

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
Facultad de Ingeniería en Electricidad y Computación



MAESTRÍA EN SEGURIDAD INFORMÁTICA APLICADA
PROMOCIÓN IV

**“IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD
PERIMETRAL EN UNA EMPRESA PYME DESPUÉS DE
REALIZADA UNA AUDITORÍA INFORMÁTICA”**

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

AUTOR

ÁNGEL FERNANDO LACERNA CÓRDOVA

GUAYAQUIL – ECUADOR

AÑO: 2021

AGRADECIMIENTO

Agradezco primeramente a Jehová Dios por haberme otorgado la capacidad de aprender nuevos conocimientos y transmitirlos a otras personas, al director del programa MSIA Ms. Lenín Freire, a los profesores y todo el personal de MSIA/MSIG, también a todos los excelentes profesionales, colegas y amigos que tuve la oportunidad de interactuar en este programa académico.

DEDICATORIA

Este trabajo está dedicado especialmente a mi familia: mi esposa Gabriela y mi hijo Matías por darme tantas alegrías y las ganas de luchar por ellos, a mi madre Diana que ha sido un pilar fundamental en mi desarrollo personal, académico y profesional, también a mi hermana y sobrinos.

A handwritten signature in blue ink, appearing to be 'Julio César', written in a cursive style.

TRIBUNAL DE SUSTENTACIÓN

MSIG. Lenin Freire Cobo

COORDINADOR MSIA

MSIG. Juan Carlos García Plúas

PROFESOR MSIA

RESUMEN

En el presente trabajo se documentó el proceso de la implementación de una solución de seguridad perimetral a una empresa PYME que tiene dos locales comerciales ubicados en un sector estratégico de la ciudad, la misma que luego de realizada una auditoría informática los accionistas de la empresa decidieron ejecutar algunas de las recomendaciones como el crear un túnel privado virtual por Internet a través de una VPN y poder intercomunicar sus dos locales.

En el primer capítulo se muestra una descripción breve, se expone el problema y se explica la solución recomendada que se propuso en lo referente a la solución de seguridad perimetral.

En el segundo capítulo se muestra a detalle el desarrollo de la solución propuesta, primero se hace un análisis de la situación actual y luego se explica y define la solución que se aplicó; para esto se explica todos los cambios que tuvieron que realizarse, así como el proceso de configuración de la solución de seguridad perimetral, y al finalizar este capítulo se describe brevemente los ajustes de configuraciones que se realizaron en los diferentes dispositivos finales de la empresa.

El tercer capítulo muestra el análisis de resultados basados en la aplicación de la solución de seguridad el perimetral y los cambios efectuados a nivel de conectividad que afectaron a todos los equipos de la empresa.

INDICE GENERAL

AGRADECIMIENTO	i
DEDICATORIA	ii
TRIBUNAL DE SUSTENTACIÓN	iii
RESUMEN.....	iv
INDICE GENERAL	vi
ABREVIATURAS Y SIMBOLOGÍA	ix
INDICE DE TABLAS	x
INDICE DE FIGURAS.....	xi
INTRODUCCIÓN.....	xiii
CAPÍTULO 1.....	1
GENERALIDADES	1
1.1. DESCRIPCIÓN DEL PROBLEMA	1
1.2. SOLUCIÓN PROPUESTA.....	5
CAPÍTULO 2.....	7
DESARROLLO DE LA SOLUCIÓN	7

2.1.	ANÁLISIS DE LA SITUACIÓN ACTUAL.....	7
2.2.	INVENTARIO FÍSICO/LÓGICO	9
2.3.	DEFINICIÓN DE LA SOLUCIÓN	13
2.3.1.	DESCRIPCION DE FIREWALL XG106	13
2.3.2.	SEGMENTACIÓN DE LA RED.....	15
2.3.3.	CONFIGURACIÓN DE SOLUCIÓN FIREWALL	17
2.3.3.1.	VERIFICACIÓN DE ESTADO Y LICENCIAMIENTO DE FIREWALL.	17
2.3.3.2.	CONFIGURACIÓN INICIAL DE LOS EQUIPOS FIREWALL.	18
2.3.3.3.	ESTABLECIMIENTO DE CONFIGURACIÓN PARA VPN.	32
2.3.3.4.	ESTABLECIMIENTO DE REGLAS DE FIREWALL PARA TRÁFICO VPN.	36
2.3.4.	AJUSTE DE CONFIGURACIONES A LOS DISPOSITIVOS FINALES.....	36
	CAPÍTULO 3.....	39
	RESULTADO DE LA SOLUCIÓN	39
3.1.	ANÁLISIS DE RESULTADOS	39

3.1.1.	TÚNEL VPN PUNTO A PUNTO.	39
3.1.2.	APLICACIÓN DE NUEVO SEGMENTO DE RED.....	41
3.1.3.	PRUEBAS DE CONECTIVIDAD DE LA RED.	42
3.1.4.	VERIFICACIÓN DE ANCHO DE BANDA.	43
	CONCLUSIONES Y RECOMENDACIONES.	44
	BIBLIOGRAFÍA.....	47

ABREVIATURAS Y SIMBOLOGÍA

AP	Punto de acceso (por sus siglas en inglés)
DHCP	Protocolo de configuración dinámica de host (por sus siglas en inglés)
DVR	Grabador de video digital (por sus siglas en inglés)
HTTPS	Protocolo seguro de transferencia de hipertexto (por sus siglas en inglés)
ICMP	Protocolo de control de mensajes de Internet (por sus siglas en inglés)
IP	Protocolo de Internet (por sus siglas en inglés)
IPSEC	Seguridad del protocolo de Internet (por sus siglas en inglés)
ISP	Proveedor de servicio de Internet (por sus siglas en inglés)
LAN	Red de área local (por sus siglas en inglés)
PDF	Formato de documentos portátiles (por sus siglas en inglés)
PtP	Red de punto a punto (por sus siglas en inglés)
PYME	Pequeña y media empresa
VPN	Red privada virtual (por sus siglas en inglés)
WEB	Red o telaraña (por sus siglas en inglés)
WLAN	Red de área local inalámbrica (por sus siglas en inglés)

INDICE DE TABLAS

Tabla 1: Inventario físico de equipos	11
Tabla 2: Inventario lógico de aplicaciones	13
Tabla 3: Características de rendimiento XG106.....	15
Tabla 4: Esquema de segmentación.....	16
Tabla 5: Asignación de direccionamiento IP	16
Tabla 6: Contenido físico del producto firewall.....	18
Tabla 7: Características de Network Protection	26
Tabla 8: Parámetros básicos de configuración VPN	33

INDICE DE FIGURAS

Figura 1.1: Diseño lógico de red PtP	2
Figura 1.2: Ancho de banda Internet local sucursal	3
Figura 1.3: Diseño de red actual	5
Figura 2.1: Especificaciones Sophos XG106	14
Figura 2.2: Licenciamiento/suscripción de producto firewall.....	18
Figura 2.3: Registro de producto firewall.....	19
Figura 2.4: Prueba de conectividad inicial ping	20
Figura 2.5: Página de inicialización de producto firewall	21
Figura 2.6: Requisitos mínimo de credenciales.....	22
Figura 2.7: Establecimiento de credenciales al producto firewall	22
Figura 2.8: Aceptación del acuerdo de licencia.....	23
Figura 2.9: Establecimiento de zona horaria	24
Figura 2.10 Configuración básica completada	25
Figura 2.11: Configuración básica de red inicial.....	27
Figura 2.12: Configuración de respaldos y notificaciones de correo	27
Figura 2.13: Configuración final de inicialización del firewall.....	28
Figura 2.14: Prueba de conectividad ping del firewall	29
Figura 2.15: Ingreso por primera vez a consola de administración	29
Figura 2.16: Personalización de parámetros de red.....	30
Figura 2.17: Prueba de conectividad ping de firewall.....	31
Figura 2.18: Consola de administración de firewall.....	31

Figura 2.19: Definición de red LAN local y remota	32
Figura 2.20: Asistente de configuración VPN	33
Figura 2.21: Definición de tipo de conexión VPN	34
Figura 2.22: Resumen de configuraciones VPN IPsec	34
Figura 2.23: Conexión IPsec aplicada para local 1	35
Figura 2.24: Estado activo de conexión IPsec para local 1	35
Figura 2.25: Reglas de tráfico para red local y remota	36
Figura 3.1: Conexión de túnel VPN activado en local 1	40
Figura 3.2: Conexión de túnel VPN activado en local 2	40
Figura 3.3: Reporte de uso de túnel VPN	40
Figura 3.4: Validación de reglas de tráfico del firewall	41
Figura 3.5: Validación de reglas de tráfico del firewall	41
Figura 3.6: Prueba de conectividad a dispositivo final	42
Figura 3.7: Conectividad entre dispositivos de ambos segmentos de red	43
Figura 3.8: Test de velocidad de ancho de banda de Internet	43

INTRODUCCIÓN

Mejorar y asegurar el flujo de información en una empresa comercial PYME para sus procesos de ventas, mediante la implementación de una red virtual privada que permita a sus locales reducir los tiempos de acceso a su sistema de información de negocio brindando una mejor experiencia de atención al cliente

Con la llegada de la pandemia de COVID19 [1], la empresa comercial PYME tuvo que ofrecer nuevas formas de atención a sus clientes para recuperarse del impacto económico que esta emergencia sanitaria ha provocado en todos los sectores comerciales a nivel mundial.

CAPÍTULO 1

GENERALIDADES

1.1. DESCRIPCIÓN DEL PROBLEMA

La empresa PYME se dedica a la comercialización al por mayor y menor de componentes y accesorios electrónicos, accesorios de computación, audio y video, entre otros dispositivos desde hace más de 25 años en la ciudad de Guayaquil y cuenta con dos locales ubicados en un sector estratégico de la ciudad en el que se encuentran otros competidores que ofrecen los mismos productos, por lo que la experiencia de atención al cliente es la prioridad en todos los procesos de negocio de la empresa para la satisfacción de sus clientes existentes, como para la atracción de nuevos potenciales clientes debido a la alta competencia de empresas dedicadas al mismo nicho de mercado de la empresa comercial PYME.

Para automatizar sus procesos claves de negocio como contabilidad, ventas, facturación e inventario la empresa adquirió en el año 2016 el sistema de información VMULTINEG con soporte de un proveedor local [2], lo que le llevó a implementar una red inalámbrica PtP (punto a punto por sus siglas en inglés) entre sus dos locales para compartir el tráfico de datos y de Internet desde uno de los dos locales utilizando dos dispositivos antenas radiales de marca Ubiquiti [3].

En la Figura 1.1 se puede apreciar el diseño original de la red inalámbrica entre sus dos locales.

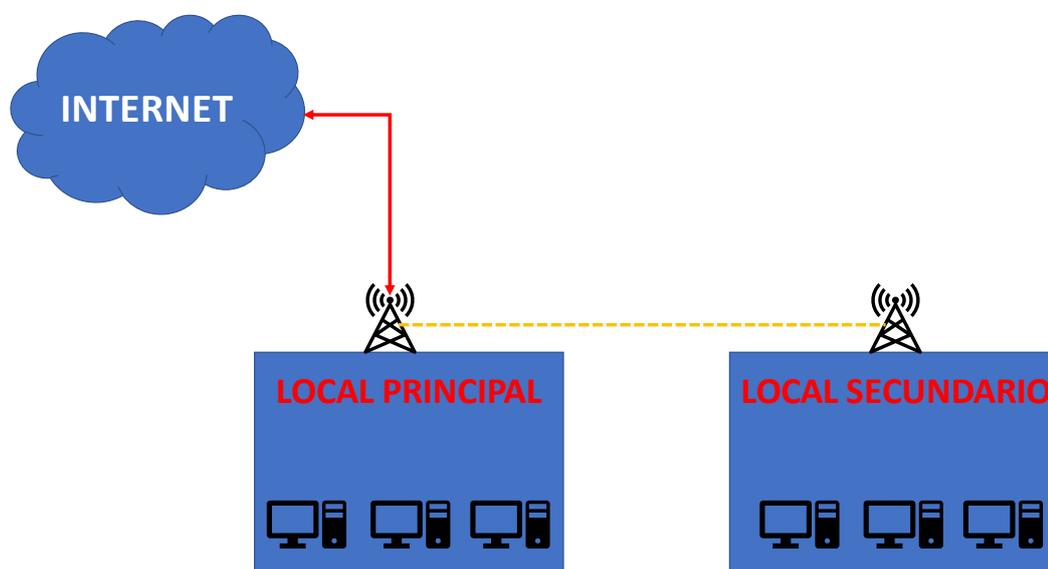


Figura 1.1: Diseño lógico de red PtP

Fuente: Autor

A pesar de que el ancho de banda de Internet es de 20 Mbps con compartición 2:1 para el local principal, esta solución no dio los resultados esperados ya que experimentaron al poco tiempo de su implementación una lentitud excesiva en el acceso a su sistema de información, acentuándose el problema en la sucursal donde no está el servidor de aplicaciones y base de datos.

La Figura 1.2 muestra la medición del ancho de banda [4], y se observa una baja considerablemente con el diseño original de red PtP por medio de las antenas Ubiquiti [3].



Figura 1.2: Ancho de banda Internet local sucursal

Fuente: Autor

Este problema ha ocasionado que sus procesos como la facturación se estén manejando de manera manual, además de no contar con información actualizada del stock en el inventario al momento de ofrecer o vender un producto; incluso la pérdida de clientes que se ven atraídos

por otros locales del sector que ofrecen una mayor rapidez en la consulta de precios, stock y sustitutos de productos.

Ante esta situación, la empresa PYME sin el debido asesoramiento informático decidió desconectar el enlace de comunicación entre las antenas radiales para solucionar en parte el problema de lentitud en sus comunicaciones. Este nuevo escenario obligó a que cada local tenga contratado Internet de tipo “hogar” con diferentes ISP para manejar las consultas con sus proveedores mayoristas y las redes sociales que maneja la empresa en su proceso de ventas; sin embargo, ya no se contaba con la comunicación de su sistema de información entre ambos locales, llevando a que muchos procesos se mantengan de manera manual.

Si bien es cierto, el tener enlaces de Internet separados para local resolvió el problema de lentitud en la navegación web, esto afectó al diseño original de red inalámbrica entre sus locales como se puede apreciar en la Figura 1.3, pero cabe recalcar que no lograron agilizar sus procesos claves de negocio ni tener una red intercomunicada entre sus locales por lo que muchas de las tareas de comunicación entre sus locales las tienen que realizar por llamada telefónica, aplicaciones de mensajería instantánea

como Whatsapp e incluso usando dispositivos de comunicación del tipo transmisor-receptor portátiles.

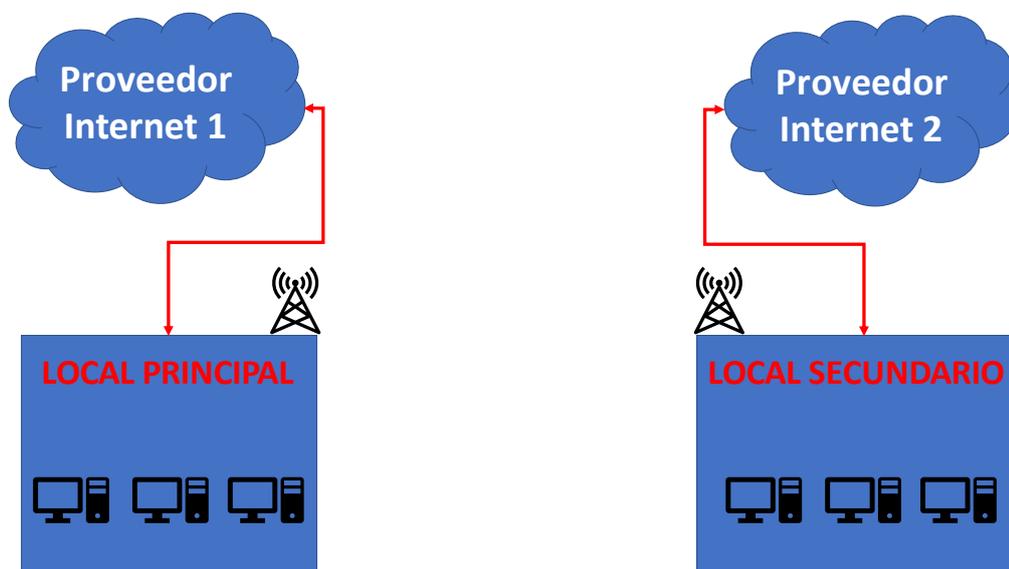


Figura 1.3: Diseño de red actual

Fuente: Autor

1.2. SOLUCIÓN PROPUESTA

Es importante señalar que la empresa no cuenta con un departamento de informática y que las condiciones medioambientales en las que se encontraron ubicadas las antenas no es la mejor, ya que están expuestas al aire libre y no tienen un punto fijo que permita la visibilidad punto a punto, así como también se ha incrementado considerablemente en el sector un gran número de otras antenas que interfieren en la señal de estas.

Para lograr tener un mejor entendimiento de los problemas presentados en el proceso de ventas de la empresa comercial PYME, se propuso realizar una auditoría informática [5] para evidenciar lo que realmente está sucediendo en torno a sus equipos físicos, sus aplicaciones y la conectividad dentro de la empresa.

Se propuso además el reemplazo de las antenas radiales por dos dispositivos de seguridad perimetral firewall que permitan la conectividad de una red privada virtual VPN [6] punto a punto a través de Internet para que el flujo del tráfico de la información sea continuo y no sufra los problemas de lentitud presentados en la descripción del problema.

CAPÍTULO 2

DESARROLLO DE LA SOLUCIÓN

2.1. ANÁLISIS DE LA SITUACIÓN ACTUAL

Los resultados de la auditoría informática [5] confirmaron que en la empresa existen varios problemas a nivel físico y lógico que deberán ser corregidos para poder mejorar sus procesos de negocio y obtener mayor rentabilidad en sus operaciones.

En este informe solo se documentará el problema relacionado con la conectividad y el entorno a los equipos informáticos de la empresa. Los principales hallazgos que se evidenciaron fueron:

- El esquema de la red es plano y usa un segmento abierto de tipo C 192.168.100.x/24.
- Usan como red WLAN la que estableció el ISP y se comparte el SSID/clave tanto a los usuarios internos como clientes que llegan a los locales.

- Los equipos de red WLAN son de uso doméstico.
- Las credenciales de acceso a la administración de los equipos de red WLAN se encuentran en los valores por defecto del fabricante.
- Los equipos informáticos (servidor, antenas Ubiquiti) de la infraestructura de la empresa no tiene soporte técnico con fabricante o un canal autorizado.
- Se realizan mantenimientos físicos a los equipos informáticos cada año, pero no se tienen informes ni documentación de soporte de los trabajos efectuados.
- No existe un área climatizada para los equipos de comunicaciones y servidores.
- Los puntos de red no están certificados.
- El cableado en los locales no es estructurado.
- El cableado hacia el exterior para la interconexión de las antenas Ubiquiti está expuesto a la intemperie.
- Al restablecer el enlace entre las antenas Ubiquiti se confirmó que el ancho de banda del Internet en los locales se saturaba.
- No tienen la documentación de la configuración de las antenas Ubiquiti ni tampoco cuentan con las credenciales de acceso a dichos dispositivos.

- Se verificó que las antenas Ubiquiti no tenían habilitadas las credenciales de acceso por defecto.
- No tienen licenciamiento en sistema operativo y aplicaciones ofimáticas en la mayoría de los equipos.
- No tienen software antivirus en todas las estaciones de trabajo de los locales.

2.2. INVENTARIO FÍSICO/LÓGICO

Se realizó el inventario físico y lógico de los equipos tecnológicos y las aplicaciones que utiliza la empresa en ambos locales comerciales. Respecto a la parte física, la información que se pudo verificar se muestra en la siguiente tabla, la misma que describe los elementos que se encontraron, las cantidades, observaciones y la ubicación de dicho elemento dentro de la empresa.

DESCRIPCIÓN	CANTIDAD	OBSERVACIONES	UBICACIÓN
Servidor DELL T30	1	Servidor de aplicaciones, facturación electrónica, base datos, sistema de información	Local 1
Computadoras escritorio	3	Estaciones de trabajo administrativas	Local 1 y 2
Puntos de venta	6	PCs de escritorio de atención al cliente final.	Local 1 y 2
Impresora Epson L4160	2	Impresora de uso compartido	Local 1 y 2
Equipo DVR	2	Equipo de grabación de video para 32 cámaras análogas.	Local 1 y 2
Switch TP-Link TL-SF1016D	1	Conmutador de escritorio de 16 puertos 10/100 Mbps no gestionable	Local 1
Switch TP-Link TL-SG116		Conmutador de escritorio de 16 puertos 10/100/1000 Mbps no gestionable	Local 2

DESCRIPCIÓN	CANTIDAD	OBSERVACIONES	UBICACIÓN
Punto de Acceso Ubiquiti NanoStation M2	2	Antena para acceso punto a punto con local sucursal.	Local 1 y 2
Punto de Acceso	2	Dispositivos para conectividad WLAN en cada local.	Local 1 y 2

Tabla 1: Inventario físico de equipos

Fuente: Autor

De manera similar se realizó el inventario lógico, el mismo que se describe las aplicaciones que utiliza la empresa, el uso que se le da, la cantidad y observaciones; esta información se la muestra en la siguiente tabla:

APLICACIÓN	DESCRIPCIÓN	CANTIDAD	OBSERVACIONES
Microsoft Windows 10	Sistema operativo de POS y PCs administrativas	9	Se evidenció que las estaciones de trabajo no tenían licenciamiento legal.
Microsoft Windows Server 2012 R2	Sistema operativo de Servidor de	1	Se evidenció que el servidor no contenía licenciamiento legal.

APLICACIÓN	DESCRIPCIÓN	CANTIDAD	OBSERVACIONES
	aplicaciones, base de datos.		
Microsoft Office 2016 Professional Plus	Utilitario de ofimática	9	Se evidenció que la aplicación de ofimática de las estaciones de trabajo no tenía licenciamiento legal.
Consola de antivirus ESET	Consola de antivirus centralizada	1	Licenciado
Clientes de antivirus ESET	Cliente de antivirus ESET	4	Licenciado solo en el local 1.
VMultineg	Sistema core de negocio (facturación, inventario, cuentas por cobrar, cuentas por pagar)	1	Instalado en el servidor DELL T30, con soporte del fabricante del software.
Sistema de facturación electrónica	Sistema de facturación electrónica instalado en servidor local.	1	Instalado en el servidor DELL T30, con soporte del fabricante del software.
Correo electrónico	Sistema de correo electrónico en la	1	Lo usan solo para el envío y recepción de documentos de

APLICACIÓN	DESCRIPCIÓN	CANTIDAD	OBSERVACIONES
	nube con dominio propio.		facturación electrónica.

Tabla 2: Inventario lógico de aplicaciones

Fuente: Autor

2.3. DEFINICIÓN DE LA SOLUCIÓN

De acuerdo con los datos evidenciados en la auditoría informática [5], se estableció el plan de acción para diseñar una solución de seguridad perimetral entre ambos locales, el mismo que entre sus características principales estaría el ser escalable, modular y confiable para crecimiento futuro en los nuevos proyectos de TI que implementen en la empresa.

2.3.1. DESCRIPCION DE FIREWALL XG106

Según el portal del fabricante los equipos de la serie XG se caracterizan por “expone riesgos ocultos, bloquea amenazas desconocidas y responde automáticamente a incidentes” [6]. El equipo de seguridad perimetral escogido para la implementación de la solución de seguridad perimetral es el Sophos XG 106, el mismo que “ofrece una buena relación precio-rendimiento y diversas opciones de conectividad integradas y complementarias” [6].

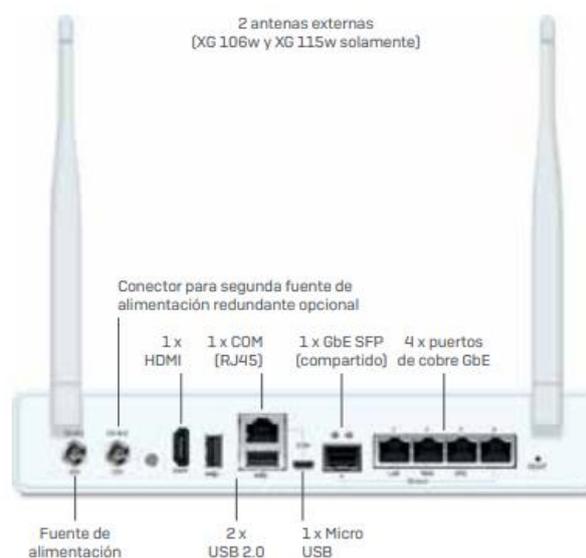


Figura 2.1: Especificaciones Sophos XG106

Fuente: [6]

En la siguiente tabla se puede observar las características principales del modelo XG106.

CARACTERÍSTICAS DE RENDIMIENTO	VALORES
Rendimiento del Firewall	3550 Mbps
Rendimiento del IPS	490 Mbps
Rendimiento del NGFW	400 Mbps

CARACTERÍSTICAS DE RENDIMIENTO	VALORES
Rendimiento de la protección contra amenazas	150 Mbps
Conexiones simultáneas	1570000
Conexiones nuevas/seg.	14700
Rendimiento de VPN IPsec	330 Mbps

Tabla 3: Características de rendimiento XG106

Fuente: [6]

2.3.2. SEGMENTACIÓN DE LA RED

Como el esquema tiene un direccionamiento IP (192.168.100.x/24) que se evidenció es plano y no está definido de manera organizada, se optó por realizar un rediseño de la red separando las redes de los locales con dos segmentos de redes más pequeños, además se realizó la reserva de las cinco primeras direcciones IP para direccionamiento estático para los equipos que tienen esta necesidad y el resto de las direcciones IP del segmento se utilizaría para direccionamiento dinámico DHCP.

La Tabla 4 muestra los cambios en la segmentación de red recomendados y la Tabla 5 la forma en que se distribuirían las direcciones IP.

PARÁMETROS DE RED	VALORES
SEGMENTO DE RED	<ul style="list-style-type: none"> • 192.168.110.0 (local 1) • 192.168.120.0 (local 2)
MASCARA DE RED:	<ul style="list-style-type: none"> • 255.255.255.224

Tabla 4: Esquema de segmentación

Fuente: Autor

DIRECCIÓN IP	DESCRIPCIÓN
1	Equipo UTM
2	Equipo AP
3	DVR
4	Servidor (local principal) PC administración (local sucursal)
5	Libre
6 ...30	Libres para DHCP

Tabla 5: Asignación de direccionamiento IP

Fuente: Autor

2.3.3. CONFIGURACIÓN DE SOLUCIÓN FIREWALL

En esta sección se muestra los pasos que se llevaron a cabo para configurar los equipos firewall de seguridad perimetral. Las actividades que se ejecutaron fueron las siguientes:

- Verificación de estado y licenciamiento de los equipos firewall.
- Configuración inicial de los equipos firewall.
- Establecimiento de configuración para túnel VPN.
- Establecimiento de reglas de firewall para tráfico VPN.

2.3.3.1. VERIFICACIÓN DE ESTADO Y LICENCIAMIENTO DE FIREWALL.

El primer paso fue verificar el estado de los equipos firewall, estos se encontraban en dos cajas selladas y se realizó la apertura de estas en presencia del personal designado por la empresa PYME.

ITEM	OBSERVACIÓN
Dispositivo firewall	Uno por caja
Adaptador de poder 110v	Uno por caja
Cable de red categoría 5e	Uno por caja

ITEM	OBSERVACIÓN
Cable serial USB	Uno por caja
Manuales de especificaciones y garantía	Uno por caja

Tabla 6: Contenido físico del producto firewall.

Fuente: Autor

2.3.3.2. CONFIGURACIÓN INICIAL DE LOS EQUIPOS FIREWALL.

Para proceder a configurar los equipos, primero se realizó la verificación de las licencias y suscripciones del producto que serían cargadas a cada dispositivo firewall. Estas licencias habían llegado vía correo electrónico en archivo PDF y se pueden observar en la siguiente figura:

Product	Term (Months)	Serial Number
XG 106 rev.1 Security Appliance (EU/UK/US power cord) (SKU: XG1ZTCHEK)		C1C1073B [REDACTED]
XG 106 rev.1 Security Appliance (EU/UK/US power cord) (SKU: XG1ZTCHEK)		C1C1073B [REDACTED]

Product	Term (Months)	License Key
XG 106 Enhanced Support - 12 MOS (SKU: EN1Z1CEAA)	12	ESUPXG10612: [REDACTED]
XG 106 Enhanced Support - 12 MOS (SKU: EN1Z1CEAA)	12	ESUPXG10612: [REDACTED]
XG 106 Network Protection - 12 MOS (SKU: XN1Z1CSAA)	12	NWPXG10612: [REDACTED]
XG 106 Network Protection - 12 MOS (SKU: XN1Z1CSAA)	12	NWPXG10612: [REDACTED]

Figura 2.2: Licenciamiento/suscripción de producto firewall

Fuente: Documento de licencia electrónica SOPHOS

Con estos datos se procedió a la creación de un usuario utilizando una cuenta de correo corporativo de la empresa PYME en el portal del fabricante para poder ingresar las licencias adquiridas para cada equipo firewall. Completado este proceso en el portal del fabricante, se realizó la agregación de las licencias/suscripción como se muestra en la Figura 2.3.

Ver dispositivos

A continuación se muestra una lista con todos los dispositivos que ha registrado usted /su empresa. Haga clic en Descargar para descargar software y en Suscribirse para ver y cambiar las suscripciones para un dispositivo.

Opciones de búsqueda

Modelo, número de serie o Información [Búsqueda avanzada](#) [Borrar](#)

Mostrando entradas de 1 a 2 de 2

10 |< < > >|

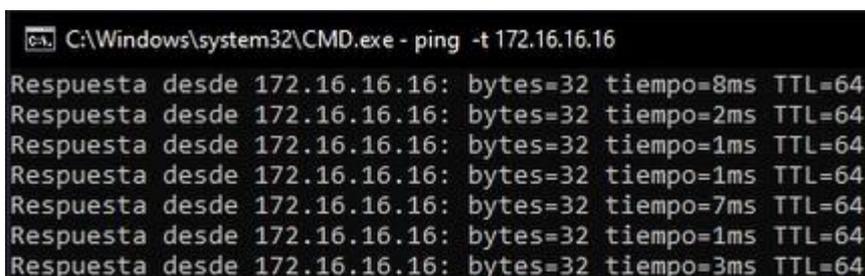
Nº de serie	Fecha de registro	Tipo de producto	Modelo	Acciones	¿Mostrar?
C1C1073 crear información adicional		UTM	XG106	Suscribir Descargar	<input checked="" type="checkbox"/>
C1C1073 crear información adicional		UTM	XG106	Suscribir Descargar	<input checked="" type="checkbox"/>

Figura 2.3: Registro de producto firewall

Fuente: Portal de licencias de SOPHOS

Finalizado el proceso de licenciamiento/suscripción en el portal del fabricante se dio paso a realizar la conexión del adaptador de poder a una toma de corriente proporcionada por la empresa PYME y se conectó al dispositivo firewall a un equipo laptop para la respectiva inicialización del producto.

Se verificó en el manual de configuración que estaba en la caja de los equipos firewall los parámetros de red por defecto y se evidenció que el mismo era 172.16.16.16, con este dato se configuró la tarjeta de red del equipo laptop con una dirección IP del segmento 172.16.16.x/24 y se realizó pruebas de conectividad ICMP utilizando la utilidad ping del sistema operativo para proceder con la configuración de los dispositivos firewall. La Figura 2.4 muestra que el dispositivo firewall respondía exitosamente a la prueba de conectividad inicial.



```
C:\Windows\system32\CMD.exe - ping -t 172.16.16.16
Respuesta desde 172.16.16.16: bytes=32 tiempo=8ms TTL=64
Respuesta desde 172.16.16.16: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.16.16: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.16.16: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.16.16: bytes=32 tiempo=7ms TTL=64
Respuesta desde 172.16.16.16: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.16.16: bytes=32 tiempo=3ms TTL=64
```

Figura 2.4: Prueba de conectividad inicial ping

Fuente: Autor

Una vez comprobado que la conectividad entre la laptop y el dispositivo firewall estaba correctamente establecida se ingresó a través de un navegador de Internet a la dirección IP 172.16.16.16:4444 como se muestra a continuación:

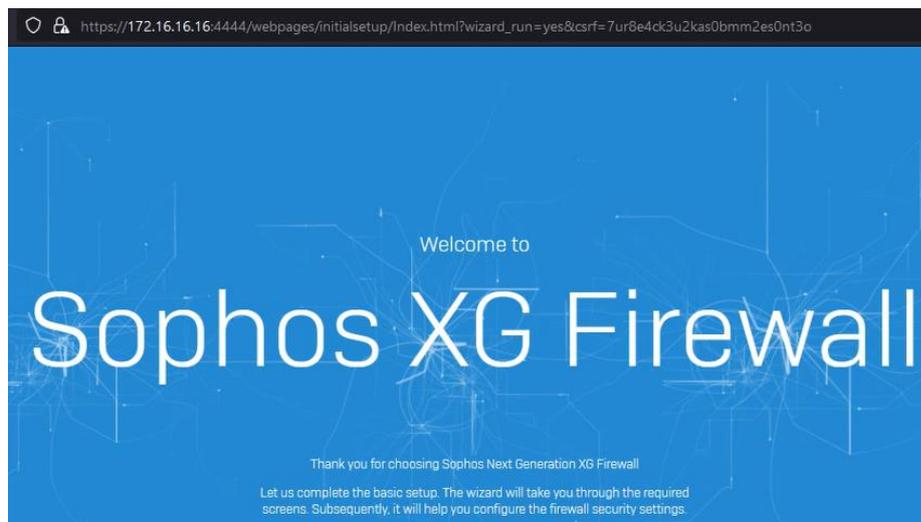


Figura 2.5: Página de inicialización de producto firewall

Fuente: Autor

Para iniciar se ingresó las credenciales por defecto del equipo según las especificaciones del fabricante y paso seguido apareció la pantalla de establecimiento de credenciales de usuario. La Figura 2.6 muestra la recomendación del fabricante en el proceso de inicialización del producto de establecer credenciales con las siguientes características:

- Al menos 8 caracteres de longitud.
- Al menos 1 carácter en mayúsculas.
- Al menos 1 carácter en minúsculas.
- Al menos 1 dígito numérico.

Basic configuration

You can log in to the firewall only through the administrator account currently. You must create a password before you continue. We recommend that you use a long password, with a mix of letters, numbers and special characters to make it strong. If you have an existing configuration that you wish to use, or an existing firewall that you wish to connect to in HA, choose the relevant options below.

[Restore backup](#)

Create new admin account

New admin password:

Usar una contraseña generada de forma segura
 pzwCZV1FUSXZFF8
 Firefox va a guardar esta contraseña para este sitio web.
 Ver credenciales guardadas

We recommend:

- At least 8 characters
- At least one uppercase letter
- At least one lowercase letter
- At least one number

Install the latest firmware automatically during setup

Password strength:

Figura 2.6: Requisitos mínimo de credenciales

Fuente: Autor

Se dio cumplimiento a las características mínimas de seguridad para las credenciales del dispositivo firewall de acuerdo con la recomendación del fabricante antes señalado.

Basic configuration

You can log in to the firewall only through the administrator account currently. You must create a password before you continue. We recommend that you use a long password, with a mix of letters, numbers and special characters to make it strong. If you have an existing configuration that you wish to use, or an existing firewall that you wish to connect to in HA, choose the relevant options below.

[Restore backup](#)

Create new admin account

New admin password:

Reenter the password:

Figura 2.7: Establecimiento de credenciales al producto firewall

Fuente: Autor

Se aceptaron los términos y acuerdos de licencia del producto y además se consintió la recomendación del asistente de configuración de buscar las últimas

actualizaciones de firmware del producto en el proceso de inicialización.

Para lograr el objetivo de la actualización de firmware del equipo se conectó a Internet la interfaz de red WAN al modem del ISP para que se puedan descargar y aplicar estas actualizaciones.

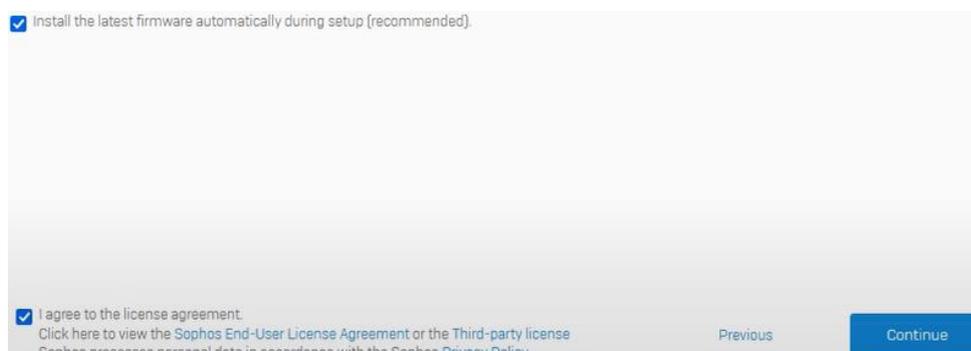
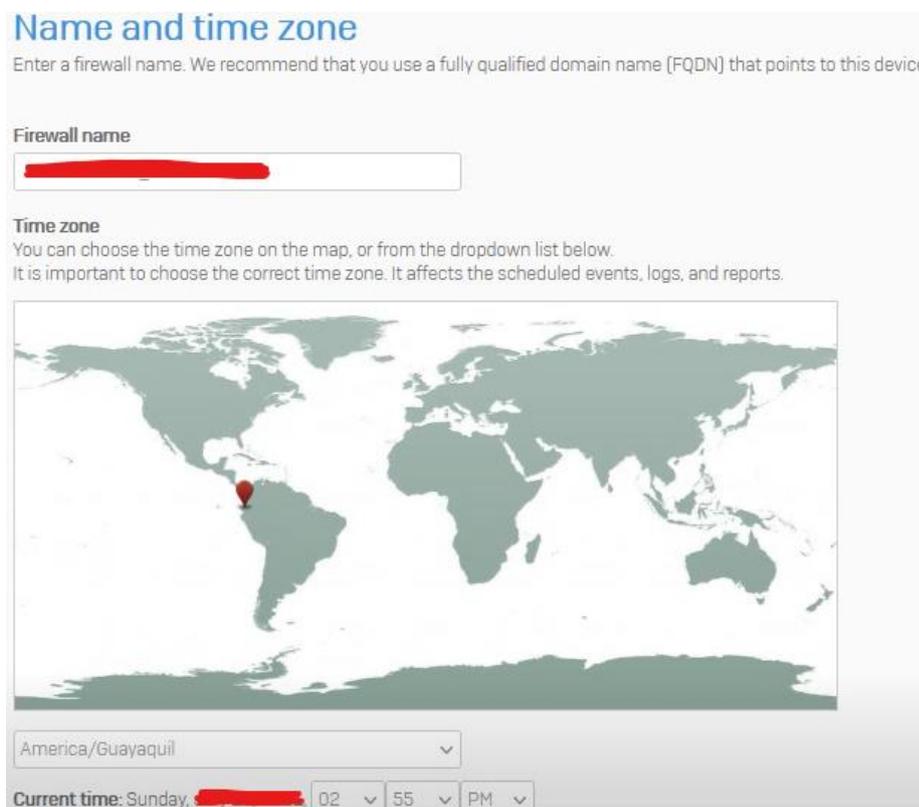


Figura 2.8: Aceptación del acuerdo de licencia

Fuente: Autor

El proceso de descarga y aplicación de nuevo firmware tardó varios minutos en completarse, seguidamente el equipo se reinició automáticamente y al establecerse las conexiones se volvió a la ventana de inicialización del producto. La Figura 2.9 nos muestra la pantalla de establecimiento de nombre del equipo y zona horaria, el nombre del dispositivo se

estableció de acuerdo con lo establecido por la empresa y se estableció la zona horaria de América/Guayaquil.



Name and time zone
Enter a firewall name. We recommend that you use a fully qualified domain name (FQDN) that points to this device.

Firewall name
[Redacted]

Time zone
You can choose the time zone on the map, or from the dropdown list below. It is important to choose the correct time zone. It affects the scheduled events, logs, and reports.

[Map showing South America with a red pin]

America/Guayaquil

Current time: Sunday, [Redacted] 02:55 PM

Figura 2.9: Establecimiento de zona horaria

Fuente: Autor

A continuación, se puede apreciar en la Figura 2.10 que el proceso básico de configuración quedó completado y se observa las licencias que han sido adquiridas para la empresa para el funcionamiento de estos dispositivos firewall. Las licencias que están cargadas a los firewalls son las siguientes:

- Base firewall (por defecto, ilimitada)
- Network protection (licenciado)
- Enhanced support (licenciado)

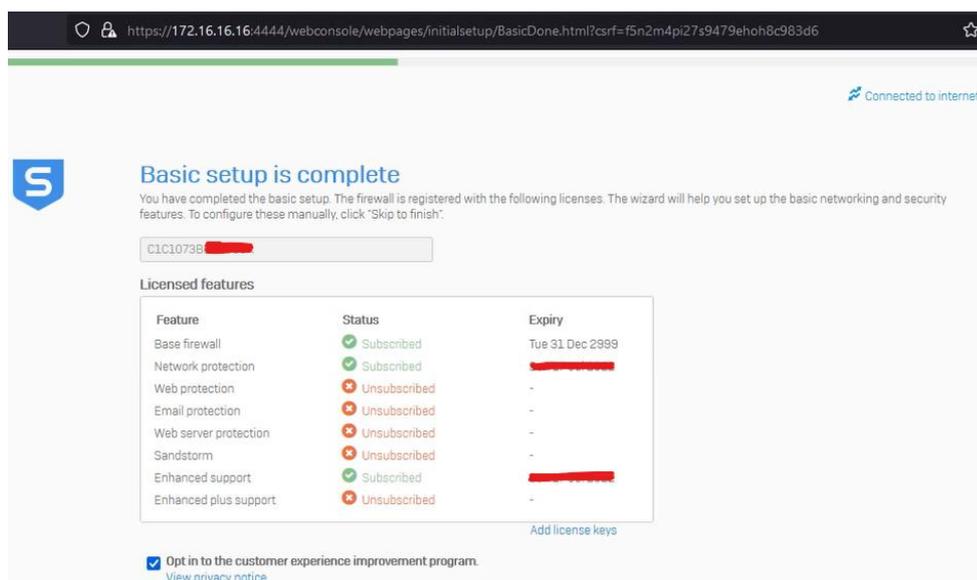


Figura 2.10 Configuración básica completada

Fuente: Autor

La licencia “**Network Protection**” [6] según documentación del fabricante incluye varias características interesantes que les permitirá a la empresa sacar el mayor provecho a la solución de seguridad a implementarse.

Un resumen de estas características se puede observar en la siguiente tabla:

CARACTERÍSTICA	BENEFICIO
Sistema de prevención contra intrusiones de última generación	Proporcionar protección avanzada contra ataques.
Security Heartbeat	Crear protección entre dispositivos protegidos por software de Sophos y el firewall permitiendo una identificación de amenazas más proactiva y eficiente.
Protección contra amenazas avanzadas	Identificar y responder de manera inmediata ataques más sofisticados.
Tecnologías VPN avanzadas	Establecimiento de conexiones más sencillas y fáciles de usar

Tabla 7: Características de Network Protection

Fuente: [6]

Se dejó los parámetros básicos de red como se muestra en la Figura 2.11.



The screenshot shows a web-based configuration interface for a firewall. At the top, there is a section titled "Choose gateway" with a dropdown menu set to "This firewall (route mode)". Below this is a paragraph of explanatory text. The next section is "LAN address and internal client network size", featuring a text input field with "172.16.16.16" and a dropdown menu set to "/24 (up to 254 client devices)". There is a link "Edit internet connection" in blue. Below that, the "Enable DHCP" checkbox is checked, with the text "Let the firewall assign IP addresses to your internal devices." underneath. The final section is "DHCP lease range", with two text input fields: the first contains "172.16.16.17" and the second contains "172.16.16.254".

Figura 2.11: Configuración básica de red inicial

Fuente: Autor

Posteriormente completada esta inicialización de producto se procedió a establecer los parámetros finales según el rediseño de la red aprobado por la empresa.

Antes de concluir la inicialización, se estableció una cuenta de correo electrónico para que lleguen las notificaciones de alerta y los respaldos de configuración de los dispositivos firewall.



The screenshot shows a configuration page titled "Notifications and backups" with a blue shield icon containing a white 'S'. Below the title is a sub-header and a paragraph: "It is important to have quick access to backups. Enter the details to receive the latest backups and notifications by email." The form contains several fields: "Email recipient" and "Email sender" are text input fields with redacted content; "Send weekly configuration backup" is a checked checkbox; "Encryption password" and "Confirm encryption password" are password input fields with masked characters.

Figura 2.12: Configuración de respaldos y notificaciones de correo

Fuente: Autor

La Figura 2.13 muestra la pantalla final de la configuración que explica que para la correcta aplicación de cambios se tiene que esperar varios minutos y que existirá un reinicio automático del equipo.

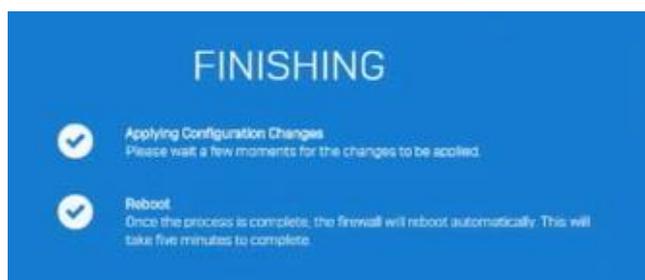


Figura 2.13: Configuración final de inicialización del firewall

Fuente: Autor

Para conocer que el firewall estaba nuevamente habilitado, se dejó establecido un ping extendido a la dirección IP por defecto de la interfaz LAN del firewall hasta que se volvió a tener respuesta a la prueba de conectividad con el comando ping.

Esto se lo hizo desde la laptop en la que se estaban realizando las configuraciones de inicialización del producto.

```
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.16.16.16: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.16.16: bytes=32 tiempo=9ms TTL=64
Respuesta desde 172.16.16.16: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.16.16: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.16.16: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.16.16: bytes=32 tiempo<1m TTL=64
```

Figura 2.14: Prueba de conectividad ping del firewall

Fuente: Autor

Se digitó la dirección IP predeterminada en un navegador de internet a través de conexión segura https://, la Figura 2.15 muestra una advertencia de seguridad antes de ingresar a la administración del equipo, en este caso se aceptó el riesgo y se continuó para proceder al ingreso.

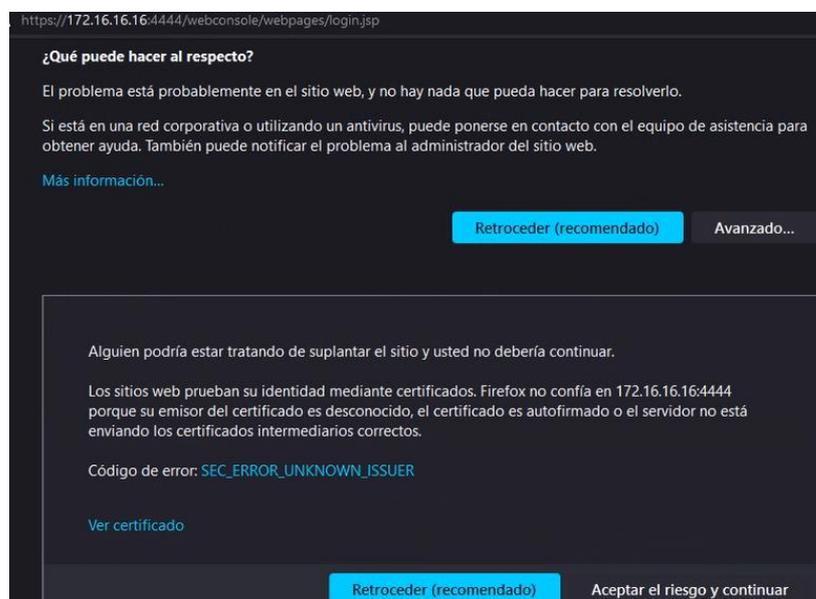


Figura 2.15: Ingreso por primera vez a consola de administración

Fuente: Autor

Se procedió a ingresar a la consola de administración del dispositivo y se pudo visualizar que el equipo cargó con los valores por defectos según las configuraciones establecidas en la inicialización, paso seguido se procedió a realizar el cambio de dirección IP para el equipo firewall según lo definido en la Tabla 4: Esquema de segmentación. La Figura 2.16 muestra los cambios efectuados en la configuración de red para la interfaz LAN.

Interface	Status/Interface speed	IP address
 GuestAP WiFi Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static
 Porte WAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	 /255.255.255.0 DHCP
 br0 N/A Bridge-pair	Connected N/A	192.168.110.1/255.255.255.224 Static

Figura 2.16: Personalización de parámetros de red

Fuente: Autor

Seguidamente de establecidos los nuevos parámetros se guardaron los cambios en el equipo y se realizó prueba de conectividad ICMP con la aplicación ping para validar la conectividad según la Figura 2.17.

```

C:\> Símbolo del sistema - ping -t 192.168.110.1

Respuesta desde 192.168.110.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.110.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.110.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.110.1: bytes=32 tiempo=1ms TTL=64

```

Figura 2.17: Prueba de conectividad ping de firewall

Fuente: Autor

La Figura 2.18 muestra la consola de administración con los cambios ya aplicados correctamente.

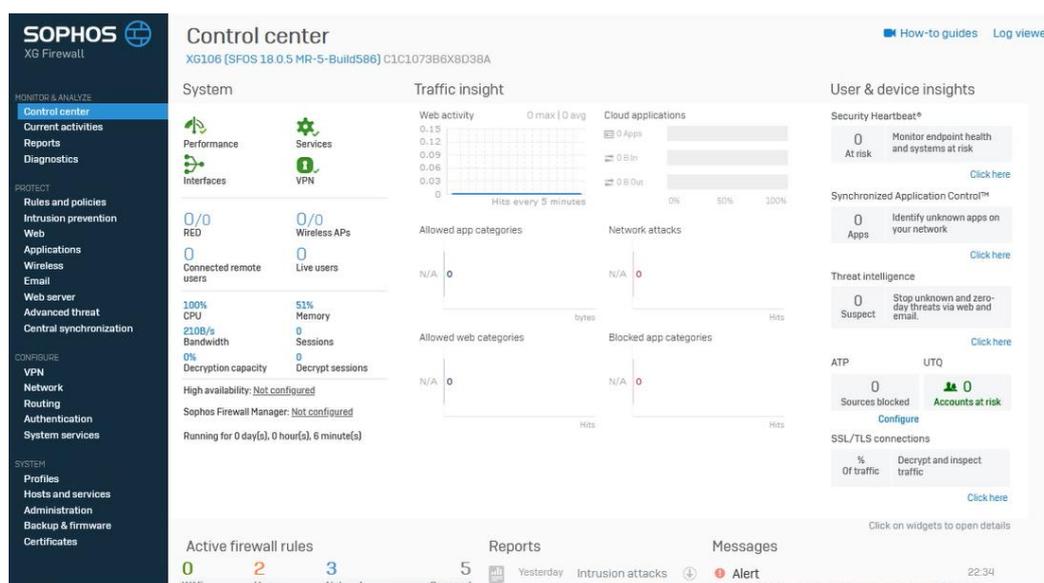


Figura 2.18: Consola de administración de firewall

Fuente: Autor

Una vez completado el proceso de cambio de direccionamiento IP en el dispositivo firewall y con el acceso

correcto comprobado desde la consola de administración, se pudo ver que los equipos quedaron listos para que se realicen las configuraciones de túnel VPN, dicho proceso se lo explicará a continuación.

2.3.3.3. ESTABLECIMIENTO DE CONFIGURACIÓN PARA VPN.

Aquí se explicará el proceso que se siguió para establecer la configuración de túnel VPN del tipo IPsec [7], esta configuración se realizó de acuerdo con la documentación recomendada del fabricante del equipo firewall para el establecimiento de una conexión VPN IPsec sitio a sitio [8]. Para iniciar, se creó la definición del nombre de la interfaz LAN local y remota asociada a la dirección IP del firewall del local 1, y lo mismo se hizo con el equipo del local 2. Se siguió el esquema de direccionamiento IP señalado en la Tabla 4 tal como se muestra en la Figura 2.19 a continuación:



The image shows a web-based configuration interface for a network device. At the top, there is a navigation bar with tabs: "IP host" (selected), "IP host group", "MAC host", "FQDN host", "FQDN host group", and "Country group". Below the navigation bar, there are several configuration fields:

- Name ***: A text input field with a redacted value.
- IP version ***: Radio buttons for "IPv4" (selected) and "IPv6".
- Type ***: Radio buttons for "IP" (selected), "Network", "IP range", and "IP list".
- IP address ***: A text input field containing "192.168" followed by a redacted value. To its right is a "Subnet" field containing "/27 (255.255.255.224)".

Figura 2.19: Definición de red LAN local y remota

Fuente: Autor

Los parámetros básicos de configuración para la VPN se muestran en la Tabla 8.

ITEM	LOCAL 1	LOCAL 2
Rol	Principal	Sucursal
Política	DefaultHeadOffice	DefaultBranchOffice
Acción	Solo respuesta	Iniciar conexión
Tipo de autenticación	Clave pre-compartida	Clave pre-compartida

Tabla 8: Parámetros básicos de configuración VPN

Fuente: Autor



Figura 2.20: Asistente de configuración VPN

Fuente: Autor

Se procedió a iniciar el asistente de configuración VPN, para este caso se definió el nombre **TUNEL_VPN** para estas configuraciones. A continuación, se eligió el tipo de conexión **VPN Site To Site** como muestra la Figura 2.21:

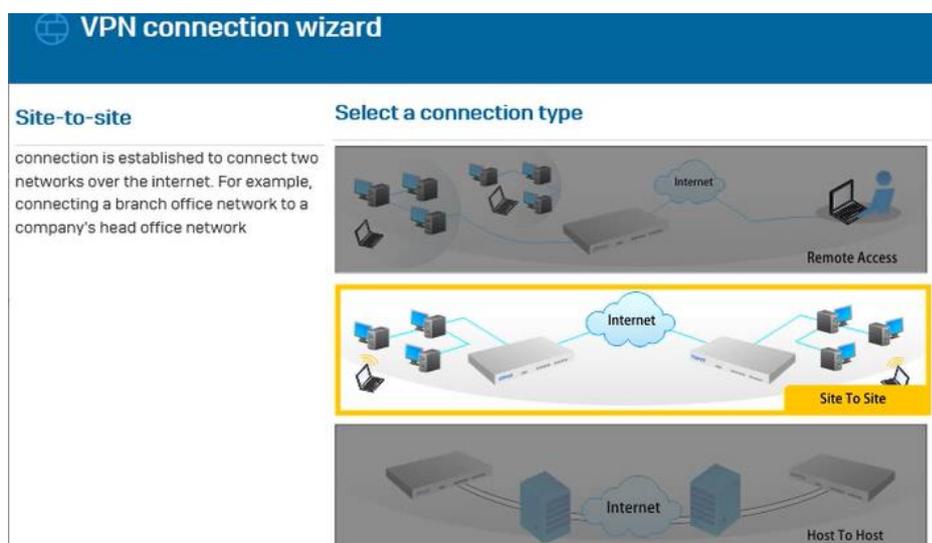


Figura 2.21: Definición de tipo de conexión VPN

Fuente: Autor

Al finalizar la configuración básica en el dispositivo firewall del local 1, el asistente muestra el resumen de configuraciones como se puede apreciar en la Figura 2.22.

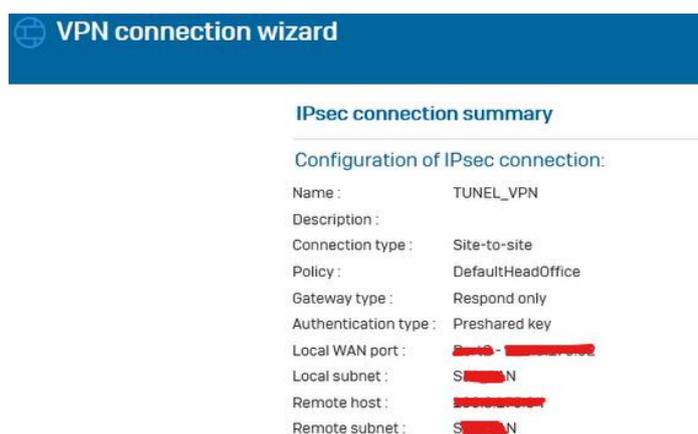


Figura 2.22: Resumen de configuraciones VPN IPsec

Fuente: Autor

Para continuar, se guardaron los cambios para que se apliquen en el primer dispositivo configurado como muestra la Figura 2.23.

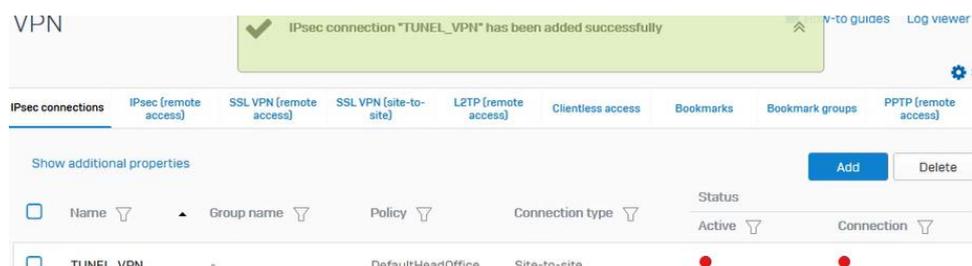


Figura 2.23: Conexión IPsec aplicada para local 1

Fuente: Autor

Inmediatamente de aplicados los cambios, el estado de la conexión IPsec se activó exitosamente en el primer dispositivo como se observa en la Figura 2.24 en el botón de color verde ●. El botón rojo ● de la conexión permanecerá en ese estado hasta que esté correctamente aplicada la configuración de VPN en el dispositivo firewall del local2.

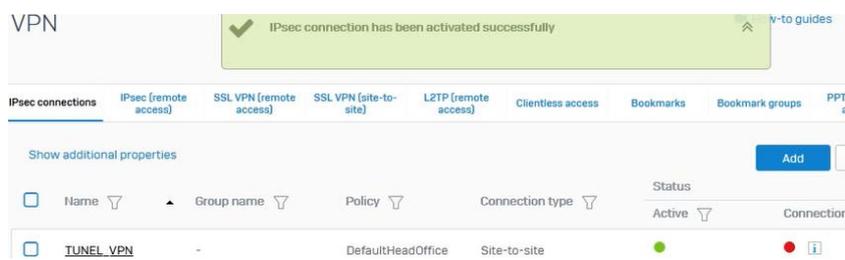


Figura 2.24: Estado activo de conexión IPsec para local 1

Fuente: Autor

2.3.3.4. ESTABLECIMIENTO DE REGLAS DE FIREWALL PARA TRÁFICO VPN.

Se agregaron 2 reglas para tráfico saliente y entrante en ambos dispositivos firewall. Se eligieron los parámetros de origen y destino que previamente habían sido configurado y se aplicó la configuración. En la Figura 2.25 se puede observar que estas reglas de tráfico se habían agregado a las configuraciones del firewall.

#	Name	Source	Destination	What	ID	Action
3	Traffic to Interna... in 0 B, out 0 B			To LAN, WiFi, VPN, DMZ. Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping...		
1	Traffic to WAN in 0 B, out 0 B			Outbound traffic to WAN. Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the d...		
1	Traffic to DMZ in 0 B, out 0 B			Inbound traffic to DMZ. Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the de...		

Figura 2.25: Reglas de tráfico para red local y remota

Fuente: Autor

2.3.4. AJUSTE DE CONFIGURACIONES A LOS DISPOSITIVOS FINALES.

Una vez configurado los equipos firewall, establecido el túnel VPN y agregadas las reglas de tráfico entrante y saliente, se tuvo que realizar el ajuste de configuraciones en los dispositivos finales

(puntos de acceso inalámbricos, grabador de video, estaciones de trabajo e impresoras) que tiene la empresa para que la solución implementada pueda funcionar de manera correcta.

Para los puntos de acceso se realizaron las siguientes actividades:

- Restauración de configuración de fábrica de los dispositivos de punto de acceso para la red WLAN en ambos locales.
- Se asignaron credenciales de usuario administrador y se cambió la clave de usuarios a los puntos de acceso.
- Se asignó las direcciones IP de manera estática que se reservaron según la Tabla 4: Esquema de segmentación.
- Se establecieron nuevos SSID y clave para la red WLAN de ambos locales.
- Se eligió el método de autenticación y el protocolo de encriptación más compatible con los dispositivos.
- Se deshabilitó la asignación dinámica de direcciones IP por DHCP.
- Se definió la configuración de los puntos de acceso en modo AP.
- Se deshabilitó la configuración inalámbrica de invitados para la red WLAN.

Para los equipos de grabación DVR, estaciones de trabajo e impresoras se realizó lo siguiente:

- Se asignó las direcciones IP de manera estática que se reservaron según la Tabla 4: Esquema de segmentación.
- Se guardaron las configuraciones en la aplicación del equipo de grabación DVR.
- Se refrescaron el estado de conexión en las interfaces de red desde sistema operativo.

CAPÍTULO 3

RESULTADO DE LA SOLUCIÓN

3.1. ANÁLISIS DE RESULTADOS

En esta sección se analizará los resultados obtenidos en la implementación de la solución propuesta en base a las pruebas de comprobación realizadas en el proceso del despliegue de la solución de seguridad.

3.1.1. TÚNEL VPN PUNTO A PUNTO.

Se evidenció que una vez culminado el proceso de configuración del segundo dispositivo firewall, el estado de conexión del túnel VPN pasó a estar activado en ambos equipos de seguridad perimetral como se puede apreciar en la Figura 3.1 y Figura 3.2.

IPsec connections

Show additional properties Add Delete

<input type="checkbox"/>	Name ▾	Group name ▾	Policy ▾	Connection type ▾	Status	Connection ▾
					Active ▾	
<input type="checkbox"/>	TUNEL_VPN	-	DefaultHeadOffice	Site-to-site	●	● ⓘ

Figura 3.1: Conexión de túnel VPN activado en local 1

Fuente: Autor

IPsec connections

Show additional properties Add Delete

<input type="checkbox"/>	Name ▾	Group name ▾	Policy ▾	Connection type ▾	Status	Connection ▾
					Active ▾	
<input type="checkbox"/>	Tunel_VPN	-	DefaultBranchOffice	Site-to-site	●	● ⓘ

Figura 3.2: Conexión de túnel VPN activado en local 2

Fuente: Autor

Se comprobó el estado de uso del túnel VPN y se evidenció que el mismo estaba correctamente establecido y en funcionamiento óptimo.

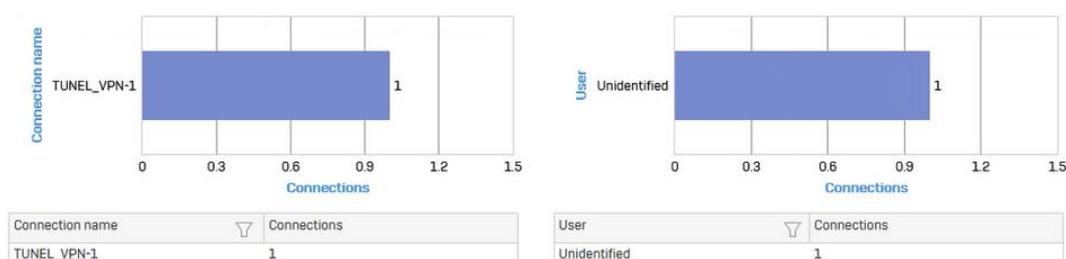


Figura 3.3: Reporte de uso de túnel VPN

Fuente: Autor

Se comprobó que las reglas del firewall para el tráfico entrante y saliente del túnel VPN fueron correctamente aplicadas y quedaron establecidas como se muestra en la Figura 3.4.

#	Name	Source	Destination	What	ID	Action	Feature and service
3	Traffic to Interna... in 0 B, out 1705 KB	To LAN, WIFI, VPN, DMZ. Firewall rules with the destination zone as LAN, WIFI, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping...					
1	[example] Traffic... in 0 B, out 0 B	Any zone, Any host, Any live user...	LAN, DMZ, WIFI, VPN, Any host...	Any service	#4	Drop	[PS] [AV] [WEB] [APP] [OS] [TR] [LINK] [NAT] [PRX] [LOG]
2	Outbound_VPN_Traf... in 0 B, out 1705 KB	LAN, SF1_LAN	VPN, SF2_LAN	Any service	#6	Accept	[PS] [AV] [WEB] [APP] [OS] [TR] [LINK] [NAT] [PRX] [LOG]
3	Inbound_VPN_Traffi... in 0 B, out 0 B	VPN, SF2_LAN	LAN, SF1_LAN	Any service	#7	Accept	[PS] [AV] [WEB] [APP] [OS] [TR] [LINK] [NAT] [PRX] [LOG]

Figura 3.4: Validación de reglas de tráfico del firewall

Fuente: Autor

3.1.2. APLICACIÓN DE NUEVO SEGMENTO DE RED.

Se pudo observar que las estaciones de trabajo obtuvieron las direcciones IP por DHCP que se establecieron según el local en el que estaban ubicado. La Figura 3.5 muestra el estado de LAN de una estación de trabajo de los locales.

Habilitado para DHCP	Sí
Dirección IPv4	192.168.1. [REDACTED]
Máscara de subred IPv4	255.255.255.224
Concesión obtenida	sábado, 24 de [REDACTED] 10:05:23
La concesión expira	domingo, 25 de [REDACTED] 10:05:23
Puerta de enlace predet...	192.168. [REDACTED]
Servidor DHCP IPv4	192.168. [REDACTED]
Servidor DNS IPv4	192.168. [REDACTED]

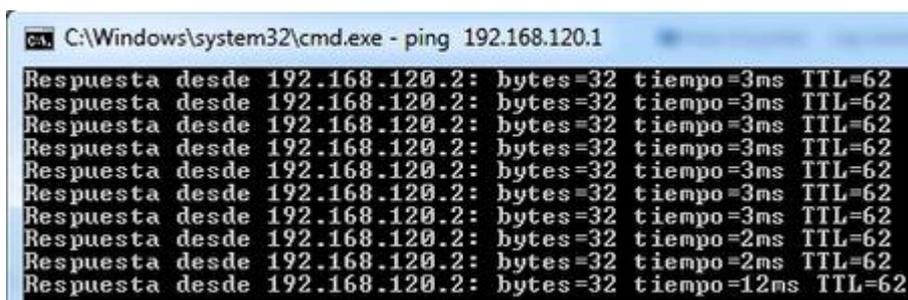
Figura 3.5: Validación de reglas de tráfico del firewall

Fuente: Autor

3.1.3. PRUEBAS DE CONECTIVIDAD DE LA RED.

Se hicieron pruebas de conectividad entre los dispositivos finales de cada local y se evidenció que existía comunicación entre los 2 segmentos de red aplicados.

Para los dispositivos firewall se restringió la respuesta ICMP, pero si se dejó habilitado el acceso WEB para administración local. La Figura 3.6 evidencia la prueba de conectividad exitosa a uno de los dispositivos de la red LAN del local 2.



```
C:\Windows\system32\cmd.exe - ping 192.168.120.1
Respuesta desde 192.168.120.2: bytes=32 tiempo=3ms TTL=62
Respuesta desde 192.168.120.2: bytes=32 tiempo=2ms TTL=62
Respuesta desde 192.168.120.2: bytes=32 tiempo=2ms TTL=62
Respuesta desde 192.168.120.2: bytes=32 tiempo=12ms TTL=62
```

Figura 3.6: Prueba de conectividad a dispositivo final

Fuente: Autor

En la Figura 3.7 se observa de fondo la consola de administración del firewall del local 2 y en la prueba de conectividad ping se aprecia que no existen pérdidas de paquetes en las pruebas de conectividad a los dispositivos del local 1.

```

C:\Users\MI-ADMIN>ping 192.168.110.3 -t
Haciendo ping a 192.168.110.3 con 32 bytes de datos:
Respuesta desde 192.168.110.3: bytes=32 tiempo=3ms TTL=62
Respuesta desde 192.168.110.3: bytes=32 tiempo=4ms TTL=62
Respuesta desde 192.168.110.3: bytes=32 tiempo=3ms TTL=62
Respuesta desde 192.168.110.3: bytes=32 tiempo=4ms TTL=62
Estadísticas de ping para 192.168.110.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 3ms, Máximo = 4ms, Media = 3ms
Control-C
^C
C:\Users\MI-ADMIN>ping 192.168.110.4 -t
Haciendo ping a 192.168.110.4 con 32 bytes de datos:
Respuesta desde 192.168.110.4: bytes=32 tiempo=3ms TTL=126
Respuesta desde 192.168.110.4: bytes=32 tiempo=3ms TTL=126
Estadísticas de ping para 192.168.110.4:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 3ms, Máximo = 3ms, Media = 3ms
  
```

Figura 3.7: Conectividad entre dispositivos de ambos segmentos de red

Fuente: Autor

3.1.4. VERIFICACIÓN DE ANCHO DE BANDA.

Se validó que el ancho de banda en ambos locales era el que correspondía según lo contratado con el ISP, tal como se muestra a continuación



Figura 3.8: Test de velocidad de ancho de banda de Internet

Fuente: Autor

CONCLUSIONES Y RECOMENDACIONES.

Las conclusiones y recomendaciones que se presentan en este documento están basadas en el entendimiento del problema presentado al inicio de este trabajo, así como la experiencia adquirida a lo largo del desarrollo de la solución propuesta y la libre comunicación entre los interesados como son los usuarios internos, jefes de áreas y accionistas de la empresa.

CONCLUSIONES

1. Mejoró las comunicaciones entre los locales comerciales en procesos de consulta y reportes de su sistema de información de minutos a pocos segundos.
2. Se aceleró considerablemente el acceso a la información alojada en el servidor de base de datos para cada dispositivo de usuario final.

3. Se independizó la conectividad de Internet del tipo pymes para ambos locales.
4. Se mejoró en la experiencia de los usuarios internos como del cliente final.
5. La implementación de la solución de seguridad perimetral no resolverá todos los problemas que contiene la empresa, más bien es un primer paso para adoptar nuevas tecnologías y la aplicación de mejores prácticas para poder sacarle el mayor provecho a la inversión realizada.

RECOMENDACIONES

1. Implementar los futuros proyectos de tecnología con personal calificado para el despliegue de las nuevas soluciones.
2. Regularizar el proceso de legalización de sistema operativo y aplicaciones de ofimática, o de lo contrario utilizar soluciones de código abierto.
3. Estandarizar la solución de antivirus existente, aplicándolas a todas las estaciones de trabajo de la empresa para contar con un nivel adecuado de protección ante amenazas de seguridad.

4. Ejecutar un hackeo ético en ambos locales que permita identificar vulnerabilidades y riesgos en los equipos.
5. Ejecutar en la medida de lo posible las recomendaciones que se han planteado a los accionistas de la empresa.

BIBLIOGRAFÍA

- [1] OMS, «Información básica sobre la COVID-19,» 12 Octubre 2020. [En línea]. Available: <https://www.who.int/es/news-room/q-a-detail/coronavirus-disease-covid-19>. [Último acceso: Julio 2021].
- [2] Ricardo Vera & Asociados, «VMULTINEG,» 2021. [En línea]. Available: <https://sistemasvmultineg.com/>.
- [3] UBIQUITI, «NanoStation M,» 2021. [En línea]. Available: <https://www.ui.com/airmax/nanostationm/>. [Último acceso: Julio 2021].
- [4] OOKLA, LLC, «Test de velocidad,» 2021. [En línea]. Available: <https://www.speedtest.net/es>. [Último acceso: Julio 2021].
- [5] M. G. Piattini y E. d. Peso, Auditoría Informática: Un enfoque práctico, 2da ampliada y revisada ed., Ra-Ma, Ed., Alfaomega, 2001, p. 704.
- [6] SOPHOS, «Serie XG de Sophos,» 2021. [En línea]. Available: <https://www.sophos.com/es-es/medialibrary/pdfs/factsheets/sophos-xg-series-appliances-brna.pdf>. [Último acceso: Agosto 2021].
- [7] IBM, «Conceptos de protocolo de seguridad ip,» 2005. [En línea]. Available: <https://www.ibm.com/docs/es/i/7.3?topic=concepts-ip-security-protocols>. [Último acceso: Julio 2021].
- [8] SOPHOS, «Sophos Firewall: How to set a Site-to-Site IPsec VPN connection using a preshared key,» 05 Agosto 2021. [En línea]. Available: https://support.sophos.com/support/s/article/KB-000035717?language=en_US. [Último acceso: Agosto 2021].
- [9] Laudon, Kenneth C y Laudon, Jane P, Sistemas de información gerencial, 14va ed., Pearson, 2016, p. 680.