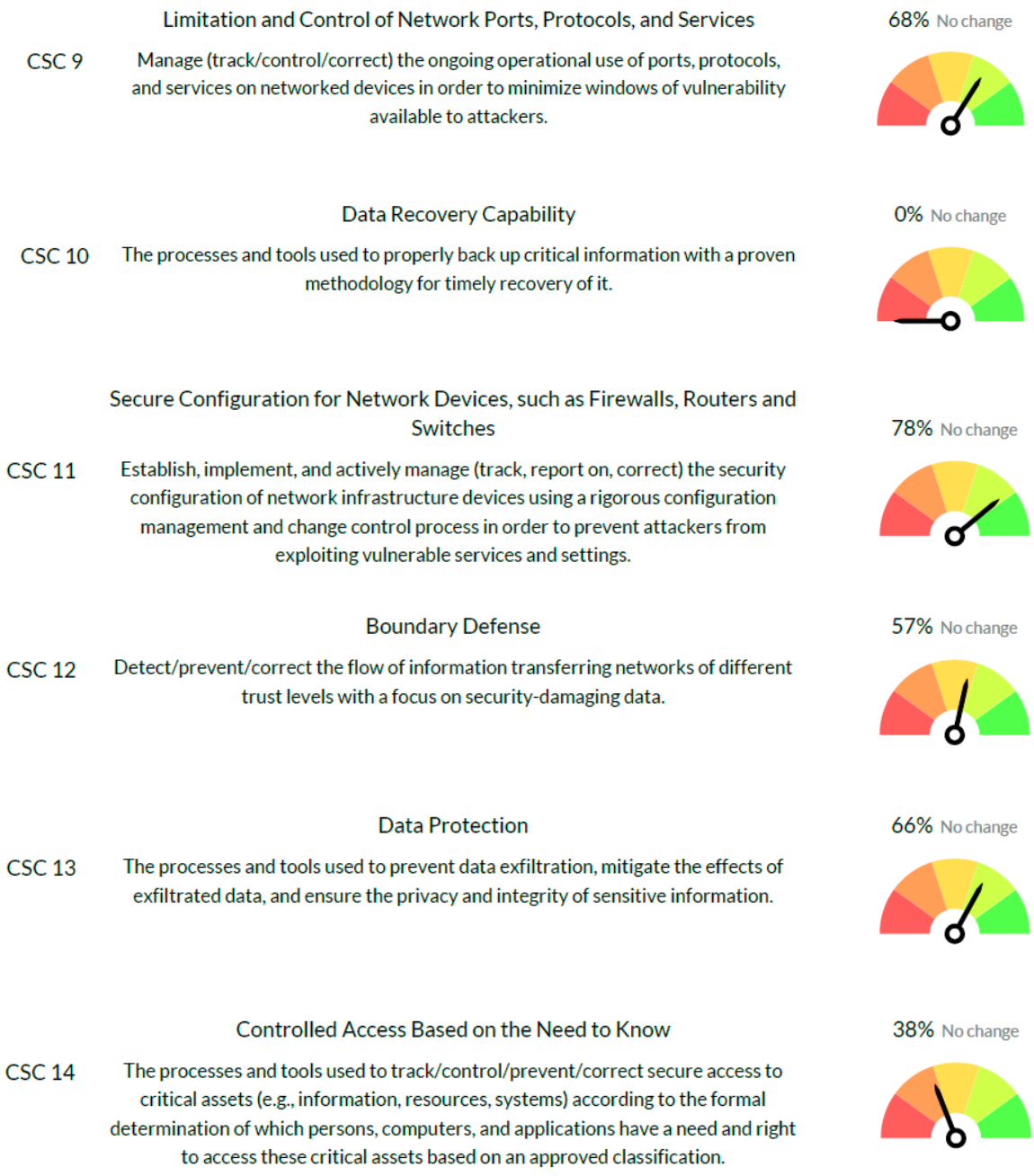


Figura 5-6 Resumen de Controles de Seguridad Críticos (CSC)
Fuente: (Palo Alto Networks, 2021)

EL BPA realiza 354 pruebas de todas las configuraciones que se encuentran en la solución de seguridad perimetral, el archivo Excel del informe que el BPA presenta indica los resultados de cada una de esas pruebas, como prueba pasada, fallida o con observaciones. En la Tabla 5-2 se presentan los resultados obtenidos de las configuraciones realizadas para el esquema de evaluación presentado.

Tabla 5-2 Resultados del BPA generado

Feature	Passed	Failed	Notes	Total
Objects > Anti-Spyware	4	0	0	4
Objects > Antivirus	4	0	0	4
Objects > Application Filters	0	0	1	1
Objects > File Blocking	1	1	0	2
Objects > Tags	0	1	0	1
Objects > URL Filtering	8	12	0	20
Objects > Vulnerability Protection	2	0	0	2
Objects > WildFire Analysis	1	0	0	1
Network > GlobalProtect Gateways	1	7	0	8
Network > GlobalProtect Portals	4	10	4	18
Network > IPSec Crypto	7	2	0	9
Network > Interface Mgmt	2	0	0	2
Network > Zones	12	17	5	34
Policies > Decryption Rulebase	0	1	0	1
Policies > Security	118	61	2	181
Device > Administrators	0	2	0	2
Device > Authentication Profile	0	4	1	5
Device > Authentication Profiles	0	1	0	1
Device > Authentication Sequences	0	1	0	1
Device > Authentication Settings	0	6	0	6
Device > Dynamic Updates	0	5	1	6
Device > General Settings	1	3	0	4
Device > Licenses	3	0	2	5
Device > Logging and Reporting Settings	0	1	2	3
Device > Management Interface Settings	1	1	0	2
Device > Minimum Password Complexity	0	1	0	1
Device > Policy Rulebase	1	0	0	1
Device > Setup > Content-ID	2	3	2	7
Device > Setup > Services	2	2	0	4
Device > Setup > Session	4	0	0	4
Device > Setup > Telemetry	1	0	0	1
Device > Setup > WildFire	11	1	1	13
Total	**190**	**143**	**21**	**354**

Fuente: Resultados obtenidos de la generación de BPA a través de la página de soporte de Palo Alto Networks

Se presenta un 54% de pruebas pasadas y un 6% de pruebas pasadas con observación, esto indica que la solución presentada tiene un 60% de efectividad con relación a las recomendaciones de configuraciones de Palo Alto Networks. La ventaja con esta solución es que Palo Alto Networks presenta la guía para poder ir mejorando el rendimiento de la solución. En la siguiente tabla se presenta algunas de las recomendaciones que el BPA generó, la empresa puede ir adoptando estas configuraciones, por ejemplo se presenta la recomendación para políticas de desencripción para poder tener visualización completa del tráfico, para este parámetro se requiere de certificados instalados en todos los cliente para generar la confianza entre el NGFW y el cliente, esto se puede ir adoptando conforme la empresa realice la instalación del certificado de confianza en todos los clientes.

Tabla 5-3 Ejemplo de recomendaciones del BPA

Feature	Check	Message	Complexity
Device > General Settings	Login Banner	It is recommended to have a descriptive Login Banner	Easy
Device > Management Interface Settings	Permitted IP Addresses	Permitted IP Addresses should be configured	Advanced
Policies > Decryption Rulebase	SSH Proxy / SSH Tunnel	It is recommended to configure SSH Proxy to detect and block SSH Tunneling and to limit user access to SSH traffic	Medium
Policies > Security	Inbound Malicious IP Address Feed	It is recommended to configure and enable a deny rule with the 'Palo Alto Networks - Known malicious IP addresses' EDL in the source address, Log at Session End enabled, and a Log Forwarding Profile configured	Medium
Policies > Security	Quic App Deny Rule	It is recommended to have a security policy rule to block QUIC on its UDP service ports (80 and 443) and a separate rule to block the 'quic' application before any allow rules to ensure encrypted traffic is decrypted and inspected	Medium

Fuente: Recomendaciones propuestas una vez generado el BPA mediante el archivo de soporte a través de la página de soporte de Palo Alto Networks.

5.2 EVALUACIÓN DE LAS POLÍTICAS DE SEGURIDAD PROPUESTAS.

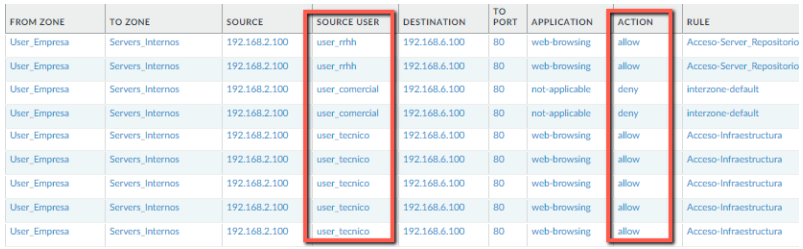
En esta sección se analiza la aplicabilidad de las políticas de seguridad propuestas con el uso de la metodología de seguridad seleccionada. Se utiliza los mismos criterios para los niveles de cumplimiento presentados en los capítulos anteriores en conjunto con las pruebas realizadas que permite el esquema de evaluación en plataformas virtuales.

Tabla 5-4 Niveles de cumplimiento

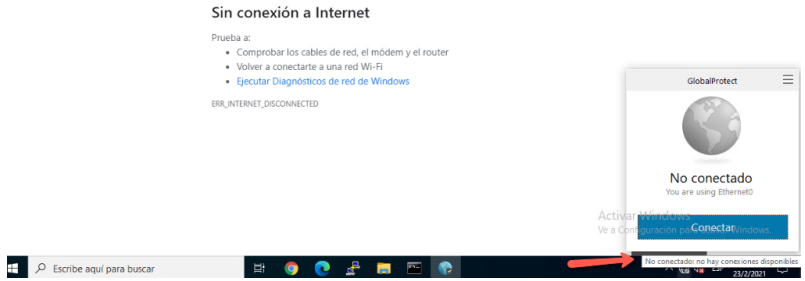
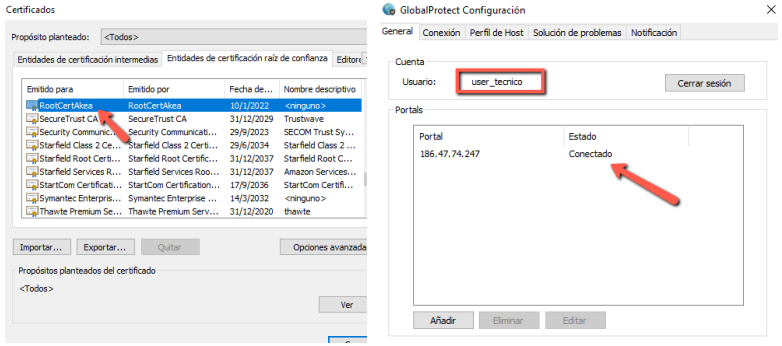
NIVEL	COLOR	DETALLE
Si cumple		La metodología de seguridad perimetral y la arquitectura permiten la aplicación de la política de seguridad propuesta y se lleva a cabo los controles de seguridad en los sistemas de información.
Cumple parcialmente		La metodología de seguridad perimetral y la arquitectura permiten en parte la aplicación de la política de seguridad propuesta, sin embargo no cumple con todos los controles de seguridad en los sistemas de información.
No cumple		La metodología de seguridad perimetral y la arquitectura no permiten la aplicación de la política de seguridad propuesta y no se lleva a cabo los controles de seguridad en los sistemas de información.
Neutro		No aplica para seguridad perimetral

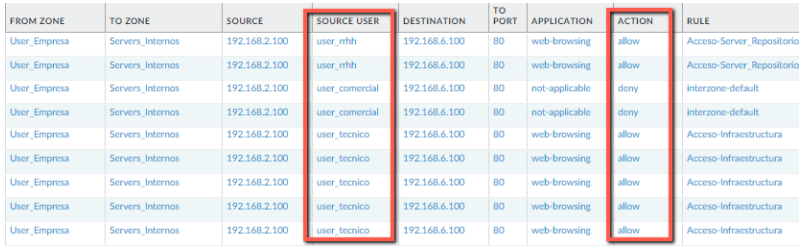
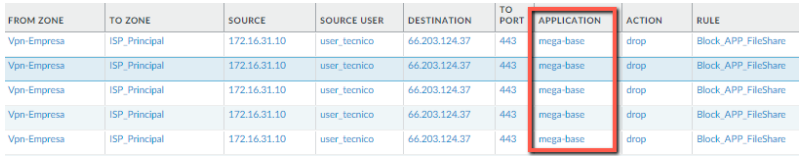
A continuación, en la Tabla 5-5 se presenta los resultados del análisis en base a los controles seleccionados para mejorar las políticas de seguridad y las pruebas realizadas con el apoyo del ambiente virtual.

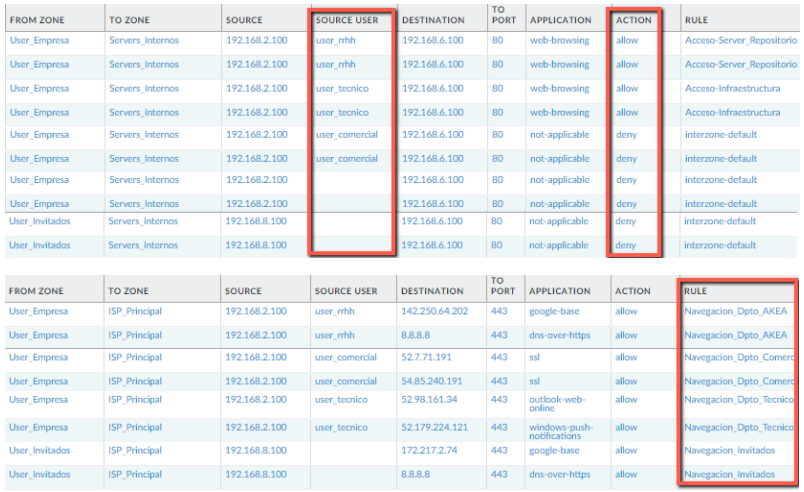
Tabla 5-5 Cumplimiento de políticas de seguridad propuestas

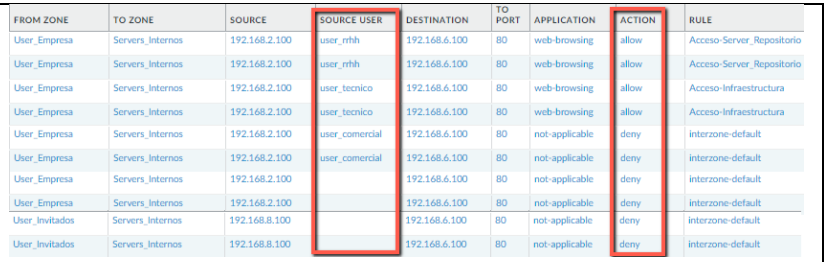
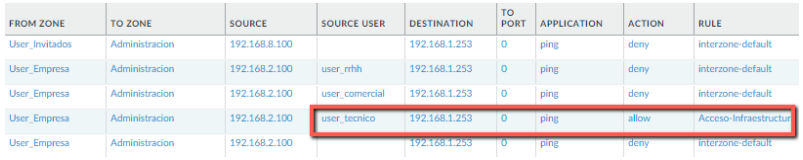
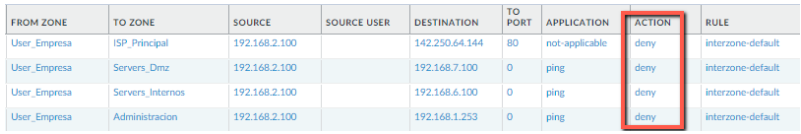
	CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	APLICABILIDAD	DETALLE
A5	**Políticas de seguridad de la información**		
A5.1	**Directrices de gestión de la seguridad de la información**		
A5.1.1	Políticas para la seguridad de la información		Este control no tiene relación directa con la metodología de seguridad, pero esta propuesto ya que es necesario la documentación oficial de las políticas de seguridad que deben ser de conocimiento general de todo el personal de la empresa
A5.1.2	Revisión de las políticas para la seguridad de la información		Este control no tiene relación directa con la metodología de seguridad, pero esta propuesta ya que es indispensable que las políticas sean revisadas por las gerencia para su correcta aplicación de acuerdo al giro de negocio.
A6	**Organización de la seguridad de la información**		
A6.1	**Organización interna**		
A6.1.1	Roles y responsabilidades en seguridad de la información		La metodología de seguridad permite los controles en base a usuarios, en este caso se configuran usuarios locales y cada grupo de usuarios tienen sus correspondientes permisos y privilegios. 

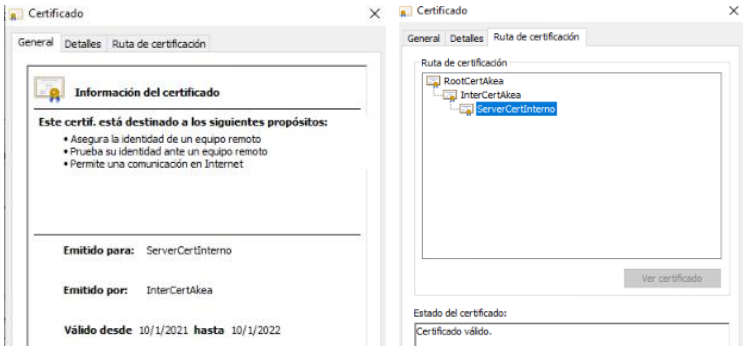
FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
User_Empresa	Servers_Internos	192.168.2.100	user_rrhh	192.168.6.100	80	web-browsing	allow	Acceso-Server_Repositorio
User_Empresa	Servers_Internos	192.168.2.100	user_rrhh	192.168.6.100	80	web-browsing	allow	Acceso-Server_Repositorio
User_Empresa	Servers_Internos	192.168.2.100	user_comercial	192.168.6.100	80	not-applicable	deny	interzone-default
User_Empresa	Servers_Internos	192.168.2.100	user_comercial	192.168.6.100	80	not-applicable	deny	interzone-default
User_Empresa	Servers_Internos	192.168.2.100	user_tecnico	192.168.6.100	80	web-browsing	allow	Acceso-Infraestructura
User_Empresa	Servers_Internos	192.168.2.100	user_tecnico	192.168.6.100	80	web-browsing	allow	Acceso-Infraestructura
User_Empresa	Servers_Internos	192.168.2.100	user_tecnico	192.168.6.100	80	web-browsing	allow	Acceso-Infraestructura
User_Empresa	Servers_Internos	192.168.2.100	user_tecnico	192.168.6.100	80	web-browsing	allow	Acceso-Infraestructura
User_Empresa	Servers_Internos	192.168.2.100	user_tecnico	192.168.6.100	80	web-browsing	allow	Acceso-Infraestructura

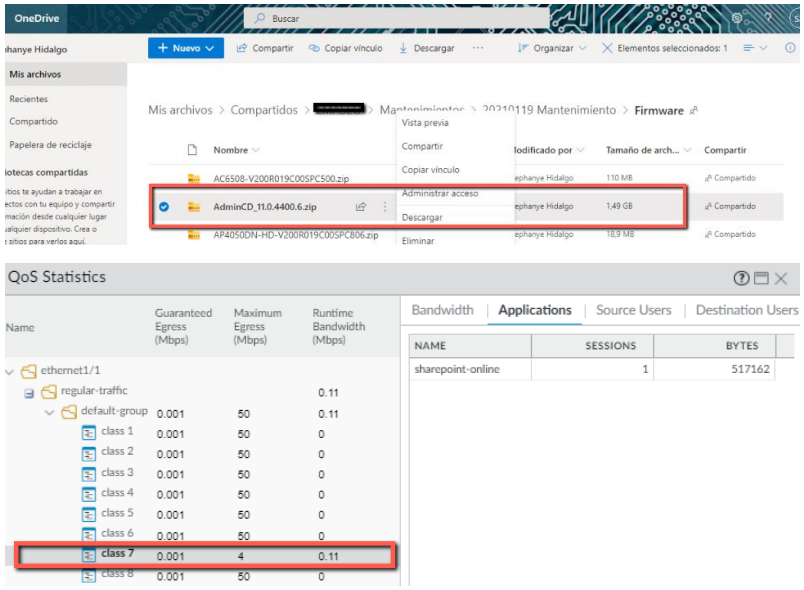
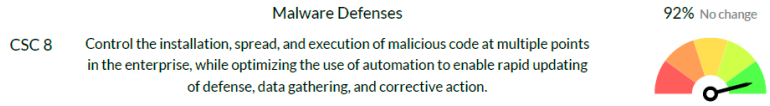
A6.2	Los dispositivos móviles y el teletrabajo		
A6.2.1	Política de dispositivos móviles		Gracias a la capacidad de controles en base a usuarios, el control de dispositivos móviles se lo realiza en base al aplicativo de Global Protect, tanto en laptops como en smartphones. En el ambiente virtual se pudo corroborar que, si un usuario se conecta a la red empresarial sin un usuario registrado, no tiene acceso a los recursos. 
A6.2.2	Teletrabajo		La metodología de seguridad tiene la capacidad de realizar una conexión VPN cliente servidor mediante el mismo aplicativo de Global Protect, esta conexión es segura y encriptada mediante un certificado autofirmado instalado en el dispositivo externo. 

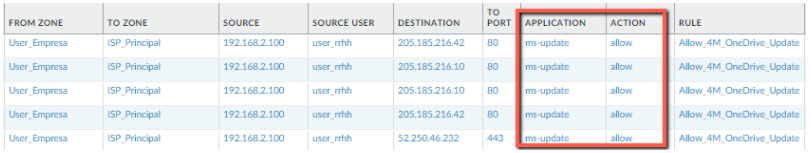
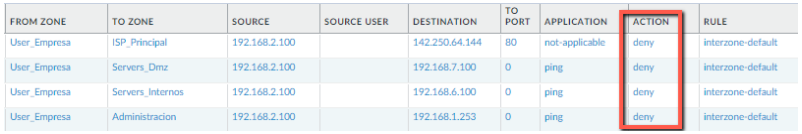
<table>
<tr><td>A8</td><td colspan="3">Gestión de activos</td></tr>
<tr><td>A8.2</td><td colspan="3">Clasificación de la información</td></tr>
<tr><td>A8.2.1</td><td>Clasificación de la información</td><td></td><td>A pesar de ser un control que no se aplica directamente en la metodología de seguridad perimetral, se la propone porque es necesario identificar el tipo de información que circula en la red para configurar las políticas de seguridad correspondientes.</td></tr>
<tr><td>A8.2.2</td><td>Etiquetado de la información</td><td></td><td>A pesar de ser un control que no se aplica directamente en la metodología de seguridad perimetral, se la propone porque es necesario etiquetar el tipo de información que circula en la red para configurar las políticas de seguridad correspondientes.</td></tr>
<tr><td>A8.2.3</td><td>Manipulado de la información</td><td></td><td>La metodología de seguridad permite el control en base a usuarios, y define políticas de accesos a los recursos de la empresa.
 
<table>
<tr><th>FROM ZONE</th><th>TO ZONE</th><th>SOURCE</th><th>SOURCE USER</th><th>DESTINATION</th><th>TO PORT</th><th>APPLICATION</th><th>ACTION</th><th>RULE</th></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_rrhh</td><td>192.168.6.100</td><td>80</td><td>web-browsing</td><td>allow</td><td>Acceso-Server_Repositorio</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_rrhh</td><td>192.168.6.100</td><td>80</td><td>web-browsing</td><td>allow</td><td>Acceso-Server_Repositorio</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_comercial</td><td>192.168.6.100</td><td>80</td><td>not-applicable</td><td>deny</td><td>interzone-default</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_comercial</td><td>192.168.6.100</td><td>80</td><td>not-applicable</td><td>deny</td><td>interzone-default</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_tecnico</td><td>192.168.6.100</td><td>80</td><td>web-browsing</td><td>allow</td><td>Acceso-Infraestructura</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_tecnico</td><td>192.168.6.100</td><td>80</td><td>web-browsing</td><td>allow</td><td>Acceso-Infraestructura</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_tecnico</td><td>192.168.6.100</td><td>80</td><td>web-browsing</td><td>allow</td><td>Acceso-Infraestructura</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_tecnico</td><td>192.168.6.100</td><td>80</td><td>web-browsing</td><td>allow</td><td>Acceso-Infraestructura</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_tecnico</td><td>192.168.6.100</td><td>80</td><td>web-browsing</td><td>allow</td><td>Acceso-Infraestructura</td></tr>
</table>
Tiene la capacidad de realizar control por aplicaciones la cual define que únicamente se puede utilizar los servicios de Microsoft para la trasferencia de archivos, los demás repositorios están bloqueados.
 
<table>
<tr><th>FROM ZONE</th><th>TO ZONE</th><th>SOURCE</th><th>SOURCE USER</th><th>DESTINATION</th><th>TO PORT</th><th>APPLICATION</th><th>ACTION</th><th>RULE</th></tr>
<tr><td>Vpn-Empresa</td><td>ISP_Principal</td><td>172.16.31.10</td><td>user_tecnico</td><td>66.203.124.37</td><td>443</td><td>mega-base</td><td>drop</td><td>Block_APP_FileShare</td></tr>
<tr><td>Vpn-Empresa</td><td>ISP_Principal</td><td>172.16.31.10</td><td>user_tecnico</td><td>66.203.124.37</td><td>443</td><td>mega-base</td><td>drop</td><td>Block_APP_FileShare</td></tr>
<tr><td>Vpn-Empresa</td><td>ISP_Principal</td><td>172.16.31.10</td><td>user_tecnico</td><td>66.203.124.37</td><td>443</td><td>mega-base</td><td>drop</td><td>Block_APP_FileShare</td></tr>
<tr><td>Vpn-Empresa</td><td>ISP_Principal</td><td>172.16.31.10</td><td>user_tecnico</td><td>66.203.124.37</td><td>443</td><td>mega-base</td><td>drop</td><td>Block_APP_FileShare</td></tr>
<tr><td>Vpn-Empresa</td><td>ISP_Principal</td><td>172.16.31.10</td><td>user_tecnico</td><td>66.203.124.37</td><td>443</td><td>mega-base</td><td>drop</td><td>Block_APP_FileShare</td></tr>
</table></td></tr>
</table>

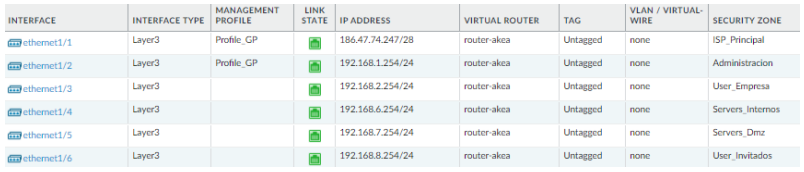
<table>
<tr><td>A9</td><td colspan="3">Control de acceso</td></tr>
<tr><td>A9.1</td><td colspan="3">Requisitos de negocio para el control de acceso</td></tr>
<tr><td>A9.1.1</td><td>Política de control de acceso</td><td></td><td>La capacidad de control en base usuarios de la metodología de seguridad permite la creación de políticas de control de acceso en base a las funciones de cada departamento, de igual manera permite la configuración de las políticas de navegación con las restricciones correspondientes para cada grupo de usuarios, empresarial y externo.

<table>
<tr><th>FROM ZONE</th><th>TO ZONE</th><th>SOURCE</th><th>SOURCE USER</th><th>DESTINATION</th><th>TO PORT</th><th>APPLICATION</th><th>ACTION</th><th>RULE</th></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_rrhh</td><td>192.168.6.100</td><td>80</td><td>web-browsing</td><td>allow</td><td>Acceso-Server_Repositorio</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_rrhh</td><td>192.168.6.100</td><td>80</td><td>web-browsing</td><td>allow</td><td>Acceso-Server_Repositorio</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_tecnico</td><td>192.168.6.100</td><td>80</td><td>web-browsing</td><td>allow</td><td>Acceso-Infraestructura</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_tecnico</td><td>192.168.6.100</td><td>80</td><td>web-browsing</td><td>allow</td><td>Acceso-Infraestructura</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_comercial</td><td>192.168.6.100</td><td>80</td><td>not-applicable</td><td>deny</td><td>interzone-default</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td>user_comercial</td><td>192.168.6.100</td><td>80</td><td>not-applicable</td><td>deny</td><td>interzone-default</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td></td><td>192.168.6.100</td><td>80</td><td>not-applicable</td><td>deny</td><td>interzone-default</td></tr>
<tr><td>User_Empresa</td><td>Servers_Internos</td><td>192.168.2.100</td><td></td><td>192.168.6.100</td><td>80</td><td>not-applicable</td><td>deny</td><td>interzone-default</td></tr>
<tr><td>User_Invitados</td><td>Servers_Internos</td><td>192.168.8.100</td><td></td><td>192.168.6.100</td><td>80</td><td>not-applicable</td><td>deny</td><td>interzone-default</td></tr>
<tr><td>User_Invitados</td><td>Servers_Internos</td><td>192.168.8.100</td><td></td><td>192.168.6.100</td><td>80</td><td>not-applicable</td><td>deny</td><td>interzone-default</td></tr>
</table>
<table>
<tr><th>FROM ZONE</th><th>TO ZONE</th><th>SOURCE</th><th>SOURCE USER</th><th>DESTINATION</th><th>TO PORT</th><th>APPLICATION</th><th>ACTION</th><th>RULE</th></tr>
<tr><td>User_Empresa</td><td>ISP_Principal</td><td>192.168.2.100</td><td>user_rrhh</td><td>142.250.64.202</td><td>443</td><td>google-base</td><td>allow</td><td>Navegacion_Dpto_AKEA</td></tr>
<tr><td>User_Empresa</td><td>ISP_Principal</td><td>192.168.2.100</td><td>user_rrhh</td><td>8.8.8.8</td><td>443</td><td>dns-over-https</td><td>allow</td><td>Navegacion_Dpto_AKEA</td></tr>
<tr><td>User_Empresa</td><td>ISP_Principal</td><td>192.168.2.100</td><td>user_comercial</td><td>52.7.71.191</td><td>443</td><td>ssl</td><td>allow</td><td>Navegacion_Dpto_Comerc</td></tr>
<tr><td>User_Empresa</td><td>ISP_Principal</td><td>192.168.2.100</td><td>user_comercial</td><td>54.85.240.191</td><td>443</td><td>ssl</td><td>allow</td><td>Navegacion_Dpto_Comerc</td></tr>
<tr><td>User_Empresa</td><td>ISP_Principal</td><td>192.168.2.100</td><td>user_tecnico</td><td>52.98.161.34</td><td>443</td><td>outlook-web-online</td><td>allow</td><td>Navegacion_Dpto_Tecnico</td></tr>
<tr><td>User_Empresa</td><td>ISP_Principal</td><td>192.168.2.100</td><td>user_tecnico</td><td>52.179.224.121</td><td>443</td><td>windows-push-notifications</td><td>allow</td><td>Navegacion_Dpto_Tecnico</td></tr>
<tr><td>User_Invitados</td><td>ISP_Principal</td><td>192.168.8.100</td><td></td><td>172.217.2.74</td><td>443</td><td>google-base</td><td>allow</td><td>Navegacion_Invitados</td></tr>
<tr><td>User_Invitados</td><td>ISP_Principal</td><td>192.168.8.100</td><td></td><td>8.8.8.8</td><td>443</td><td>dns-over-https</td><td>allow</td><td>Navegacion_Invitados</td></tr>
</table></td></tr>
<tr><td>A9.1.2</td><td>Acceso a las redes y a los servicios de red</td><td></td><td>La metodología de seguridad permite el control a las redes empresariales, así como a sus servicios y está configurado de acuerdo a los privilegios asignados por las gerencias. El personal externo no tiene acceso a los recursos internos.</td></tr>
</table>

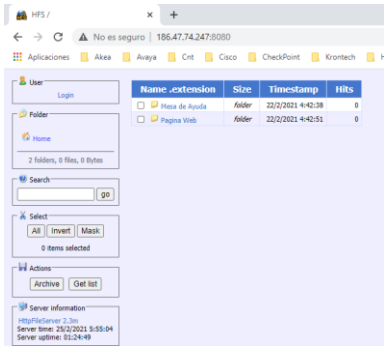
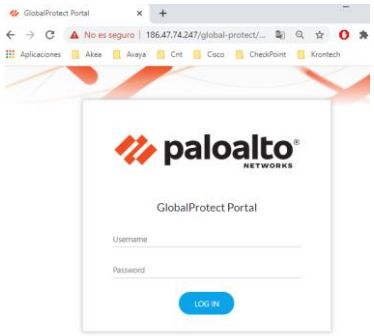
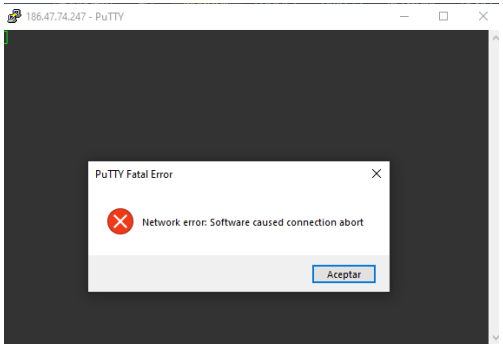
			
A9.2	**Gestión de acceso de usuario**		
A9.2.1	Registro y baja de usuario		Este control es compartido con las gerencias, el departamento de recursos humanos y el departamento técnico, sin embargo, solamente el departamento técnico puede habilitar y deshabilitar una cuenta de usuario empresarial, ya que solo ellos disponen del acceso a la administración. 
A9.2.2	Provisión de acceso de usuario		La metodología de seguridad permite proteger la red empresarial y sus servicios de conexiones no autorizadas, si un usuario se conecta a la red empresarial, no tendrá acceso a ningún servicio sin un usuario registrado. 
A9.2.3	Gestión de privilegios de acceso		Este control es compartido con las gerencias, y el departamento técnico, y solo el departamento técnico con la autorización de

			gerencia puede modificar los privilegios de un usuario. La metodología permite un registro de logs de todos los cambios realizados y de quien los ejecuto.  ADMINISTRAT... HOST CLIENT COMMA... RESULT CONFIGURATION PATH FULL PATH BEFORE CHANGE AFTER CHANGE user_tecnico 181.175.230.... Web commit Submitted user_tecnico 181.175.230.... Web commit Submitted user_tecnico 181.175.230.... Web edit Succeed... vsys vsys1 rulebase security rules Global_Protect_Interno /config/devices/... Global_Protect_I... 21c7518a-6416-4296-b8a2-47df4b1f01fa [ ] Global_Protect_I... 21c7518a-6416-4296-b8a2-47df4b1f01fa [lo user_tecnico 181.175.230.... Web commit Submitted user_tecnico 181.175.230.... Web edit Succeed... vsys vsys1 rulebase security rules Allow_4M_OneDrive_Update /config/devices/... Allow_4M_One... c1e8399c-f1a1-471c-b0ee-e9566e24d189 [Allow_4M_One... c1e8399c-f1a1-471c-b0ee-e9566e24d189 [
A10	**Criptografía**		
A10.1	**Controles criptográficos**		
A10.1.1	Política de uso de los controles criptográficos		La conexión interna y externa a través del aplicativo Global Protect, requiere de un certificado, el cual ha sido autofirmado por el NGFW considerando que puede actuar de CA, lo que permite una conexión segura de los usuarios externos e internos.  Certificado General Detalles Ruta de certificación Información del certificado Este certif. está destinado a los siguientes propósitos: • Asegura la identidad de un equipo remoto • Prueba su identidad ante un equipo remoto • Permite una comunicación en Internet Emitido para: ServerCertInterno Emitido por: InterCertAkea Válido desde 10/1/2021 hasta 10/1/2022 Certificado General Detalles Ruta de certificación Ruta de certificación RootCertAkea InterCertAkea ServerCertInterno Ver certificado Estado del certificado: Certificado válido.
A10.1.2	Gestión de claves		La renovación del certificado de conexión por Global Protect la realiza el departamento técnico, ya que solo ellos tienen la autorización del acceso a la administración del NGFW.

A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		
A12.1.3	Gestión de capacidades		La metodología de seguridad tiene la capacidad de realizar controles de ancho de banda para aplicaciones que pueden afectar a los servicios de la empresa, esto esta aplicado para los servicios de Microsoft para file sharing y para las actualizaciones. 
A12.2	**Protección contra el software malicioso (malware)**		
A12.2.1	Controles contra el código malicioso		La metodología de seguridad permite la protección de la infraestructura contra ataques de malware conocido y de día cero. 

A12.5	**Control del software en explotación**		
A12.5.1	Instalación del software en explotación		La metodología de seguridad permite el control de instalación de software de explotación, así como la identificación de dispositivos que se encuentren vulnerados. Además, se permite las actualizaciones de los sistemas operativos con el fin de mantener sus últimas versiones y disminuir la brecha de explotación de vulnerabilidades. 
A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red		La metodología de seguridad permite identificar si un usuario no autorizado se conecta a la red de la empresa, sin embargo, este usuario no autorizado no tendrá acceso a ningún recurso, lo que permite un control de las redes empresariales y sus servicios. 
A13.1.2	Seguridad de los servicios de red		La metodología de seguridad tiene la capacidad de proteger a toda la infraestructura de red de ataques de malware, phising, virus, exploits, etc. gracias a sus perfiles de seguridad configurados en todas las políticas.

			
A13.1.3	Segregación en redes		La metodología de seguridad es zonal, por lo que permite la segregación de redes, además de ser zero trust lo que implica que requiere de una política explicita para permitir el tráfico entre zonas. 

A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		
A14.1	**Requisitos de seguridad en los sistemas de información**		
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas		La metodología de seguridad tiene la capacidad de control en base a aplicaciones y puertos, lo que permite la configuración de políticas de acceso a través de redes públicas únicamente a los servicios que se requiere, en este caso web-browsing por el puerto 8080 y ssl para Global Protect. Los demás servicios no son autorizados.   

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

El análisis realizado en este proyecto determinó que la metodología de seguridad perimetral actual de la empresa AKEA S.A no cuenta con las funcionalidades necesarias para la detección y prevención de ataques debido a que su protección es a base de direcciones IP y protocolos, lo cual es un mecanismo de seguridad muy básico, los atacantes pueden romper esta seguridad sin mayor esfuerzo. Además, no cuenta con un sistema de prevención de intrusos ni de antivirus ni análisis de amenazas de día cero, por lo cual la seguridad de la red se encuentra expuesta a ataques como malware, phishing, comando y control.

La metodología de seguridad actual no tiene la capacidad para cumplir totalmente con las políticas de seguridad propuestas por la empresa, ya que no cuenta con los módulos de prevención/detección de intrusos, antivirus, antispyware y tampoco cuenta con un control en base a aplicaciones y a usuarios, lo que representa un riesgo de acceso para los servicios internos de la empresa.

Se seleccionaron los controles necesarios mediante las recomendaciones presentadas en la norma ISO/IEC 27002, las cuales son aplicadas y probadas en varios proyectos de seguridad y se complementan con las recomendaciones de Palo Alto Networks para la reducción de los riesgos que presenta la metodología de seguridad actual, así como el afinamiento del documento de políticas de seguridad.

Mediante un análisis comparativo entre las tres marcas líderes, se llegó a la conclusión que la metodología de seguridad perimetral que Palo Alto Networks ofrece es la mejor opción para mitigar los riesgos actuales que presenta la empresa y representa más beneficio a largo plazo con menor inversión.

Palo Alto Networks ofrece una solución de seguridad zonal, zero trust haciendo que todo el tráfico sea analizado sin excepción, y también cuenta con un sistema de procesamiento paralelo (SP3), lo que permite mantener todos los módulos de seguridad activos a la vez sin reducir su desempeño.

Se realizó la propuesta de políticas de seguridad en base a los controles seleccionados de la norma ISO/IEC 27002, estas políticas están orientadas a la seguridad perimetral y alinea el documento de políticas de seguridad actual a las recomendaciones de la norma.

Una vez seleccionada la metodología de seguridad y realizada la propuesta de políticas, se presentó un rediseño de la arquitectura de red y el modelo de equipamiento de seguridad perimetral para la empresa, Adicional, se definió una arquitectura segmentada por redes y un equipamiento zonal. Debido al tráfico que la empresa presenta y a la cantidad de usuarios que operan en ella, se propuso el modelo PA-220 el cual cuenta con un throughtput de 350Mbps con todas las funcionalidades de seguridad activas.

Finalmente, se realizó una evaluación de la metodología y las políticas de seguridad mediante la generación de un informe de BPA (Best Practice Assessment) el cual permitió concluir que las configuraciones propuestas para la metodología de seguridad en base a las políticas de seguridad presentan un alto porcentaje de adopción a nivel de capacidades de los perfiles de seguridad, sin embargo, el mismo informe BPA presentan algunas recomendaciones que permitirá a la empresa alcanzar un mayor porcentaje de adopción a nivel de industria considerándose como industria de telecomunicaciones.

Por lo tanto, la metodología de seguridad perimetral y las políticas de seguridad propuestas permiten mejorar los controles de acceso y de navegación de los usuarios, así como disminuir la brecha de seguridad y la superficie de ataque permitiendo de esta manera presentar una red más segura y una arquitectura dispuesta a enfrentar cualquier ciberataque.

6.2 RECOMENDACIONES

Se recomienda realizar un análisis a nivel de red considerando un equipamiento mínimo de 1Gbps, debido a que, del levantamiento de información realizado, se identificó que el equipamiento de red opera a 100Mbps, por lo que los servicios podrían presentar lentitud generando un cuello de botella en las solicitudes realizadas.

Es recomendable mantener actualizado el equipamiento de la metodología de seguridad perimetral con las ultimas firmas de antivirus, antispyware y clasificación de aplicaciones y url mediante las actualizaciones automáticas, para contar con un equipamiento capaz de mitigar amenazas inclusive de día cero.

Se recomienda hacer uso de las herramientas de BPA cada 90 días, de acuerdo a las recomendaciones de Palo Alto Networks, para poder ir adoptando paulatinamente las mejores prácticas de configuración e ir disminuyendo la superficie de ataque en base a estas guías.

De acuerdo a lo que se propone en las políticas de seguridad de este proyecto, es recomendable realizar un análisis de mejora continua por parte de las gerencias y del departamento técnico al menos tres veces al año con el fin de mantener las políticas actualizadas y alineadas al giro de negocio de la empresa.

Finalmente, se recomienda que el personal técnico de la empresa AKEA S.A mantenga una actualización y capacitación sobre conocimientos de ciberseguridad para poder aplicarlos de manera eficiente en pro de la empresa y también para poder capacitar al personal interno en el manejo adecuado de los recursos empresariales.

BIBLIOGRAFÍA

Aguayo Morales, J. L. (2020). *Análisis y Propuesta de Mejoras a la Infraestructura y Seguridad de la Red LAN de la Empresa SICCEC para Perfeccionar la Disponibilidad de sus Servicios.* Universidad Politécnica Salesiana. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/18454/1/UPS - ST004457.pdf

AKEA. (2020). Obtenido de http://www.akea.ec/nosotros/

ARCOTEL. (2017). *Estatuto Orgánico de Gestión Organizacional por Procesos de la ARCOTEL*. Obtenido de https://www.arcotel.gob.ec/mision-vision-principios-y-valores2/

Bolaños Botina, J. (2018). *Diseño de la Arquitectura de Seguridad Perimetral de la Red Informatica en la Industria de Licores del Valle.* Universidad Autónoma de Occidente. Obtenido de http://red.uao.edu.co/bitstream/10614/10248/4/T07892.pdf

Check Point. (2017). Check Point Software Blade Architecture. Obtenido de https://www.checkpoint.com/downloads/product-related/brochure/Software-Blades-Architecture.pdf

Check Point. (2019). *Policy Based Routing*. Obtenido de https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_Gaia_Advanced_Routing_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_Gaia_Advanced_Routing_AdminGuide/93034

Check Point. (2020a). Check Point Infinity Architecture.

Check Point. (2020b). Check Point Infinity Total Protection. Obtenido de https://www.checkpoint.com/downloads/products/check-point-infinity-brochure.pdf

Check Point. (2020c). Check Point Security Appliances. Obtenido de https://www.checkpoint.com/downloads/products/check-point-appliances-brochure.pdf

Check Point. (2020d). *Data Loss Prevention Software Blade*. Obtenido de https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_Nex

tGenSecurityGateway_Guide/Content/Topics-FWG/Data-Loss-Prevention-Blade.htm?tocpath=_____15

Check Point. (2020e). *IPsec VPN Software Blade*. Obtenido de https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_NextGenSecurityGateway_Guide/Content/Topics-FWG/IPSec-VPN-Blade.htm?tocpath=_____7

Check Point. (2020f). *Identity Awareness R80.10 Administration Guide*. Obtenido de https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/148517

Check Point. (2020g). *Next Generation Firewalls (NGFW)*. Obtenido de https://www.checkpoint.com/products/next-generation-firewall/#

Check Point. (2020h). *Remote Access VPN*. Obtenido de https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_NextGenSecurityGateway_Guide/Content/Topics-FWG/Remote-Access-VPN.htm?tocpath=_____8

Cisco. (2019). *Cisco Catalyst 2960-Plus Series Switches Data Sheet*. Obtenido de https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-plus-series-switches/data_sheet_c78-728003.html

Delgado, S. (2018). *Propuesta de plan para certificación en la norma ISO.* Universidad Politécnica de Sinaloa. Obtenido de http://repositorio.upsin.edu.mx/Fragmentos/tesinas/TesinaDelgadoSamanthaFinal5295.pdf

Denwa. (2020). *TELÉFONO IP DW-210P*. Obtenido de https://www.denwaip.com/DATASHEET-DW-210P-ESP.pdf

Fortinet. (2019). One Next-Generation Firewall Designed to Protect an Expanding Attack Surface — the FortiGate NGFW.

Fortinet. (2020a). *File-filter*. Obtenido de https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/610893/file-filter

Fortinet. (2020b). *FortiClient licensing and support*. Obtenido de https://kb.fortinet.com/kb/documentLink.do?externalID=FD48147

Fortinet. (2020c). *FortiGate-to-third-party*. Obtenido de https://docs.fortinet.com/document/fortigate/latest/administration-guide/822881/fortigate-to-third-party

Fortinet. (2020d). *Información general de las unidades de procesamiento seguro*. Obtenido de https://www.fortinet.com/lat/products/fortigate/fortiasic

Fortinet. (2020e). *Next-Generation Firewall (NGFW)*. Obtenido de https://www.fortinet.com/lat/products/next-generation-firewall#overview1

Fortinet. (2020f). *Policy routing*. Obtenido de https://docs.fortinet.com/document/fortigate/6.0.0/handbook/34912/policy-routing

Fortinet. (2020g). *Seguridad para la empresa*. Obtenido de https://www.fortinet.com/lat/solutions/enterprise-midsize-business/enterprise-security

Fortinet. (2020h). *User and User Group*. Obtenido de https://docs.fortinet.com/document/fortigate/6.0.0/handbook/518646/users-and-user-groups

Gartner. (2020). *Magic Quadrant for Network Firewalls.* Obtenido de https://www.gartner.com/doc/reprints?id=1-24KX0CRM&ct=201111&st=sb?utm_source=marketo&utm_medium=email&utm_campaign=2020-12-10%2005:58:58-Global-DA-EN-20-10-08-7014u000001Z8CVAA0-P1-Strata-2020-gartner-mq-for-firewalls

Gómez Vieites, Á. (2019). Tipos de Ataques e Intrusos en las Redes Informáticas. 13. Obtenido de https://www.edisa.com/wp-content/uploads/2019/08/ponencia_-_tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

HP. (2019). *HP PageWide Enterprise Color MFP 586 series*. Obtenido de https://www8.hp.com/h20195/v2/getpdf.aspx/4aa6-4502enuc.pdf

Inteco. (2012). *Implantación de un SGSI en la empresa.* Obtenido de https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISO/IEC. (2013). *International Standard ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls.*

ISO/IEC. (2018). *International Standard ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary.* Obtenido de https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

Khan, M. S., Siddiqui, S., & Ferens, K. (2017). A Cognitive and Concurrent Cyber Kill Chain Model. *Computer and Network Security Essentials*, 585-602. doi:10.1007/978-3-319-58424-9

Khelf, R., & Ghoualmi-Zine, N. (2019). IPsec/Firewall Security Policy Analysis: A Survey. *2018 International Conference on Signal, Image, Vision and their Applications, SIVA 2018*, 1-7. doi:10.1109/SIVA.2018.8660973

Lenovo. (2015). *Lenovo ThinkServer TS150*. Obtenido de https://download.lenovo.com/parts/ThinkCentre/ts150_overview.pdf

Lenovo. (2020). *Servidor en torre ThinkSystem ST50*. Obtenido de https://www.lenovo.com/ec/es/data-center/servers/towers/ThinkSystem-ST50/p/77XX7TRST51

Lyons, C. (2012). Enterprise IT Security Architecture Security Zones: Network Security Zone Standards. Obtenido de https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/network_security_zone_standards.pdf

Maraj, A., Jakupi, G., Rogova, E., & Grajqevci, X. (June de 2017). Testing of Network Security Systems Through DoS Attacks. *2017 6th Mediterranean Conference on Embedded Computing, MECO 2017 - Including ECYPS 2017, Proceedings*, 11-15. doi:10.1109/MECO.2017.7977239

Mero Garcia, A. F. (2016). *Implantación de un Sistema de Gestión de Seguridad de Información (SGSI) En el Distrito de Salud 13D04 24 de Mayo – Santa Ana – Olmedo – Salud de la Provincia de Manabí.* Pontificia Universidad Católica del Ecuador. Obtenido de http://repositorio.puce.edu.ec/handle/22000/11322

Mikrotik. (2013). *RB1100AHx2*. Obtenido de https://mikrotik.com/product/RB1100AHx2

Mikrotik. (2020). *Intelligent Firewall for complete data confidence* . Obtenido de https://i.mt.lv/pdf/archive/routeros_firewall.pdf

MINTEL. (2020). *Ciclo de Deming (PDCA).* Obtenido de https://www.gobiernoelectronico.gob.ec/ciclo-de-deming-pdca/

ON2IT. (2020). *Zero Trust Strategy*. Obtenido de https://on2it.net/en/zero-trust/

Palo Alto Networks. (2015). Palo Alto Networks Single-Pass Architecture: Integrated, Prevention-Oriented Security For.

Palo Alto Networks. (2018). *How to Configure Internal GlobalProtect Only*. Obtenido de https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClH1CAK

Palo Alto Networks. (2019). PAN-OS 8.1 Courseware Version B.

Palo Alto Networks. (2020a). *Best Practice Assessment (BPA).* Obtenido de https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technology-solutions-briefs/best-practice-assessment-solution-brief.pdf

Palo Alto Networks. (2020b). *Catálogo de productos de Palo Alto Networks*. Obtenido de https://www.paloaltonetworks.es/resources/ebooks/portfolio-product-brochure

Palo Alto Networks. (2020c). *Create Best Practice Security Profiles for the Internet Gateway*. Obtenido de https://docs.paloaltonetworks.com/best-practices/10-0/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles.html

Palo Alto Networks. (2020d). *Dashboard Principal Cliente AKEA S.A*. Obtenido de https://186.47.74.254/?#dashboard::vsys1

Palo Alto Networks. (2020e). *PA-220 Datasheet.* Obtenido de https://www.paloaltonetworks.com/resources/datasheets/pa-220-specsheet

Palo Alto Networks. (2020f). *PBF*. Obtenido de https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/policy/policy-based-forwarding/pbf

Palo Alto Networks. (2020g). *Palo Alto Networks ML-Powered Next-Generation Firewall Specifications and Features Summary.*

Palo Alto Networks. (2020h). *Set Up Site-to-Site VPN*. Obtenido de https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/vpns/site-to-site-vpn-overview.html

Palo Alto Networks. (2021). *Customer Support Portal*. Obtenido de https://support.paloaltonetworks.com/Support/Index

Puga Hermosa, C. d. (2017). *Propuesta de un Modelo de Gestión para Mejorar la Capacidad de Gestión de la Seguridad de la Información de una Institución Financiera del Sector Público.* Universidad de las Americas. Obtenido de http://dspace.udla.edu.ec/bitstream/33000/8282/1/UDLA-EC-TMGSTI-2017-21.pdf

Samote, A. (2020). Network Security Reference. Obtenido de https://www.fortinet.com/content/dam/fortinet/assets/document-library/ra-network-security-reference-architecture.pdf

Soewito, B., & Andhika, C. (2019). Next Generation Firewall for Improving Security in Company and IoT Network. *Proceedings - 2019 International Seminar on Intelligent*

Technology and Its Application, ISITIA 2019, 205-209. doi:10.1109/ISITIA.2019.8937145

Tarnowski, I. (2017). How to use cyber kill chain model to build cybersecurity? 22. Obtenido de https://www.eunis.org/download/TNC2017/TNC17-IreneuszTarnowski-cybersecurity.pdf

Tarun, Y., & Rao, A. M. (2015). Technical Aspects of Cyber Kill Chain. *Security in Computing and Communications - Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings*, 438-452. doi:10.1007/978-3-319-22915-7

Ubiquiti. (2019). *UniFi AC.* Obtenido de https://dl.ubnt.com/datasheets/unifi/UniFi_AC_APs_DS.pdf

Uctu, G., Alkan, M., Dogru, I. A., & Dorterler, M. (2019). Perimeter Network Security Solutions: A Survey. *3rd International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2019 - Proceedings*. doi:10.1109/ISMSIT.2019.8932821

Uttarwar, V. U., & Kalia, A. A. (2019). Latest Trend in Network Security as Zero Trust Security Model. *National Journal of Computer and Applied Science*, 5-8. Obtenido de http://www.njcas.co.in/index.php/njcas/article/download/30/33

Weever, C. D., & Andreou, M. (2020). Zero Trust Network Security Model in containerized environments. 1-12. Obtenido de https://work.delaat.net/rp/2019-2020/p01/report.pdf

Yeastar. (2014). *MyPBX - Embedded Hybrid IP-PBX for Small Businesses*. Obtenido de http://www.bcroee.pt/ficheiros/file/Home/Catalogos/MyPBX_Standard&Pro_Datasheet_en.pdf

ANEXOS

Anexo A: Política de seguridad informática AKEA S.A

Anexo B: Autorización de uso de documento de Políticas de seguridad informática AKEA S.A

Anexo C: ISO/IEC 27002:2013. 14 Dominios, 35 Objetivos de Control y 114 Controles

Anexo D: Palo Alto Networks Product Summary Specsheet

Anexo E: Cotización Referencial QUO-7192879-G1Q2K9-0-AKEA

Anexo F: Best Practice Assessment PA-AKEA_2021-02-22