



Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Electrónica y Eléctrica
Escuela Profesional de Ingeniería de Telecomunicaciones

**Diseño e implementación de una solución de internet
dedicado con seguridad perimetral virtual para una
entidad gubernamental**

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de Ingeniero de
Telecomunicaciones

AUTOR

Rosa Estefanny JUAREZ CASTILLO

ASESOR

Mg. Arlich Joel PORTILLO ALLENDE

Lima, Perú

2025



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Juarez, R. (2025). *Diseño e implementación de una solución de internet dedicado con seguridad perimetral virtual para una entidad gubernamental*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Facultad de Ingeniería Electrónica y Eléctrica]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Rosa Estefanny Juarez Castillo
Tipo de documento de identidad	DNI
Número de documento de identidad	75344874
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Arlich Joel Portillo Allende
Tipo de documento de identidad	DNI
Número de documento de identidad	10125495
URL de ORCID	https://orcid.org/0000-0002-3175-3377
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Celso Ysidro Gerónimo Huamán
Tipo de documento	DNI
Número de documento de identidad	09191500
Miembro del jurado 1	
Nombres y apellidos	Williams Fernando Acosta Solorzano
Tipo de documento	DNI
Número de documento de identidad	06434186
Miembro del jurado 2	
Nombres y apellidos	Angel Orlando Sumoso Huaman
Tipo de documento	DNI
Número de documento de identidad	06842634
Datos de investigación	
Línea de investigación	C.0.3.10 Redes de datos.
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica

Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: San Isidro Latitud: -12.09681 Longitud: -77.03211
Año o rango de años en que se realizó la investigación	Junio 2024 – Diciembre 2024
URL de disciplinas OCDE	Telecomunicaciones. https://purl.org/pe-repo/ocde/ford#2.02.05



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



**ACTA DE SUSTENTACIÓN
TRABAJO DE SUFICIENCIA
PROFESIONAL
ACTA N°29/FIEE-CTGT/2025**

Los suscritos Miembros del Jurado, docentes permanentes de las Escuelas Profesionales de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha 25 de setiembre del 2025, como presidente de Jurado el **DR. CELSO YSIDRO GERÓNIMO HUAMÁN**, integrado por el Miembro de Jurado el **DR. WILLIAMS FERNANDO ACOSTA SOLORZANO**, el Miembro de Jurado **ING. ANGEL ORLANDO SUMOSO HUAMAN** y Miembro Asesor el **MG. ARLICH JOEL PORTILLO ALLENDE**.

Después de escuchar la Sustentación Presencial del Trabajo de Suficiencia Profesional de la Bachiller **ROSA ESTEFANNY JUAREZ CASTILLO** con código 16190296 que para optar el Título Profesional de Ingeniera de Telecomunicaciones sustentó el Trabajo de Suficiencia Profesional titulado **DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE INTERNET DEDICADO CON SEGURIDAD PERIMETRAL VIRTUAL PARA UNA ENTIDAD GUBERNAMENTAL**.

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió otorgarle el calificativo de 15 (Quince.).

Ciudad Universitaria, 25 de setiembre del 2025

DR. CELSO YSIDRO GERÓNIMO HUAMÁN
Presidente Jurado

DR. WILLIAMS FERNANDO ACOSTA SOLORZANO
Miembro Jurado

ING. ANGEL ORLANDO SUMOSO HUAMAN
Miembro Jurado

MG. ARLICH JOEL PORTILLO ALLENDE
Miembro Asesor



UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

CERTIFICADO DE SIMILITUD

Yo , **ARLICH JOEL PORTILLO ALLENDE** en mi condición de asesor acreditado con el Dictamen N°04/FIEE-CTGT/2025 de Trabajo de Suficiencia Profesional **DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE INTERNET DEDICADO CON SEGURIDAD PERIMETRAL VIRTUAL PARA UNA ENTIDAD GUBERNAMENTAL.**, presentado por la bachiller **ROSA ESTEFANNY JUAREZ CASTILLO**, para optar al título profesional de Ingeniera de Telecomunicaciones. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 08% de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su publicación en el repositorio institucional.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título de Ingeniera de Telecomunicaciones.

Lima, 25 de Setiembre del 2025


Firma del Asesor

DNI: 10125495

Nombres y apellidos del asesor:
ARLICH JOEL PORTILLO ALLENDE

DEDICATORIA

Este trabajo está dedicado a mis padres, por ser mi mayor motivación y por enseñarme el valor de la perseverancia. Su apoyo y confianza me han impulsado a ser cada día una mejor profesional.

AGRADECIMIENTOS

Al Mg. Arlich Portillo, por su valiosa orientación y constante apoyo. Gracias por compartir sus conocimientos, los cuales fueron fundamentales para culminar con éxito esta investigación.

RESUMEN

Las redes empresariales han evolucionado significativamente en la última década. Los colaboradores de una empresa ya no están limitados a trabajar en una sola oficina. Con la expansión de las organizaciones, aumenta también el número de sucursales y oficinas remotas.

Tradicionalmente, las oficinas remotas solían estar conectadas a una oficina principal a través de un enlace WAN de conmutación de etiquetas multiprotocolo (MPLS). Sin embargo, cada vez es más común la interconexión de sedes a través de una red privada virtual (VPN) mediante un enlace de acceso directo a Internet.

El tráfico que se dirige a Internet debe estar mínimamente protegido con servicios de antivirus, detección de malware en tiempo real y otras medidas de seguridad avanzadas.

El presente trabajo de investigación tiene por finalidad el diseño y la implementación de una red para interconectar (05) sedes de una entidad gubernamental. Cada sede contará con una conexión directa a Internet bajo una topología descentralizada, garantizando la seguridad mediante un firewall en la nube. Esto permitirá que todas las sedes accedan al servidor de alertas de emergencia alojado en la sede principal mediante un software cliente VPN propio de la Entidad, optimizando la comunicación y fortaleciendo la seguridad de la red.

Palabras clave: Internet, VPN, seguridad, interconexión, firewall.

ABSTRACT

Enterprise networks have evolved significantly over the last decade. Employees are no longer limited to working in a single office. As organizations expand, the number of branches and remote offices also increases.

Traditionally, remote offices were connected to a main office through a Multiprotocol Label Switching (MPLS) WAN link. However, it is increasingly common for branches to be interconnected through a Virtual Private Network (VPN) using a direct Internet access link.

Traffic directed to the Internet must be minimally protected with antivirus services, real-time malware detection, and other advanced security measures. This research aims to design and implement a network to interconnect five (05) branches of a government entity. Each branch will have a direct Internet connection under a decentralized topology, ensuring security through a cloud-based firewall. This will allow all branches to access the emergency alert server hosted at the main branch via the entity's proprietary VPN software, optimizing communication and strengthening network security.

Keywords: Internet, VPN, security, interconnection, firewall.

INDICE GENERAL

CARÁTULA	i
DEDICATORIA	ii
AGRADECIMIENTOS	iii
RESUMEN	iv
ABSTRACT	v
ÍNDICE GENERAL	vi
LISTA DE FIGURAS	viii
LISTA DE TABLAS	x
CAPITULO I: INTRODUCCIÓN	1
CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLA LA ACTIVIDAD	2
2.1 Institución – Actividad que desarrolla	2
2.2 Periodo de duración de la actividad	2
2.3 Finalidad y objetivos de la entidad	2
2.4 Razón social	3
2.5 Dirección postal	3
2.6 Nombre y correo electrónico del profesional a cargo	3
CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD	4
3.1 Organización de la actividad	4
3.2 Finalidad y objetivos de la actividad	5
3.2.1 Finalidad	5
3.2.2 Objetivos	6
3.3 Problemática	6
3.3.1 Problema General	8
3.3.2 Problemas Específicos	9
3.3.3 Justificación e importancia de la investigación	9

3.4	Metodología	11
3.4.1	Bases teóricas	11
3.4.2	Marco conceptual	15
3.5	Procedimiento	36
3.5.1	Diseño inicial de la investigación	36
3.5.2	Implementación del servicio	48
3.6	Resultado de la actividad	58
CAPITULO IV: DISCUSIÓN DE LOS RESULTADOS.....		60
4.1	Descripción de la implementación	60
4.2	Evaluación Económica	61
4.2.1	Identificación de costos y plan de inversión	62
4.2.2	Identificación y clasificación de beneficios	63
CAPITULO V: CONCLUSIONES.....		66
CAPITULO VI: RECOMENDACIONES.....		68
CAPITULO VII: BIBLIOGRAFÍA		70
CAPITULO IX: ANEXOS		74
ANEXO A: UBICACIÓN DE LAS SEDES		75
ANEXO B: CRONOGRAMA DE IMPLEMENTACIÓN.....		77
ANEXO C: INSTALACIÓN DE EQUIPOS EN SEDES REMOTAS		78
ANEXO D: VALIDACIÓN DE ACTIVACIÓN DE EQUIPOS CPE		80
ANEXO E: PRUEBAS DE VALIDACIÓN DEL SISTEMA EN CAMPO.....		85

LISTA DE FIGURAS

<i>Figura 1:</i> Topología física de red actual de la Entidad. -----	8
Figura 2: Clasificación de tipos de redes en base a la distancia geográfica. 16	
Figura 3: Tipos de redes según su topología física. -----	18
Figura 4: Comparación de parámetros de tipos de fibra multimodo. -----	24
Figura 5: Dashboard Panorama para gestión centralizada de VM-Series. --	30
Figura 6: Topología de red de solución actual. -----	37
Figura 7: Instalación de CPE Cisco C3560G-24TS-S en Sede Principal. ---	50
Figura 8: Tenant de Virtualización vSphere de VM-Series. -----	51
Figura 9: Portal del acceso a Palo Alto VM-700. -----	52
Figura 10: Suscripciones habilitadas en Palo Alto VM-700. -----	53
Figura 11: Comparativa de Costos: Firewall virtual vs Firewall físicos en cada sede por 1 año. -----	63
Figura 12: Análisis de Costos y Beneficios Acumulados en 5 Años: Firewall físico vs Firewall virtual Centralizado. -----	64
Figura 13: Ubicación de la Sede Principal. -----	75
Figura 14: Ubicación de la Sede Remota 1. -----	75
Figura 15: Ubicación de la Sede Remota 2. -----	76
Figura 16: Ubicación de la Sede Remota 3. -----	76
Figura 17: Ubicación de la Sede Remota 4. -----	76
Figura 18: Instalación de CPE Cisco 1121-4P en Sede Remota 1. -----	78
Figura 19: Instalación de CPE Cisco 1121-4P en la Sede Remota 2. -----	78
Figura 20: Instalación de CPE Cisco 1121-4P en la Sede Remota 3. -----	79
Figura 21: Instalación de CPE Cisco 1121-4P en la Sede Remota 4. -----	79
Figura 22: Activación de Router Cisco C3560G-24TS en Sede Principal. --	80
Figura 23: Activación de Router Cisco 1121-4P en la Sede Remota 1. -----	81
Figura 24: Activación de Router Cisco 1121-4P en la Sede Remota 2. -----	82
Figura 25: Activación de Router Cisco 1121-4P en la Sede Remota 3. -----	83

Figura 26: Activación de Router Cisco 1121-4P en la Sede Remota 4. -----	84
Figura 27: Prueba de Ping y Round Trip Time (RTT) de Sede Principal a las Sedes Remotas. -----	85
Figura 28: Prueba de Ping y RTT desde Sede Remota 1 a Sede Principal. -----	86
Figura 29: Prueba de Ping y RTT desde Sede Remota 2 a Sede Principal. -----	86
Figura 30: Prueba de Ping y RTT desde Sede Remota 3 a Sede Principal -----	87
Figura 31: Prueba de Ping y RTT desde Sede Remota 4 a Sede Principal. -----	87
Figura 32: Medición de ancho de banda en la Sede Principal. -----	88
Figura 33: Medición de ancho de banda en la Sede Remota 1. -----	89
Figura 34: Medición de ancho de banda en la Sede Remota 2. -----	90
Figura 35: Medición de ancho de banda en la Sede Remota 3. -----	91
Figura 36: Medición de ancho de banda en la Sede Remota 4. -----	92
Figura 37: Configuración WAN/LAN en Palo Alto VM-700. -----	93
Figura 38: Configuración de pool de IPs en Palo Alto VM-700. -----	94
<i>Figura 39: Tabla de rutas en Palo Alto VM-700. -----</i>	<i>94</i>
<i>Figura 40: Configuración de políticas de firewall en Palo Alto VM-700. -----</i>	<i>95</i>
<i>Figura 41: Categoría de webfilter bloqueadas en Palo Alto VM-700. -----</i>	<i>97</i>
<i>Figura 42: Portal de Monitoreo en Palo Alto VM-700 para el uso de aplicaciones. -----</i>	<i>98</i>
<i>Figura 43: Portal de Monitoreo en Palo Alto VM-700 para la actividad de usuarios. -----</i>	<i>99</i>

LISTA DE TABLAS

Tabla 1: Componentes de la solución de Firewall virtualizado Palo Alto Networks y VMware NSX-T.	34
Tabla 2: Sedes de la Entidad.	41
Tabla 3: Metraje de Fibra óptica de las sedes de la Entidad.	42
Tabla 4: Características y funcionalidades de equipos CPE propuestos.	44
Tabla 5: Funcionalidades de la VM-700 de PAN.	47
Tabla 6: Provisionamiento de recursos.	49
Tabla 7: Provisionamiento lógico para Sede Principal.	54
Tabla 8: Provisionamiento lógico para VM-700.	55
<i>Tabla 9:</i> Provisionamiento lógico para Sede Remota 1.	55
<i>Tabla 10:</i> Provisionamiento lógico para Sede Remota 2.	56
<i>Tabla 11:</i> Provisionamiento lógico para Sede Remota 3.	56
<i>Tabla 12:</i> Provisionamiento lógico para Sede Remota 4.	57
Tabla 13: Gastos de capital del proyecto.	62
Tabla 14: Gastos operativos del proyecto.	62
<i>Tabla 15:</i> Detalle de actividades, tiempos y responsables en la fase de implementación de la solución. propuesta.	77
Tabla 16: Valores de pruebas realizadas en Sede Principal.	85
Tabla 17: Valores de pruebas realizadas en sede Remota 1.	86
Tabla 18: Valores de pruebas realizadas en sede Remota 2.	86
Tabla 19: Valores de pruebas realizadas en sede Remota 3.	87
Tabla 20: Valores de pruebas realizadas en Sede Remota 4.	87
Tabla 21: Resumen de las políticas de seguridad configuradas en el firewall VM-700.	96

CAPITULO I INTRODUCCIÓN

El presente trabajo de investigación aborda el diseño e implementación de un esquema de conectividad basado en internet dedicado y firewall virtual para 5 sedes de una Entidad Gubernamental, migrando de una tecnología de interconexión centralizada hacia una solución más flexible, económica y compatible con entornos modernos. Se propone la integración de un enlace de 1 Gbps para la sede principal y un enlace de 200 Mbps para cada una de sus 4 sedes remotas, mejorando significativamente el ancho de banda disponible y garantizando una conexión segura hacia internet mediante la implementación de una seguridad perimetral basada en un entorno virtual.

El desarrollo de la propuesta responde a la necesidad de modernizar la infraestructura de red de la institución, permitiendo mayor escalabilidad, reducción de costos operativos y mejor capacidad de respuesta ante emergencias. Este cambio, el cual permitirá optimizar la comunicación entre las sedes, se realiza para que la Entidad pueda habilitar una conexión segura al servidor de alertas de emergencia en la sede principal mediante un software cliente VPN propio, asegurando la continuidad operativa y la protección de los datos sensibles.

Asimismo, el esquema propuesto está fundamentado en las ventajas técnicas y económicas que ofrece el modelo de Internet dedicado con soluciones de seguridad en la nube, las cuales se han consolidado como estándares en el diseño de redes modernas. Se busca contribuir al fortalecimiento de las capacidades operativas de la institución, asegurando que las comunicaciones sean robustas, seguras y alineadas con las tendencias tecnológicas actuales.

CAPITULO II INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

2.1 Institución – Actividad que desarrolla

El presente trabajo de suficiencia profesional desarrolla el diseño y la implementación de interconexión de 5 sedes de una Entidad Gubernamental, proponiendo una topología con tecnologías actuales mediante la empresa WIN Empresas S.A.C, una empresa peruana de telecomunicaciones y tecnologías de la información.

2.2 Periodo de duración de la actividad.

La planificación se llevó a cabo a partir de junio del 2024 y la ejecución se culminó en diciembre del 2024.

2.3 Finalidad y objetivos de la entidad.

Acelerar la evolución digital de las empresas para asegurar un servicio con una propuesta de valor distinta, ofreciendo una amplia gama de servicios que incluyen conectividad, cloud híbrido, ciberseguridad, servicios gestionados, data center, comunicaciones unificadas y telefonía corporativa. Se distingue por su enfoque en la flexibilidad, agilidad y cercanía con sus clientes, lo que le permite identificar y comprender sus necesidades, adelantándose a ellas con un compromiso constante hacia la excelencia.

2.4 Razón social

WIN EMPRESAS S.A.C

2.5 Dirección postal

Av. José Gálvez Barrenechea 645, Lima – 15036

2.6 Nombre y correo electrónico del profesional a cargo.

Rudy Carlos Ostoá
Correo: rcarlos@winempresas.pe

CAPITULO III

DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la actividad

Para el diseño e implementación planteados en el presente TSP, las actividades se organizaron en diversas fases, con el propósito de abordar de manera integral los objetivos establecidos. Estas etapas abarcan desde la planificación inicial hasta la implementación y posterior validación de la solución propuesta. A continuación, se describe la estructura de la organización de las actividades:

- Se realizó un análisis de la topología de red actual de la entidad y se identificaron las limitaciones del modelo centralizado basado en tecnología MPLS. En adición, se recopilaron los requerimientos técnicos y operativos necesarios para realizar una migración hacia un esquema descentralizado basado en internet dedicado y seguridad perimetral.
- Para diseñar este esquema de conectividad, se consideraron una serie de parámetros que aseguren que el servicio satisfaga las necesidades actuales y futuras de la organización. La importancia de definir correctamente dichos parámetros técnicos radica en la necesidad de que la Entidad pueda configurar su VPN de software cliente sobre una red de baja latencia, la cual garantizará una comunicación cifrada entre las sedes remotas y la sede principal para el acceso al servidor de alertas de emergencia.
- Se evaluaron diversas tecnologías y se seleccionaron los equipos para brindar el servicio de Internet dedicado y la tecnología para la seguridad

perimetral mediante un firewall perimetral virtualizado en base a beneficios técnicos y económicos.

- Se llevó a cabo la implementación del servicio en base al dimensionamiento previo, realizándose las configuraciones necesarias para la activación de los enlaces de Internet dedicado en todas las sedes. Asimismo, se implementó el firewall perimetral virtualizado.
- Se realizaron pruebas funcionales y de seguridad para verificar el desempeño del nuevo esquema de conectividad.
- Se elaboró la documentación técnica del proyecto, incluyendo diagramas de red, configuraciones y procedimientos operativos.

3.2 Finalidad y objetivos de la actividad

3.2.1 Finalidad

La finalidad de este trabajo es diseñar e implementar un esquema de conectividad moderno, seguro y eficiente para interconectar 5 sedes de una entidad gubernamental, con una solución descentralizada basada en Internet dedicado y protegidas con un firewall virtualizado.

Se busca mejorar la comunicación entre las sedes, garantizar la seguridad de los datos mediante tecnologías avanzadas de seguridad perimetral y optimizar la capacidad de respuesta ante emergencias mediante el acceso seguro al servidor de alertas en la sede principal.

Se pretende lograr una infraestructura escalable, económica y alineada con las tendencias tecnológicas actuales. Además, se busca fortalecer la continuidad operativa de la entidad mediante soluciones resilientes ante fallas de conectividad o ciberataques, reduciendo riesgos en la prestación de servicios críticos.

3.2.2 Objetivos

3.2.2.1 Objetivo General

Diseñar e implementar un esquema de conectividad basado en internet dedicado y firewall virtual para cinco sedes de una entidad gubernamental, migrando de una arquitectura centralizada a una solución más flexible, económica y compatible con entornos modernos, con el fin de mejorar el ancho de banda, garantizar la seguridad de las comunicaciones y optimizar la operatividad de la Entidad.

3.2.2.2 Objetivos Específicos

- Garantizar la mejora de la conectividad y el rendimiento en cada sede mediante la implementación de enlaces de internet dedicados, reduciendo la latencia y optimizando el uso del ancho de banda disponible.
- Implementar una solución de seguridad perimetral virtualizada en VMware para proteger las sedes remotas de amenazas externas e internas, asegurando la correcta aplicación de políticas de seguridad.
- Evaluar el impacto de la implementación del nuevo esquema en términos de costos operativos, así como los beneficios económicos indirectos derivados de la mejora en la eficiencia operativa y la respuesta ante emergencias.

3.3 Problemática

Una entidad del estado que se encarga de la protección civil y gestión de emergencias enfrenta desafíos significativos al depender de una topología de red centralizada (hub and spoke) mediante MPLS, en la cual el tráfico de Internet de las sedes remotas con ancho de banda de 10 Mbps es redirigido

a través de la sede principal, generando cuellos de botella en el tráfico de datos y latencia elevada, lo que afecta el desempeño de aplicaciones críticas como los servidores de alertas de emergencia.

La protección de todas las sedes remotas depende exclusivamente de un único firewall físico ubicado en la sede principal, lo que limita la capacidad de aplicar políticas por cada sede remota. Asimismo, estas sedes se encuentran vulnerables frente a ataques locales y amenazas internas, puesto que carecen de protección distribuida y de mecanismos de defensa independiente.

El modelo actual no se adapta eficientemente al crecimiento de la organización ni a la integración de nuevas tecnologías. La dependencia de enlaces MPLS encarece la operación y limita la flexibilidad para gestionar el tráfico y priorizar aplicaciones. Adicionalmente, la falta de segmentación adecuada y de visibilidad en tiempo real impide detectar de manera temprana incidentes de seguridad o fallas de conectividad, lo que incrementa el riesgo de interrupciones en los servicios esenciales.

Por otro lado, el esquema vigente limita la escalabilidad, dificultando la incorporación de nuevas sedes o la ampliación del ancho de banda cuando la demanda de usuarios y aplicaciones así lo requiere. Esta rigidez tecnológica impacta directamente en la continuidad operativa y en la eficiencia de los procesos institucionales.

En la Figura 1 se muestra la topología actual de la red, en la que se evidencia la concentración del tráfico en la sede principal, dado que todas las sedes se interconectan a esta sede mediante MPLS y salen a internet mediante la misma.

Esto pone de manifiesto la necesidad urgente de migrar hacia una arquitectura más moderna, distribuida y segura, que asegure la continuidad operativa, fortalezca la protección de todas las sedes y garantice la sostenibilidad tecnológica de la entidad en el mediano y largo plazo. Solo mediante una transformación tecnológica integral será posible responder de manera

oportuna a las emergencias, proteger la información sensible y asegurar la disponibilidad de los servicios en todo momento.

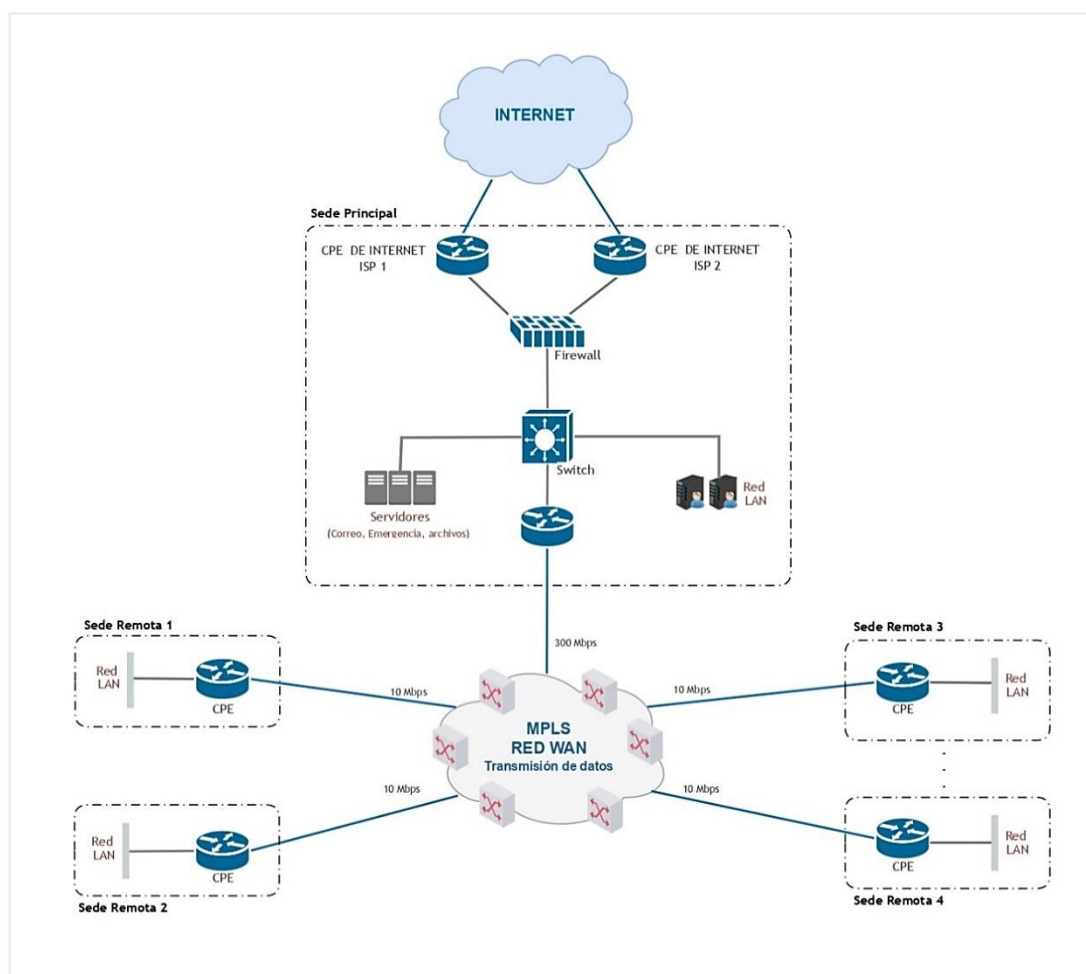


Figura 1: Topología física de red actual de la Entidad. Fuente. Elaboración propia.

3.3.1 Problema General

¿Cómo diseñar e implementar un esquema de conectividad basado en internet dedicado y firewall virtual para cinco sedes de una entidad gubernamental, migrando de una arquitectura centralizada a una solución más flexible, económica y compatible con entornos modernos, puede mejorar el ancho de banda, garantizar la seguridad de las comunicaciones y optimizar la operatividad de la Entidad?

3.3.2 Problemas Específicos

- ¿Cómo garantiza un enlace de internet dedicado en cada sede de la entidad una mejora en la conectividad y el rendimiento, reduciendo la latencia y optimizando el uso del ancho de banda disponible en cada sede?
- ¿Qué impacto tiene la implementación de una solución de seguridad perimetral virtualizada en VMware para proteger las sedes remotas de amenazas externas e internas, asegurando la aplicación de políticas de seguridad?
- ¿Cuál es el impacto de la implementación de esta nueva infraestructura en términos de costos operativos y qué beneficios económicos indirectos derivan de la mejora en la eficiencia operativa y la capacidad de respuesta ante emergencias?

3.3.3 Justificación e importancia de la investigación

El desarrollo de la investigación se justifica en la necesidad académica y en los aportes prácticos que el trabajo puede brindar al ámbito de las redes y telecomunicaciones, así como a la optimización de la infraestructura tecnológica de entidades gubernamentales. A continuación, se describen las razones que motivan el presente trabajo de suficiencia profesional:

- **Justificación por Conveniencia:** La investigación es conveniente debido a que aborda un problema crítico en la infraestructura de redes de una entidad gubernamental esencial. Diseñar una topología moderna y segura mejora la capacidad de respuesta en situaciones de emergencia y optimiza los recursos tecnológicos de manera eficiente.
- **Justificación Social:** Radica en que la entidad gubernamental es un organismo clave para la seguridad y el bienestar de la población. Los

beneficiarios son los colaboradores de las 5 sedes, ya que contarán con una infraestructura de red más segura y eficiente. Asimismo, se beneficia la sociedad en general, ya que la mejora en la conectividad y la seguridad de los sistemas tecnológicos de la entidad incrementa su capacidad para atender emergencias, salvando vidas y bienes.

- **Justificación Práctica:** Se abordan problemas reales de la actual infraestructura de red, como resolver la centralización de Internet en la sede principal. También mejora la seguridad perimetral mediante la virtualización de firewall, protegiendo las sedes remotas de ciberamenazas y garantizando una conectividad más estable y rápida hacia servicios críticos como el servidor de alertas de emergencia. Los resultados tienen un impacto práctico en la mejora de la topología de red y en la continuidad operativa de la entidad.
- **Justificación Teórica:** El presente trabajo aporta al ámbito académico y profesional, puesto que documenta la transición de una arquitectura de red centralizada (MPLS en topología Hub and Spoke) a una arquitectura descentralizada con Internet dedicado, seguridad virtualizada y VPN. Esto genera un conocimiento aplicable para futuras investigaciones.
- **Justificación Económica:** La solución propuesta optimiza el uso del ancho de banda, reduciendo costos asociados a ineficiencias en la conectividad. Además, minimiza los riesgos y costos derivados de interrupciones o vulnerabilidades de seguridad y permite escalabilidad sin necesidad de inversiones significativas adicionales, aumentando el retorno sobre la inversión.
- **Justificación Metodológica:** La investigación desarrolla una metodología replicable para el diseño y la evaluación de infraestructuras de red descentralizadas, así como para la implementación de soluciones de seguridad en la nube para infraestructuras críticas. Proporciona una guía de procedimiento para entidades con problemas similares.

3.4 Metodología

3.4.1 Bases teóricas

3.4.1.1 Antecedentes internacionales

- i. Citando a Diaz (2023) expresa es proyecto titulado “Análisis y Diseño de Seguridad Perimetral Basado en Software de Código Abierto para una Compañía en Crecimiento” la problemática del alto riesgo que conlleva no contar con seguridad perimetral en una empresa, lo cual incluye vulnerabilidades en los puntos de acceso a la red, falta de segmentación y escasa visibilidad del tráfico. Desde el punto de vista del autor, el objetivo es la implementación de un modelo de seguridad perimetral utilizando soluciones de software de código abierto para el enlace de internet dedicado de una empresa en proceso de expansión.

Se propone un diseño perimetral robusto que incorpora herramientas como cortafuegos de código abierto, sistemas de detección y prevención de intrusos (IDS/IPS), y una política de segmentación de red. Los resultados del estudio señalan que es posible fortalecer la seguridad sin necesidad de realizar una alta inversión, mejorando la protección de los datos corporativos y la gestión del acceso a los recursos digitales de la organización, demostrando ser una alternativa económica y eficiente para empresas en crecimiento.

- ii. Alagarsamy et al. (2022) en su artículo “A study of cloud-based VPN establishment using network function virtualization technique” analiza la implementación de Redes Privadas Virtuales (VPN) en entornos de nube mediante la Virtualización de Funciones de Red (NFV). El objetivo principal de los autores es proporcionar características de seguridad propias de las VPN sin depender de hardware dedicado, a diferencia de la MPLS que se basa principalmente en dispositivos de red de borde

que depende de los proveedores de servicios. Para lograrlo, se plantea trasladar las funciones de VPN desde dispositivos físicos específicos hacia servidores virtuales, donde se encuentran las plantillas de NFV.

Este enfoque permite una mayor flexibilidad y escalabilidad en la gestión de redes, debido a que al implementar las funciones de VPN como NFV, las organizaciones pueden reducir costos asociados al hardware físico y mejorar la eficiencia operativa, aprovechando la infraestructura de la nube y la virtualización. (Santhanamahalingam, Saravanan, & Karthikeyan, 2022)

- iii. De acuerdo con el trabajo de investigación de Morales et al. (2019) en su trabajo "Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información" menciona la importancia de prevenir amenazas internas y externas en una institución para mejorar tanto la protección de los enlaces de internet como la capacidad de respuesta ante ciberataques. El objetivo principal mencionado en el artículo es desarrollar la implementación de firewall de próxima generación (NGFW) desplegado en servidores virtualizados, integrando múltiples funciones de seguridad, como filtrado de URL, sistemas de prevención de intrusiones (IPS), antimalware, antivirus y sandboxing, las cuales deben operar de manera integrada para garantizar una salida a internet segura.

Se resalta la flexibilidad y escalabilidad de NGFW virtualizado, debido a que permite ajustar los recursos según el tráfico de datos. Brinda un sistema de monitoreo en tiempo real para mitigar posibles ataques y/o amenazas. Como resultados obtenidos, la solución perimetral mostró una alta detección y bloqueo de amenazas.

Asimismo, la tecnología virtualizada permitió optimizar los recursos de red y redujo los costos operativos, lo que demuestra escalabilidad y eficiencia en la implementación. (Morales, Toapanta, & Toasa, 2019)

3.4.1.2 Antecedentes nacionales

- i. Quintana, J. & Gallardo, E. (2021) en su tesis titulada “Diseño de una red VPN full mesh para mejorar la comunicación y seguridad en una empresa metalmecánica de Lima” señalan la problemática de una comunicación ineficiente entre las sedes de la empresa, como latencias, interrupciones en la transmisión de datos y falta de seguridad perimetral para la salida a internet. El objetivo principal de los autores es el diseño de una red VPN basada en IPSec con la finalidad de tener conexiones directas entre todas las sedes de la empresa (topología full mesh). Asimismo, se incluyó el dimensionamiento de un firewall virtualizado para mejorar la seguridad perimetral de la red.

La investigación tuvo una metodología descriptiva y experimental, debido a que se realizaron simulaciones y pruebas para evaluar parámetros como latencia, velocidad y pérdida de paquetes.

Como resultado, se obtuvo una reducción significativa de la latencia y un aumento en la velocidad de transmisión de datos entre sedes, lo que valida una mejora en la comunicación. En adición, se fortaleció la seguridad, puesto que se implementó una VPN cifrada y un firewall virtualizado para proteger información confidencial de la empresa. Finalmente, se demostró una optimización de recursos al diseñar una topología que no depende de un nodo central, ya que se redujeron costos operativos y se mejoró la fortaleza de la red. (Quintana, J. & Gallardo, E., 2021)

- ii. En el marco de Investigación de Paredes (2022), desarrolló un estudio titulado “Modelo de infraestructura de red VPN para interconexión segura de datos en la Universidad Nacional del Altiplano”, donde propone un modelo de infraestructura de red VPN para solucionar la problemática de seguridad en la interconexión de datos entre las diferentes sedes de la universidad. El objetivo principal del autor es la implementación de la VPN empleando

soluciones de software libre con el fin de optimizar los recursos económicos de la institución sin comprometer la integridad, confidencialidad y disponibilidad de los datos transmitidos. En los resultados se demuestra que el uso de tecnologías de bajo costo puede satisfacer las necesidades de conectividad segura, mejorando la eficiencia y el acceso a la información institucional.

Este estudio demuestra la viabilidad de las redes VPN con herramientas de código abierto en entornos educativos con limitaciones presupuestarias. (Paredes, 2020; Feknous, y otros, 2015)

- iii. De la Cruz, S. & Vera, J. (2020), en su investigación “Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo” menciona la problemática que presenta la intranet de la universidad, la cual está relacionada a la falta de acceso seguro de los usuarios remotos, lo que conlleva a enfrentar riesgos de interceptación de datos y accesos no autorizados a no contarse con una seguridad robusta.

Como objetivo del estudio se plantea el uso de la herramienta Open VPN, la cual es un software de código abierto que garantiza acceso seguro a las aplicaciones internas de la universidad.

La metodología de investigación tuvo un enfoque experimental, puesto que se compararon métricas de rendimiento de la red antes y después de la VPN, evaluando parámetros como velocidad y estabilidad de conexión y seguridad en la transmisión de datos.

En los resultados, se validó una mejora en seguridad debido a que la implementación de Open VPN fortaleció la seguridad de la información al reducir los riesgos de acceso no autorizado a la intranet de la universidad.

Además, al ser una herramienta de código abierto se eliminó la necesidad de adquirir licencias comerciales, por lo que la implementación de esta solución robusta tuvo un costo reducido.

En conclusión, la implementación de una VPN basada en software libre como Open VPN demostró ser una solución replicable para otras instituciones que cuenten con la misma problemática, debido a que es efectiva para mejorar la seguridad y accesibilidad y eficiencia en la gestión de las aplicaciones de intranet. (De la Cruz, S. & Vera, J., 2020)

3.4.2 Marco conceptual

En esta sección, se definen los conceptos base relacionados al presente Trabajo de Suficiencia Profesional, los cuales proporcionan una base sólida para el diseño e implementación y facilitarán a integración de las diferentes tecnologías en la solución propuesta.

3.4.2.1 Tipos de redes.

Citando a Tanenbaum & Wetherall (2012) en su libro “Redes de computadoras”, las redes se clasifican de acuerdo al alcance geográfico en:

- Red de Área Personal (PAN): Es aquella que permiten a los dispositivos comunicarse dentro de un rango de unos pocos metros. Un ejemplo es este tipo de red es una conexión inalámbrica entre una PC y sus periféricos, como un mouse o una impresora. En caso no haya una conexión inalámbrica es necesario realizar esta conexión mediante cable.
- Red de Área Local (LAN): Se trata de redes privadas con un área geográfica limitada, por lo que suelen operar solo en una casa, oficina o edificio. Su implementación más recurrente es para conectar computadoras personales y dispositivos finales con la finalidad de

compartir recursos e intercambiar información. Las redes LAN pueden ser inalámbricas, mediante el estándar IEEE 802.11 (más conocido como WiFi) o alámbricas, mediante cables de cobre o fibra óptica.

- Red de Área Metropolitana (MAN): Es aquella que se extiende sobre toda una ciudad. Conecta múltiples LAN y puede incluir servicio de Internet. Un ejemplo de estas redes es la televisión por cable. También el WiMAX es considerada una red MAN.
- Red de Área Amplia (WAN): Cubre áreas geográficas extensas para conectar redes distantes. Por lo general, las redes WAN cuentan con dos componentes: líneas de transmisión y elementos de conmutación. Las líneas de transmisión son aquellas que desplazan bits entre máquinas y el medio puede ser cobre, fibra óptica o enlaces de radio. Los elementos de conmutación hacen referencia a equipos especializados que conectan dos o más líneas de transmisión y enrutan los datos mediante una línea saliente.

La Figura 2 presenta la clasificación de los distintos tipos de redes en función de su alcance geográfico, partiendo de entornos reducidos como una red de área personal hasta llegar al Internet como red global.

1 m	Metro cuadrado	Red de área personal
10 m	Cuarto	Red de área local
100 m	Edificio	
1 km	Campus	
10 km	Ciudad	Red de área metropolitana
100 km	País	Red de área amplia
1000 km	Continente	
10000 km	Planeta	Internet

Figura 2: Clasificación de tipos de redes en base a la distancia geográfica. Fuente. Redes de Computadoras, por Tanenbaum & Wetherall (2012).

3.4.2.2 Topologías de red.

De acuerdo con Manage Engine (2024), una topología de red describe la disposición física o lógica de los dispositivos y conexiones dentro de una red informática, como computadoras, enrutadores y conmutadores. Representa cómo los componentes se organizan y comunican, lo que ayuda a mejorar la eficiencia y solucionar problemas rápidamente.

La importancia de una topología de red radica en optimizar el rendimiento y la velocidad de transferencia de datos. También facilita la comprensión de la infraestructura de red y sus dependencias. Identifica cuellos de botella al analizar cómo los dispositivos y aplicaciones se impactan entre sí y simplifica la resolución de problemas al permitir una visualización clara del sistema.

Las topologías de red se clasifican en físicas, las cuales muestran el diseño real del cableado y las conexiones, y lógica, las cuales muestran las rutas por las que viajan los datos en la red. Ambos enfoques son complementarios, ya que permiten entender tanto la infraestructura instalada como el comportamiento del tráfico dentro de la organización.

De acuerdo con Lederkremer, M. (2019) en su libro “Redes Informáticas”, las redes se clasifican según su topología en:

- Topología bus: Es aquella conecta todos los nodos directamente a través de enlaces individuales a un único canal de comunicaciones. Entre sus ventajas se encuentran la facilidad para añadir nuevos dispositivos y su escalabilidad. No obstante, presenta desventajas como la afectación de toda la red ante un fallo en el enlace y la disminución del rendimiento al incrementar más dispositivos.
- Topología anillo: Conecta los nodos formando un círculo, donde cada nodo recibe y retransmite la información en una sola dirección. Su rendimiento no disminuye al agregar más dispositivos. Sin embargo, cuenta con dificultad para detectar fallos, la falta de privacidad en las comunicaciones y la caída de toda la red si un nodo falla.

- Topología Estrella: Conecta todos los nodos con uno central. Los nodos periféricos transmiten información al concentrador, que se encarga de recibirla y enviarla a su destino. Sin embargo, un fallo en el nodo central puede provocar la caída de toda la red.
- Topología malla completa: En esta topología, cada nodo de la red posee un enlace punto a punto con cada uno de los demás nodos que también forman parte de la red. Es un tipo de red con tolerancia a fallos, ya que la caída de un nodo no afectará a la red.
- Topología mixta: Es la combinación de dos o más tipos de topología a mencionadas anteriormente. Se realiza su implementación debido a la complejidad de solución de red o por el aumento de dispositivos. Por otra parte, la configuración, administración y mantenimiento resultan costosos.

Tal como se presenta en la Figura 3, las redes pueden organizarse bajo distintas topologías físicas, cada una con ventajas y limitaciones en términos de rendimiento, escalabilidad y tolerancia a fallos.

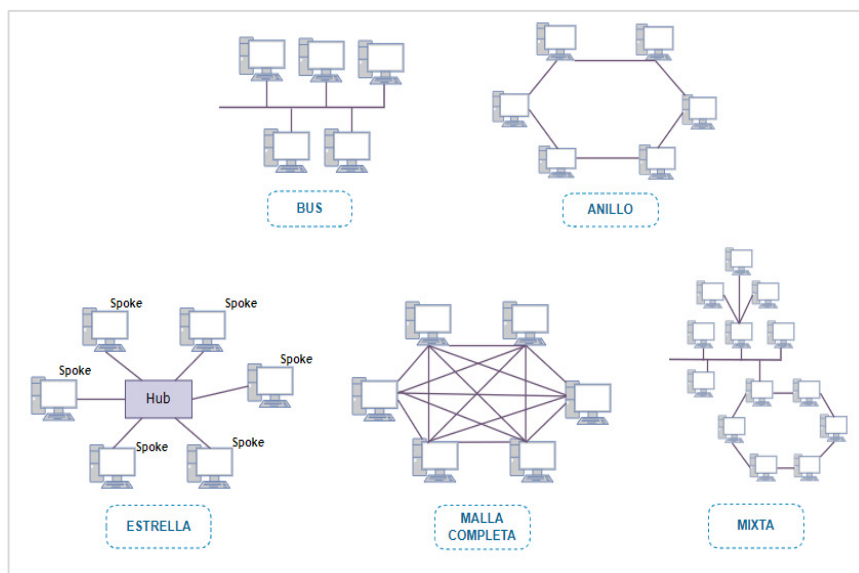


Figura 3: Tipos de redes según su topología física. Fuente. Elaboración propia.

3.4.2.3 Internet.

Internet es una red informática que interconecta miles de millones de dispositivos informáticos en todo el mundo. Inicialmente, estos dispositivos eran principalmente los tradicionales ordenadores de sobremesa, las estaciones de trabajo Linux y los denominados servidores que almacenan y transmiten información, como páginas web y mensajes de correo electrónico.

En la actualidad, se conectan más equipos a Internet, como ordenadores portátiles, teléfonos inteligentes, tablets, televisores, consolas de juegos, sistemas de seguridad para el hogar, electrodomésticos, autos, sistemas de control de tráfico y más, los cuales se denominan hosts o dispositivos finales. (Kurose & Ross, 2017)

En el presente apartado se describen los principales conceptos relacionados con el acceso y uso de Internet, los cuales resultan fundamentales para comprender la infraestructura de red propuesta:

- **ISP (Internet Service Provider):** Los proveedores de servicios de Internet (ISP) son aquellos que conectan a los usuarios finales y a las empresas a la red pública de Internet. Compiten entre sí en cuanto a precio, rendimiento, fiabilidad, etc., pero también deben cooperar entre sí para proporcionar conectividad global a todos los demás anexos de Internet. Ofrecen diversos tipos de conexión, como cable, DSL, fibra óptica, acceso telefónico y tecnologías inalámbricas. (Norton, W., 2001)
- **Customer Premises Equipment (CPE):** Son dispositivos ubicados en las instalaciones del cliente que se conectan a la red de un proveedor de servicios. Este equipo desempeña un papel crucial en las telecomunicaciones y el acceso a Internet. Hay tipos de CPE, como los Módems que son dispositivos que modulan y demodulan señales para la transmisión de datos a través de líneas telefónicas o sistemas de cable. También se encuentran los Enrutadores, los cuales se encargan de enrutar datos entre diferentes redes, lo que permite que varios dispositivos compartan una única conexión a Internet. Finalmente, los

Gateways o Puertas de enlace son dispositivos que funcionan como una "puerta" entre dos redes, a menudo combinando las funciones de un módem y un enrutador. (Muhammad, Nor, Ramli, & Ahmad, 2022)

- Point of Presence (PoP): Es un punto de acceso físico que conecta a los usuarios a Internet o a la red de un proveedor de servicios. Funciona como un componente crítico en las telecomunicaciones, permitiendo la conectividad y facilitando el intercambio de datos entre distintas redes.

Los PoP son esenciales para conectar varias redes, puesto que permiten que los datos fluyan entre ellos. Funcionan como puertas de enlace para que los ISP lleguen a los usuarios finales. Comprender la topología a nivel de PoP ayuda a optimizar el rendimiento de la red y garantiza la confiabilidad para desarrollar protocolos que respalden la comunicación fluida entre redes interconectadas. (Feknous et al., 2024)

Estos se ubican estratégicamente en varias áreas geográficas para maximizar la cobertura y minimizar la latencia para los usuarios, permitiendo múltiples conexiones entre sistemas autónomos con la finalidad de mejorar la solidez de la conectividad a Internet. (Nur & Tozal, 2024)

- Dirección IP: Es una etiqueta numérica asignada a cada dispositivo conectado a una red que utiliza el Protocolo de Internet para la comunicación. Esta dirección permite identificar y localizar dispositivos en una red, facilitando la transmisión de datos. Es única para cada conexión, por lo que no se puede acceder a internet si el dispositivo final no cuenta con una dirección IP. (Cabello, 2017)

3.4.2.4 Internet Dedicado de fibra óptica

Flores J. (2023) describe el Internet dedicado como un servicio de conectividad de alta velocidad y confiabilidad, que utiliza fibra óptica para garantizar una transmisión de datos rápida y eficiente. A diferencia de las conexiones de Internet compartido, como las residenciales o las redes públicas, el Internet dedicado está orientado específicamente a satisfacer las

necesidades de empresas y organizaciones que demandan un acceso a Internet de alto rendimiento. A continuación, se mencionan las características:

- Gran velocidad de conexión: Debido a que es una conexión basada completamente en fibra óptica, hay mínimas posibilidades de alteración en la velocidad o interferencias causadas por emisiones radioeléctricas de otros dispositivos. Gracias a ello, se pueden brindar velocidades de hasta 10 Gbps de Internet simétrico, garantizando además una latencia muy baja en el servicio. (Flores, 2023)
- Escalabilidad del servicio: Una conexión dedicada puede adaptarse al crecimiento de las operaciones y al aumento en el volumen de la empresa, garantizando así la continuidad y el soporte necesario durante los procesos de expansión. (Flores, 2023)
- Servicio dedicado al cliente: Como servicio corporativo, el Internet dedicado incluye soporte técnico especializado proporcionado por el proveedor de servicios de Internet (ISP), lo que garantiza su calidad y fiabilidad. Este soporte permite resolver contingencias de manera oportuna y facilita la escalabilidad del servicio según las necesidades de la organización. (Flores, 2023)
- Confiabilidad: Permite cuantificar qué tan seguro y consistente es un servicio prestado bajo condiciones previamente acordadas. Una de las principales ventajas del Internet dedicado es el aumento significativo en la confiabilidad de sus enlaces. Este tipo de conexión incluye Acuerdos de Nivel de Servicio (SLA, por sus siglas en inglés), que garantizan una disponibilidad del servicio extremadamente alta. En adición, los SLA especifican parámetros clave, como niveles de latencia y pérdida de paquetes, asegurando un rendimiento óptimo en todo momento. (Zapata, 2022)
- Desempeño: Debido a que se trata de una conexión exclusiva, un servicio de Internet dedicado proporciona al cliente acceso único y completo al ancho de banda contratado, el cual es 100 % garantizando.

Esto significa que nadie más puede utilizar esos recursos, lo cual asegura un rendimiento de conexión constante en todo momento, independientemente de la hora o de los picos de tráfico que puedan ocurrir durante el día. (Zapata, 2022)

La contratación de Internet dedicado puede generar importantes beneficios para grandes corporaciones, instituciones financieras, cadena de restaurantes y cualquier organización de gran escala que requiera garantizar la continuidad de sus operaciones.

De acuerdo con C3ntro Telecom (2023), el internet dedicado, además de proporcionar velocidades de ancho de banda significativamente mejoradas, ofrece numerosos beneficios adicionales para las empresas, tales como:

- Videoconferencias de alta calidad y eficiencia: Una conexión dedicada garantiza imágenes más nítidas y sonido claro, permitiendo a los participantes concentrarse en el propósito de la reunión en lugar de lidiar con problemas técnicos.
- Tiempos de respuesta más ágiles para herramientas en línea: Con la creciente popularidad de las herramientas basadas en la web en empresas de diversas industrias, una conexión rápida y confiable es clave para aprovechar al máximo sus beneficios.
- Mayor seguridad en la red: Al utilizar Internet dedicado, la conexión no se comparte con usuarios externos, lo que minimiza los riesgos de violaciones de seguridad y protege la información de la organización.

3.4.2.5 Fibra óptica.

En el marco de investigación de Rodríguez Y. (2009), la fibra óptica es un medio de transmisión que está compuesto por materiales ópticos mucho más ligeros. Estos materiales no solo son más económicos que los convencionales de cobre usados en telefonía, sino que también permiten que los cables sean mucho más finos. Como resultado, en el espacio donde antes solo cabía un cable de cobre, ahora pueden instalarse muchos más cables de fibra óptica.

Los circuitos de fibra óptica son finos filamentos hechos de vidrio, compuesto por cristales naturales, o de plástico, formado por cristales artificiales. Tienen un grosor similar al de un cabello humano, entre 10 y 300 micrones, y transportan mensajes mediante haces de luz que atraviesan su longitud de un extremo a otro.

De acuerdo con el autor Vargas I.A. (2014) la fibra óptica cuenta con las siguientes características generales:

- Cobertura más resistente: La resistencia al agua, hongos y radiación ultravioleta, junto con una cubierta duradera, un buffer de 900 μm , fibras ópticas sometidas a pruebas de 100 kpsi, y un rendimiento ambiental mejorado, garantizan mayor fiabilidad a lo largo de su vida útil. Asimismo, los avances recientes en protección contra incendios reducen el riesgo asociado a las instalaciones antiguas de fibra óptica, las cuales utilizaban cubiertas de materiales inflamables y gel de relleno, también inflamable.
- Empaquetado de alta densidad: Al incorporar la mayor cantidad de fibras en el menor diámetro posible, se logra una instalación más rápida y sencilla, especialmente en situaciones donde el cable debe soportar curvas pronunciadas y espacios reducidos. Se ha desarrollado un cable de construcción ultradensa con 72 fibras, cuyo diámetro es un 50% menor en comparación con los cables tradicionales.

Clases de Fibra óptica

Se cuentan con diferentes clases de fibra óptica, según el modo de propagación y según su composición. (Vargas, 2014)

i. Según el modo de propagación:

- Fibra monomodo: Esta fibra se caracteriza por ofrecer una mayor capacidad de transmisión de información, con una banda de paso de aproximadamente 100 GHz/km. Debido a que permite mayores flujos de datos, su implementación es compleja. Se conoce como monomodo

porque sólo transmite rayos que siguen el eje de la fibra, tiene un núcleo de entre 5 y 8 micrómetros, similar a la longitud de onda de las señales ópticas que transporta. Aunque su principal ventaja es la alta capacidad de transmisión, su pequeño tamaño dificulta el manejo y la conexión.

- **Fibra multimodo:** Una fibra multimodo se utilizan principalmente en aplicaciones de corta distancia, generalmente menores a 1 km, debido a que tienen más de mil modos de propagación, son económicas y fáciles de diseñar. Su distancia máxima es de 2 km y utilizan diodos láser de baja intensidad. El núcleo de las fibras multimodo tiene un índice de refracción ligeramente superior al de su revestimiento, lo que, junto con su mayor tamaño, facilita la conexión y tolera componentes de menor precisión.

Según el sistema de clasificación de fibras multimodo ISO 11801, la fibra óptica se divide en OM1, OM2, OM3 y OM4 según su ancho de banda. En la Figura 4 se presentan las características comparativas de cada tipo de fibra, detallando parámetros como velocidad de transmisión, distancia máxima y frecuencia. Esta información permite seleccionar la fibra adecuada según las necesidades de cada proyecto, garantizando un balance entre rendimiento, alcance y costos.

Tipo de fibra multimodo	Velocidad transmisión (Gbps)	Distancia máxima (m)	Frecuencia (MHz)	Costo
OM1	1	550	275	Económico
OM2	10	550	500	Económico
OM3	10	300	1000	Alto
OM4	40	400	1000	Alto

Figura 4: Comparación de parámetros de tipos de fibra multimodo.
Fuente. Adaptado de AscentOptics (2023)

ii. Según su composición:

- Núcleo de plástico y cubierta plástica: Las fibras de plástico ofrecen varias ventajas frente a las de vidrio, como ser más flexibles, resistentes y fáciles de instalar. También soportan mejor la presión, son más económicas y pesan alrededor de un 60% menos que las de vidrio. Sin embargo, su principal desventaja es la alta atenuación, lo que significa que no transmiten la luz de manera tan eficiente como las de vidrio. Por ello, su uso se limita a distancias cortas, como dentro de un edificio.
- Núcleo de vidrio con cubierta de plástico: Esta fibra es frecuentemente llamada fibra PCS debido al núcleo silicio y cubierta de plástico. Son menos afectadas por la radiación por lo que se usan para aplicaciones militares.
- Núcleo de vidrio y cubierta de vidrio: Esta fibra es frecuentemente llamadas SCS, debido a su núcleo de silicio y cubierta de silicio. Tiene una baja atenuación, sin embargo, son menos resistentes y más susceptibles a un aumento en la atenuación cuando están expuestas a la radiación.

3.4.2.6 Seguridad Perimetral.

Hubbard, B. (2022) define un perímetro de red como la frontera que separa la intranet privada de una organización del entorno público de Internet. Este límite es crucial para proteger la información y los recursos confidenciales, manteniéndolos fuera del alcance del público y de posibles atacantes malintencionados.

Por ello, se define el término de Seguridad Perimetral como el proceso garantizar la seguridad del perímetro de una red mediante a integración de software, dispositivos y técnicas especializadas. A continuación, se describen los componentes claves que ayudarán a mejorar la seguridad perimetral de la entidad mencionada en el presente trabajo:

- Firewall virtual: Controla el tráfico de red entrante y saliente en función de políticas de seguridad predefinidas. Su función principal es bloquear accesos no autorizados mientras permiten el tráfico legítimo. (Marín et al., 2020). Un firewall virtual ofrece un alto nivel de capacidad, continuidad y disponibilidad. Debido a que se encuentra alojado en un centro de datos dedicado, cuenta con el respaldo de una infraestructura robusta. Además, la escalabilidad de un firewall virtual permite incrementar recursos de hardware sin las limitaciones de un dispositivo físico. También presenta la ventaja de una administración unificada. (Camacho & Lopez, 2017).
- Red Privada Virtual (VPN) de Software cliente: Red Privada Virtual que utiliza software instalado en dispositivos individuales (como laptops, computadoras de escritorio o móviles) para establecer conexiones seguras con redes o servidores remotos. Es especialmente útil para trabajadores remotos o sucursales que requieren acceso seguro a recursos centralizados a través de Internet. De acuerdo con Ardila, N. (2019), los principios de seguridad para una VPN son los siguientes:
 - Autenticación y Autorización: Verifica la identidad de los usuarios mediante credenciales (nombre de usuario, contraseña, autenticación multifactor) antes de otorgar acceso.
 - No Repudio: Asegura que las acciones realizadas en la red sean atribuibles a usuarios autenticados.
 - Integridad: Garantiza que la información transmitida no sea alterada.
 - Confidencialidad: Cifra los datos enviados y recibidos para protegerlos de interceptaciones, utilizando protocolos como OpenVPN, IKEv2 o IPSec.

Pomar R. (2019) menciona dentro de los beneficios de una VPN software cliente la compatibilidad con diversos sistemas operativos

como Windows, macOS, Linux, iOS y Android permite una implementación flexible y accesible para todos los usuarios. En términos de costos, una VPN de software cliente representa una reducción de costos significativa en comparación con las redes privadas tradicionales, al eliminar la necesidad de líneas dedicadas y hardware costoso.

3.4.2.7 VM-Series: Next Generation Firewall Virtual.

VM-Series representa la versión virtualizada del firewall de próxima generación de Palo Alto Networks. Está diseñada para abordar la creciente demanda de seguridad en línea en diversos entornos de nube y virtualización.

Puede implementarse en una amplia variedad de plataformas de computación en la nube, tanto públicas como privadas, incluyendo VMware, Cisco ACI y ENCS, KVM, OpenStack, Amazon Web Services, Microsoft Azure (nubes públicas y privadas), OCI y Google Cloud Platform. Además, VM-Series se integra de manera nativa con herramientas de automatización, lo que permite una gestión más ágil y escalable en entornos de nube híbrida. (VM-series, 2024)

VM-Series protege aplicaciones y datos gracias a sus avanzadas funciones de seguridad de última generación y a sus capacidades de automatización y administración centralizada, permitiendo integrar la seguridad directamente en los procesos de desarrollo de aplicaciones, asegurando que esta se mantenga alineada con el dinámico ritmo de las operaciones en la nube. De acuerdo con Strata de Palo Alto Networks (2024), las funcionalidades claves de este firewall virtualizado son las siguientes:

1. Visibilidad de aplicaciones para decisiones de seguridad: La serie VM proporciona visibilidad completa sobre las aplicaciones en todos los entornos de nube, permitiendo obtener información relevante que facilita la toma de decisiones rápidas y fundamentadas en la configuración de políticas de seguridad.

2. Segmentación y control de acceso para seguridad y cumplimiento: Con políticas de segmentación granulares, VM-Series permite controlar las aplicaciones que se comunican entre diferentes subredes, bloqueando el movimiento lateral de amenazas y asegurando el cumplimiento de las normativas de seguridad.
3. Prevención de amenazas avanzadas dentro de los flujos de aplicaciones: La integración nativa con servicios avanzados de seguridad, como la Prevención de Amenazas Avanzadas, Seguridad Avanzada de DNS, WildFire Avanzado, y Filtrado Avanzado de URL, permite bloquear vulnerabilidades y evitar la propagación de malware dentro de las aplicaciones de la nube, protegiendo contra amenazas tanto conocidas como desconocidas.
4. Control de acceso mediante políticas de Zero Trust: Integración con repositorios de usuarios como Microsoft Exchange, Active Directory y LDAP para enriquecer las políticas de acceso a aplicaciones basadas en la identidad del usuario.
5. Escalabilidad y Flexibilidad según las Necesidades Inmediatas: VM-series permite ajustar el rendimiento y los servicios de seguridad de acuerdo a las necesidades inmediatas, garantizando la flexibilidad necesaria para adaptarse a los cambios rápidos en la infraestructura en la nube. Esto se logra mediante el modelo de créditos de Software NGFW, que permite la reconfiguración de los recursos virtuales desde 2 vCPUs hasta 64 vCPUs en cuestión de minutos.
6. Consistencia en las políticas a través de la gestión centralizada: Panorama y Strata Cloud Manager ofrecen una gestión centralizada para los firewalls VM-Series, garantizando una implementación coherente de políticas en despliegues en la nube y en entornos físicos.

La capacidad de registro y reporte centralizado permite una visibilidad completa sobre las aplicaciones, usuarios y contenidos virtualizados.

En la Figura 5, se muestra la interfaz de Panorama para la gestión centralizada de VM-Series, mediante la cual se tiene una vista gráfica interactiva de la siguiente información (Palo Alto Networks, 2021):

- Visibilidad de tráfico y aplicaciones: Identifica qué aplicaciones están siendo ejecutadas en la red. También detalla los usuarios y dispositivos conectados y muestra patrones de tráfico entre diferentes segmentos de la red, incluyendo volumen y dirección.
- Amenazas y seguridad: Se visualizan detalles de intentos de intrusión, malware detectado, ataques de phishing, y otras amenazas bloqueadas. Proporciona informes sobre amenazas detectadas por servicios como WildFire, Threat Prevention y DNS Security y muestra los eventos críticos que requieren de una atención inmediata.
- Administración de políticas: Permite observar, gestionar y actualizar las políticas de seguridad aplicadas en los dispositivos. En adición, Identifica posibles desviaciones respecto a políticas corporativas o regulatoria.
- Gestión de dispositivos: Estado de los dispositivos, como uso de CPU, memoria y actualizaciones pendientes; configuraciones centralizadas desde un único panel y log de dispositivos para registrar el historial y eventos y cambios efectuados en los dispositivos administrados.
- Análisis de reportes: Brinda reportes personalizables sobre el tráfico, uso de aplicaciones, detección de amenazas y cumplimiento. Asimismo, muestra tendencias de seguridad y paneles en tiempo real para el monitoreo en línea.
- Integración y automatización: Muestra la visualización de grupos de direcciones dinámicas para políticas automatizadas. Asimismo,

cuenta con compatibilidad de APIs para administrar procesos basados en integración de plataformas de terceros.

Finalmente, cuenta con Log de integraciones, mediante el cual se puede realizar el seguimiento de datos recibidos desde plataformas externas como un SIEMs. De esta manera, se garantiza una correlación más eficiente de eventos de seguridad y una respuesta más rápida frente a incidentes críticos.

- Monitoreo de actividades por usuario: Rastrea actividades realizadas por usuarios y visualiza accesos basados en credenciales, roles y ubicación.

Esto contribuye a una mayor trazabilidad y facilita el cumplimiento de normativas de auditoría y seguridad. Además, permite detectar comportamientos inusuales o intentos de acceso no autorizados en tiempo real.

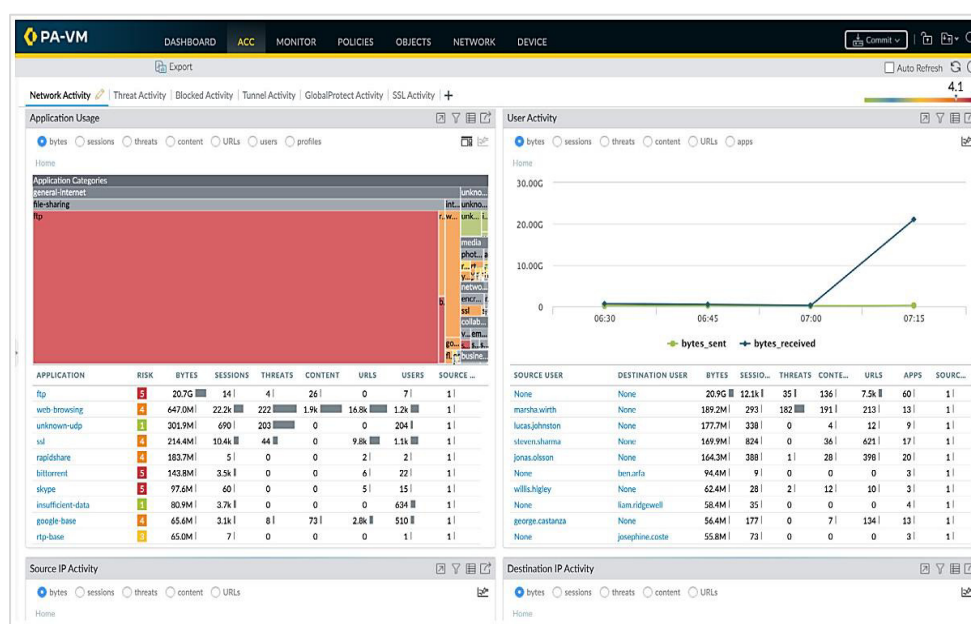


Figura 5: Dashboard de Panorama para la gestión centralizada de VM-Series. Fuente. Centralized Visibility and Automation, por Palo Alto Networks (2021).

7. Automatización en el despliegue y actualización de políticas de seguridad:

- **Provisionamiento automático:** La VM-series utiliza procesos para configurar automáticamente un firewall, incluyendo licencias, suscripciones y conexión con Panorama para la gestión centralizada.
- **Actualizaciones automáticas de políticas:** Usando APIs documentadas y grupos de direcciones dinámicas, las políticas de seguridad pueden adaptarse automáticamente a medida que cambian las cargas de trabajo, con la capacidad de ajustar dinámicamente las políticas basadas en etiquetas en entornos de nube públicos.
- **Integración con herramientas de terceros:** Se puede automatizar el despliegue y la actualización de políticas utilizando herramientas de automatización de terceros como Terraform y Ansible, garantizando que las políticas de seguridad se mantengan sincronizadas en todo momento.

Casos de Uso de la Serie VM de Palo Alto Networks

La Serie VM se adapta a diversos escenarios, permitiendo la implementación de seguridad avanzada en entornos virtualizados y de nube. A continuación, se describen los principales casos de uso:

- En nubes públicas, es compatible con plataformas como Amazon Web Services (AWS), Google Cloud, Microsoft Azure, Oracle Cloud y Alibaba Cloud. Brinda protección contra amenazas conocidas y desconocidas, asegurando el cumplimiento del modelo de responsabilidad compartida de la nube. Además, ofrece escalabilidad y simplicidad en la gestión para empresas que requieran seguridad robusta en entornos dinámicos.
- En centros de datos virtuales y nubes privadas, se puede implementar en entornos como VMware ESXi, Microsoft Hyper-V, KVM y Nutanix. Estos

permiten crear zonas de confianza que segmentan aplicaciones críticas y protegen datos sensibles frente a movimientos laterales de amenazas, además de cumplir con estándares regulatorios mediante microsegmentación y prevención de amenazas.

- VM-Series traslada aplicaciones tradicionales a la nube con seguridad integrada. Esto asegura que las aplicaciones estén protegidas tanto durante como después de la migración, garantizando su funcionamiento continuo y seguro.
- Está diseñado para proteger servicios SaaS y aplicaciones nativas en ejecución continua, integrando visibilidad y control granular para adaptarse a los rápidos cambios en los entornos de desarrollo y operación.
- Centraliza la gestión de seguridad en sucursales, data centers y nubes públicas desde un único panel de control, asegurando la segmentación y prevención de intrusiones en ubicaciones remotas.
- En entornos con SD-WAN, es compatible con despliegues tipo hub-and-spoke o arquitecturas mesh para pequeñas y medianas empresas. Garantiza conectividad segura entre sucursales, centros de datos y aplicaciones SaaS mediante firewalls virtuales.
- En redes 5G, la Serie VM ofrece protección avanzada para infraestructuras móviles, extendiendo políticas de Zero Trust a redes 5G y entornos MEC (Multi-access Edge Compute). Gracias a la integración de capacidades de machine learning, detecta y mitiga amenazas específicas del entorno.
- En escenarios de infraestructura de escritorios virtuales (VDI), los firewalls virtuales aseguran la segmentación y protegen el tráfico hacia y desde escritorios virtuales, inspeccionando el tráfico para garantizar la integridad y seguridad de los datos corporativos.

Estos casos de uso resaltan la versatilidad y eficacia de VM-Series para adaptarse a las necesidades de seguridad en distintos tipos de organizaciones y escenarios tecnológicos. Asimismo, su capacidad de escalabilidad y soporte

para arquitecturas modernas garantiza que pueda seguir respondiendo a los desafíos emergentes de ciberseguridad en entornos cada vez más distribuidos y dinámicos.

Definición de VM-Series en VMware

Para efectos del presente trabajo de investigación, se definirá el despliegue del firewall virtualizado en VMware.

Según Palo Alto Networks, las instancias virtualizadas del Firewall en entornos VMware permiten la implementación automatizada de capacidades avanzadas de seguridad, como la prevención exhaustiva de amenazas y la inspección a nivel de capa de aplicación del tráfico microsegmentado.

De igual manera, este enfoque contribuye a optimizar la utilización de recursos de red y a mantener la continuidad operativa en infraestructuras críticas.

Dentro de las capacidades de la serie VM en VMware encuentra el prevenir amenazas conocidas y desconocidas en los límites de confianza norte-sur y este-oeste en entornos microsegmentados, también la implementación automática de firewalls sin intervención manual y los grupos de seguridad nativos para aplicar automáticamente políticas de firewall a nuevas cargas de trabajo.

Arquitecturas de SDDC y VMware

Las arquitecturas de Centros de Datos Definidos por Software (SDDC) virtualizan la infraestructura de computación, almacenamiento y redes, lo que permite simplificar las operaciones, acelerar el aprovisionamiento de infraestructura y servicios de red, y mejorar significativamente la seguridad del centro de datos. VMware es una plataforma de virtualización de red que simplifica las redes en los SDDC, incluidos los entornos de nube híbrida. Los firewalls de la serie VM garantizan que el tráfico sea suficientemente inspeccionado en busca de amenazas. (Palo Alto Networks, 2017)

En la tabla 1, se muestran los componentes de la solución conjunta entre Palo Alto Networks y VMware:

Tabla 1: Componentes de la solución de Firewall virtualizado Palo Alto Networks y VMware NSX-T.

Componentes de VMware	
vCenter/ESXi	El servidor vCenter es la herramienta de administración centralizada de la suite vSphere. ESXi es un hipervisor que permite la virtualización de cómputo.
NSX-T Manager	Se requiere NSX-T Manager para implementar el firewall VM-Series en los hosts ESXi dentro de un clúster ESXi.
Componentes de Palo Alto Networks	
PAN-OS	La imagen base de VM-Series es necesaria para implementar el firewall de VM-Series en NSX-T. El requisito mínimo del sistema para implementar el firewall VM-Series para NSX en el servidor ESXi depende del modelo de VM-Series.
Panorama	Panorama es la herramienta de gestión centralizada para los firewalls de última generación de Palo Alto Networks. En esta solución, Panorama trabaja con NSX-T Manager para implementar, otorgar licencias y administrar de forma centralizada la configuración y políticas del firewall VM-Series para NSX-T. Panorama debe poder conectarse al NSX-T Manager, a los firewalls VM-Series y al servidor de actualización de Palo Alto Networks.
Complemento Panorama para VMware NSX	3.0.0 o posterior
Complemento de la serie VM	1.0.6 o posterior
Firewall de la serie VM	Modelos: VM-100, VM-300, VM-500 y VM-700

Fuente. Adaptado de Palo Alto Networks (2021), VM-Series Deployment Guide, sección “Components of the VM-Series Firewall on NSX-T (North-South)”.

Capacidades principales de la integración de VMware y la serie VM

Palo Alto Networks destaca las siguientes capacidades de integración entre VMware y la serie VM, las cuales resultan esenciales para fortalecer la seguridad perimetral, optimizar la administración de recursos en entornos virtualizados y garantizar la continuidad operativa de las organizaciones:

- **Protección avanzada contra amenazas y seguridad de red:** Los firewalls de la serie VM ofrecen capacidades para proteger contra amenazas conocidas y desconocidas, como exploits, malware, ransomware, spyware y amenazas persistentes avanzadas. El tráfico saliente se controla de manera granular mediante servicios de filtrado de URL y seguridad DNS, garantizando así una protección adaptable frente al panorama cambiante de ciberamenazas.
- **Gestión centralizada de seguridad:** Panorama actúa como una solución de gestión centralizada para administrar múltiples despliegues de VMware y otros entornos, incluidos nubes públicas como AWS, GCP y Azure, así como redes físicas, permitiendo aplicar políticas consistentes y obtener visibilidad integral en tiempo real.
- **Implementación automatizada de firewalls virtuales de la serie VM:** Panorama se comunica con NSX Manager para registrar la serie VM como un servicio de seguridad. NSX-T Manager implementa automáticamente los firewalls de la serie VM en los nodos de transporte de NSX, optimizando los tiempos de despliegue y reduciendo la complejidad operativa.
- **Políticas de seguridad dinámicas basadas en aplicaciones, contenido y usuarios:** Las nuevas cargas de trabajo virtualizadas se añaden automáticamente a los grupos de seguridad en NSX-T Manager y son reconocidas por Panorama y los firewalls de la serie VM.
- **Redirección de tráfico sin interrupciones a la seguridad de próxima generación:** El firewall distribuido de NSX dirige el tráfico permitido

hacia la serie VM sin necesidad de configuraciones manuales en los elementos de red virtual.

- Escalabilidad y flexibilidad: La integración de VMware NSX con la VM-Series permite escalar la infraestructura de seguridad de manera flexible y eficiente, sin depender de costoso hardware físico. VMware ofrece la capacidad de distribuir y mover máquinas virtuales y redes con facilidad, mientras que la VM-Series se adapta a estos cambios, garantizando la aplicación consistente de políticas de seguridad en todo el entorno.

3.5 Procedimiento

La presente sección tiene como objetivo detallar el procedimiento técnico diseñado para resolver la problemática planteada en el presente TSP. Dicho procedimiento se organiza en dos fases principales: Diseño inicial e Implementación de la infraestructura, que en conjunto permiten garantizar la validez técnica de la propuesta y la continuidad operativa de la red.

3.5.1 Diseño inicial de la investigación

En esta etapa se establecen los componentes clave del proyecto, considerando las necesidades específicas de la entidad y los requerimientos de conectividad. El proceso contempla la elaboración de la topología de red bajo un esquema descentralizado, el análisis de factibilidad de la fibra óptica y la definición de parámetros de calidad de servicio tales como disponibilidad, latencia y resiliencia ante fallos. Asimismo, se lleva a cabo el dimensionamiento de los equipos CPE en las sedes remotas y del firewall virtual en el datacenter, definiendo las capacidades de ancho de banda y seguridad necesarias. De manera complementaria, se identifican los lineamientos técnicos que servirán como base para la fase de implementación.

3.5.1.1 Descripción de topología.

La red propuesta adopta un modelo descentralizado, donde la Sede Principal y las Sedes Remotas cuentan con conexión directa a Internet dedicado y seguridad perimetral mediante firewalls virtuales. Este esquema asegura independencia operativa y resiliencia ante fallos en un enlace individual.

La Sede Principal actúa como núcleo del sistema, albergando el servidor de alertas de emergencia. Además, dispone de un firewall propio y un enlace de Internet dedicado adicional como contingencia. La Figura 6 muestra la topología propuesta, donde se evidencian sus principales componentes y la forma en que se interconectan.

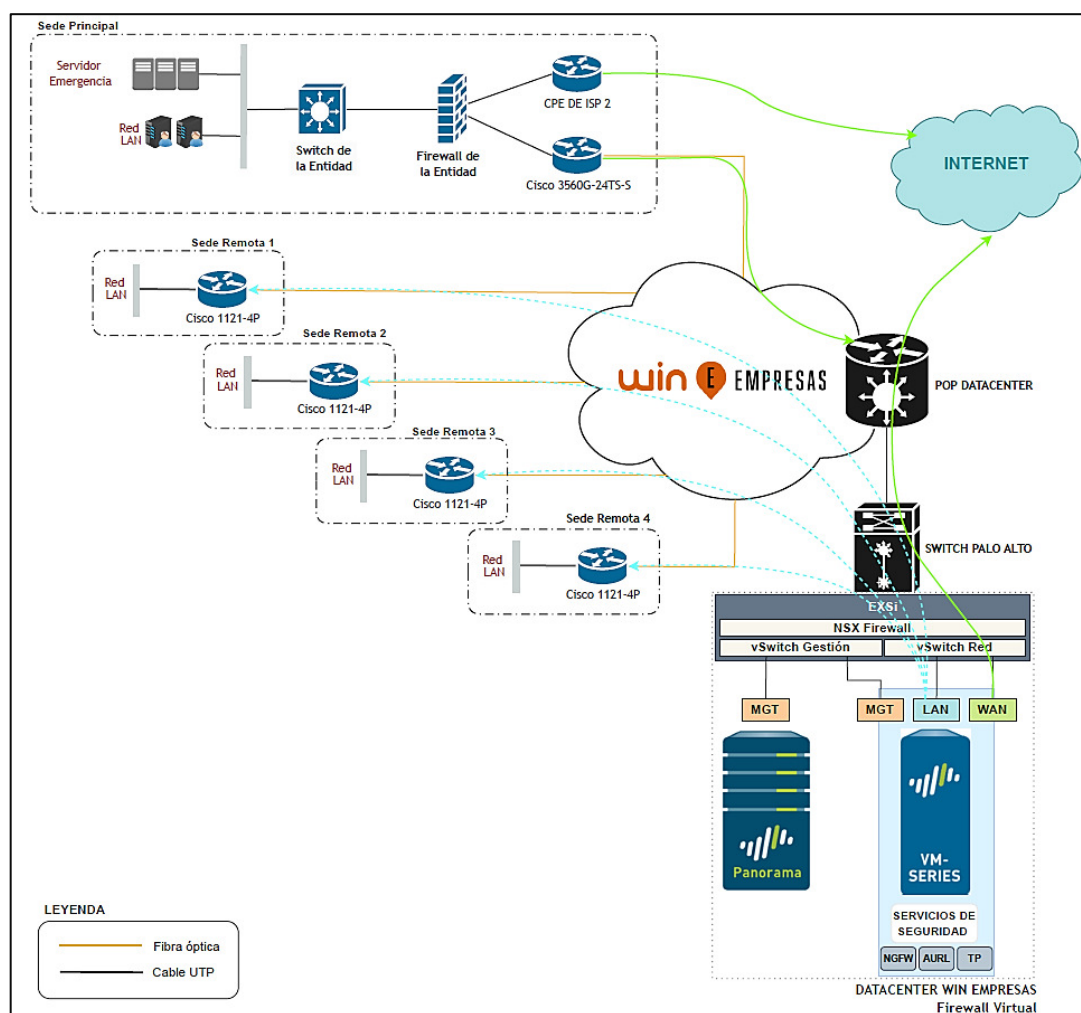


Figura 6: **Topología de red de solución actual.** Fuente. Elaboración propia.

3.5.1.2 Dimensionamiento de Internet Dedicado

El dimensionamiento de los enlaces de Internet Dedicado se basa en parámetros técnicos como el ancho de banda, cantidad de usuarios concurrentes y dispositivos, tipo de aplicaciones utilizadas, volumen de tráfico, latencia, tiempo de respuesta, escalabilidad y acuerdos de nivel de servicio. A continuación, se muestran las características definidas:

- Tipo de conexión: Servicio de conexión exclusiva para cada sede de la Entidad, es decir, no es compartida con otras entidades y/o usuarios externos, lo que garantiza un rendimiento constante.
- Última milla: El medio de transmisión es fibra óptica debido a que soporta mayores anchos de banda y es de baja latencia, a diferencia de medios de transmisión como el cobre o radioenlace.
- Ancho de banda: Debido que la Entidad utiliza aplicaciones que requieren alta capacidad de carga, se ha definido una conexión simétrica para que las velocidades de subida y bajada sean iguales. Las velocidades contratadas, las cuales deben estar garantizadas en al menos 90%, son las siguientes:
 - La Sede Principal dispone de 1 Gbps simétrico, tanto de subida como de bajada, lo que garantiza alta disponibilidad para los servicios críticos.
 - Las Sedes Remotas cuentan con 200 Mbps simétricos (subida y bajada), suficiente para el acceso a recursos institucionales y aplicaciones en línea.

Análisis de dimensionamiento de ancho de banda en la Sede Principal:

- Volumen de tráfico y tipo de aplicaciones: En la sede principal se encuentran la mayor parte de las operaciones críticas de la Entidad, incluyendo servidores de aplicaciones, bases de datos, sistemas de gestión empresarial y servicios de comunicación como

videoconferencias y VoIP. Estas aplicaciones demandan un alto ancho de banda para garantizar un rendimiento óptimo y una experiencia de usuario fluida.

- **Usuarios concurrentes:** La sede principal cuenta con un mayor número de colaboradores y dispositivos conectados simultáneamente, lo que incrementa la demanda de ancho de banda. Un enlace de 1 Gbps garantiza que todos los usuarios puedan acceder a los recursos de red sin interrupciones ni cuellos de botella.
- **Escalabilidad:** Se proyecta que la Entidad cuente con un crecimiento tanto de usuarios concurrentes como de aplicaciones, así como la incorporación de nuevos servicios que requerirán mayor capacidad de transferencia de datos. Un enlace de 1 Gbps proporciona la flexibilidad necesaria para adaptarse a estos incrementos futuros sin necesidad de realizar actualizaciones inmediatas.

Análisis de dimensionamiento de ancho de banda en cada Sede Remota:

- **Uso Específico de las Sedes Remotas:** Las sedes remotas manejan tareas administrativas, acceso a bases de datos centralizadas y comunicaciones con la sede principal. Estas funciones son esenciales; sin embargo, no demandan el mismo nivel de ancho de banda que la sede principal.
- **Número de Usuarios concurrentes:** Cada sede remota cuenta con un número reducido de empleados y dispositivos conectados en comparación con la sede principal. Un enlace de 200 Mbps es suficiente para manejar el tráfico generado por estos usuarios sin comprometer la eficiencia operativa.
- **Escalabilidad:** Aunque se espera un crecimiento en las sedes remotas, este será proporcional al desarrollo de la entidad. Un enlace de 200 Mbps permite realizar incrementos graduales en la capacidad de ancho

de banda conforme se identifiquen nuevas necesidades, evitando inversiones innecesarias en el corto plazo.

- **Acuerdos de Nivel de Servicio:** Los Acuerdos de Nivel de Servicio establecen los niveles mínimos de disponibilidad que el ISP debe cumplir, como el porcentaje de tiempo de funcionamiento garantizado.

Para este proyecto, donde las comunicaciones en la Entidad son esenciales para operaciones críticas y respuesta ante emergencias, es vital mantener la continuidad operativa y asegurar que la conexión a internet esté siempre disponible. En este contexto, resulta fundamental definir claramente los parámetros de disponibilidad e indisponibilidad, los cuales determinan la calidad y confiabilidad del servicio.

- ✓ **Disponibilidad:** Representa el porcentaje del total de horas de un mes calendario en la cual el servicio se mantiene completamente operativo sin interrupciones. Tanto la Sede Principal como las Sedes Remotas cuentan con una disponibilidad mensual del 99,50 % en sus enlaces de servicio, lo que garantiza continuidad en la operación institucional.
- ✓ **Indisponibilidad:** Los tiempos de indisponibilidad al mes por cada enlace se calculan en base a un periodo de 30 días. La suma total de minutos de interrupción del servicio no debe superar los valores permitidos. Con una disponibilidad del 99,50 %, el servicio puede presentar un máximo de 3 horas con 36 minutos de interrupción al mes.
- **Latencias:** Es el tiempo que tarda un paquete de datos en viajar desde su origen hasta su destino a través de una red. Para el presente proyecto, en el cual se requiere una conexión segura y rápida para acceder al servidor de alertas de emergencia, una baja latencia es crucial para garantizar una respuesta inmediata y efectiva ante situaciones críticas. Para cada enlace, la latencia máxima es de 10 ms.

3.5.1.3 Estudio de factibilidad para la última milla.

Se realizó un análisis preliminar de factibilidad para validar la fibra óptica desde el Punto de Presencia (POP) más cercano hacia cada sede, asegurando que el diseño propuesto sea factible y eficiente. La evaluación de la última milla resulta fundamental, ya que constituye el tramo crítico en la entrega del servicio.

A continuación, en la tabla 2, se indican las direcciones de las sedes en las cuales se deberá validar la última milla, con el fin de garantizar que la conectividad cumpla con los niveles de servicio y confiabilidad requeridos.

Tabla 2: Sedes de la Entidad.

Sede	Dirección	Latitud	Longitud
Sede Principal	Av. Salaverry N° 2495, San Isidro, Lima, Lima	-12.09134	-77.05215
Sede Remota 1	Jr. Los Heros N° 151, Callao, Callao, Lima	-12.06047	-77.13104
Sede Remota 2	Av. Los Defensores de Lima N° 1500, VMT, Lima, Lima	-12.17251	-76.94511
Sede Remota 3	Jr. Manuel Candamo N° 455, Lince, Lima, Lima	-12.08132	-77.03206
Sede Remota 4	Calle Claudio Galeno N° 200, San Borja, Lima, Lima	-12.10708	-77.00724

Fuente. Elaboración propia a partir de información obtenida de WIN Empresas (2024).

Se validó que se cuenta con un despliegue de fibra óptica dedicada en cada sede, por lo que se aprovechará la infraestructura actual para la instalación y configuración del servicio de internet dedicado.

La decisión de aprovechar el despliegue existente de fibra óptica se justifica en función de la optimización de recursos económicos y temporales, la sostenibilidad ambiental y la fiabilidad comprobada de la infraestructura,

puesto que se permite maximizar el rendimiento del servicio de Internet sin incurrir en gastos y demoras adicionales propios de una nueva instalación, manteniendo un alto nivel de calidad y eficiencia en el servicio final. Esta justificación se alinea con tendencias actuales en las telecomunicaciones, donde se prioriza el aprovechamiento de infraestructura ya existente para lograr despliegues más ágiles, sostenibles y económicamente viables.

Se empleó la herramienta de Google Earth para validar la ruta de despliegue de fibra óptica. A continuación, en la tabla 3, se presenta la información de metraje actual y tipo de ingreso en cada sede. Este procedimiento refuerza la confiabilidad de los resultados obtenidos en el estudio de factibilidad.

Tabla 3: Metraje de Fibra óptica de las sedes de la Entidad.

Sede	POP	Distancia desde POP	Observación
Principal	Pershing	300 m	Cantidad de Postes: 0 Metrado Canalizado: 0 Cámaras: 0 Tipo de Ingreso: Aéreo
Sede Remota 1	Santa Fe	447 m	Cantidad de Postes: 0 Metrado Canalizado: 0 Cámaras: 0 Tipo de Ingreso: Aéreo
Sede Remota 2	Villa el Salvador	300 m	Cantidad de Postes: 3 Metrado Canalizado: 0 Cámaras: 0 Tipo de Ingreso: Aéreo
Sede Remota 3	Lince	300 m	Cantidad de Postes: 0 Metrado Canalizado: 157.68 Cámaras: 1 Tipo de Ingreso: Canalizado
Sede Remota 4	República de Panamá	1850 m	Cantidad de Postes: 0 Metrado Canalizado: 0 Cámaras: 3 Tipo de Ingreso: Canalizado

Fuente. Elaboración propia a partir de información obtenida de WIN Empresas (2024).

La ubicación física de las sedes, obtenida mediante la herramienta Google Earth, se presenta en el Anexo A en forma de coordenadas geográficas. Este registro es fundamental para identificar con precisión la localización de cada punto de acceso y garantizar la exactitud en la planificación de la red. La información de coordenadas permite además calcular distancias, validar la factibilidad de los enlaces de fibra óptica y asegurar la correcta integración de las sedes dentro de la topología propuesta.

3.5.1.4 Dimensionamiento de equipos CPE.

El dimensionamiento de equipos CPE es una etapa clave para garantizar el correcto funcionamiento y rendimiento de la red propuesta. En esta sección se detallan las características y funcionalidades de los dispositivos seleccionados, así como de la herramienta de monitoreo que será implementada en las cinco sedes del proyecto.

Se contará con dos tipos de CPE, asignados según el rol y las necesidades de cada sede. En la sede principal, donde el ancho de banda es de 1Gbps, se instalará un Cisco modelo C3560G-24TS-S, el cual es un equipo de alto rendimiento y capacidades de conmutación avanzadas, ideal para gestionar múltiples conexiones provenientes de las sedes remotas.

Por otro lado, las sedes remotas, cuyo ancho de banda es de 200 Mbps, estarán equipadas con el CPE Cisco modelo 1121-4P, un dispositivo diseñado para conexiones seguras y confiables. Cuenta con soporte para VPN, y capacidad para manejar tráfico de hasta 640 Mbps, lo que garantiza un rendimiento adecuado a las necesidades de cada ubicación.

Las características y funcionalidades de ambos modelos se encuentran en la Tabla 4. La elección de estos modelos responde a la robustez y confiabilidad que ofrece la marca en entornos corporativos. Además, el uso de un mismo fabricante facilita la aplicación homogénea de configuraciones y la reducción de incidentes por incompatibilidad. Finalmente, esta estandarización permitirá que, en caso de futuras ampliaciones de capacidad o incorporación de nuevas

sedes, los equipos puedan ser escalados sin necesidad de reemplazos inmediatos, asegurando así la sostenibilidad tecnológica de la red.

Tabla 4: Características y funcionalidades de equipos CPE propuestos.

Modelo de Router Cisco	C3560G-24TS-S	1121-4P
Hardware		
Interfaces auto-negociables (Speed & Duplex)	10 /100 / 1000	10 /100 / 1000
Throughput (Multiservicios)	32 Gbps	640 Mbps duplex
Test de llamadas concurrentes	No aplica	250
Puertos de cobre	24 puertos	4 puertos
Puertos ópticos	4 puertos SFP	1 puerto combo
Puerto consola	1 puerto consola RJ-45	1 puerto tipo Micro-USB
Funcionalidades		
Servicios	DHCP Server/cliente y Relay, SNMP, Telnet/SSH, Netflow, Syslog	
Networking	Enrutamiento estático, dinámico IPv4, dinámico IPv6, route map, prefix lists, enrutamiento multicast, PIM, Policy Routing, VRF, router de capa 2 (Lan Extendida)	
Autenticación	Radius, TACACs	
QoS y Trunking	802.1q, Track, IPSLA, Rate-Limit, QoS, Policy Traffic	

Fuente. Elaboración propia a partir de la homologación y pruebas realizadas en WIN Empresas con los equipos Cisco C3560G-24TS-S y 1121-4P.

Para supervisar el rendimiento de la red y mantener un control continuo de su funcionamiento, se empleará una herramienta de monitoreo especializada. Esta herramienta permitirá rastrear parámetros críticos como el ancho de banda, las velocidades de transmisión y recepción, el jitter y la latencia, generando alertas automáticas en caso de anomalías y reportes históricos para análisis de desempeño. Con esta solución, se asegura la estabilidad de la red y una respuesta inmediata ante posibles problemas.

3.5.1.5 Dimensionamiento de firewall virtual Palo Alto VM-700.

El dimensionamiento del firewall virtual es un componente esencial del diseño de la red para garantizar la seguridad y el control del tráfico entre las sedes. Será desplegado en la nube y estará encargado de gestionar políticas de seguridad avanzadas, proteger contra amenazas cibernéticas y garantizar la integridad de las comunicaciones.

La VM-700 de Palo Alto fue seleccionada como la solución de seguridad centralizada para proteger las 4 sedes remotas de la entidad gubernamental debido a múltiples ventajas que cumplen con los objetivos técnicos y económicos del proyecto. A continuación, se detallan las razones principales de esta elección:

- Ofrece una seguridad robusta y avanzada que asegura que todas las sedes remotas estén protegidas de manera consistente y eficaz contra amenazas cibernéticas, manteniendo la integridad y confidencialidad de los datos sensibles manejados por la entidad gubernamental.
- Costo-efectividad en comparación con el despliegue tradicional de firewalls en cada sede. Implementar firewalls independientes requiere una inversión significativa en hardware, licencias, mantenimiento y personal técnico en cada ubicación, lo que incrementa los costos operativos y la complejidad administrativa. En contraste, la VM-700 centraliza la gestión de la seguridad mediante una única consola de administración, reduciendo los costos de adquisición y mantenimiento de múltiples dispositivos físicos. Además, simplifica las operaciones de TI al eliminar la necesidad de personal especializado en cada sede, facilita la implementación de políticas de seguridad uniformes, permite el monitoreo en tiempo real y asegura una rápida respuesta ante incidentes desde un único punto de control.
- La VM-700 se encuentra alojada en datacenter redundante, lo que asegura que el servicio de seguridad no se vea afectado en caso de

cortes de electricidad u otros incidentes en las sedes remotas. Estos datacenters cuentan con sistemas de alimentación ininterrumpida (UPS), generadores de respaldo y múltiples fuentes de energía, garantizando una alta disponibilidad y continuidad del servicio. Esto elimina el riesgo de interrupciones en la seguridad de la red debido a fallas locales, proporcionando una capa adicional de fiabilidad y tranquilidad para la Entidad.

- Debido a que se está proyectando la integración de 50 sedes remotas adicionales de la Entidad, las cuales también contarán con servicio de internet dedicado de 200 Mbps, se dimensionó el modelo VM-700, el cual ofrece soporte para hasta 10 Gbps de throughput, lo que lo hace adecuado para entornos con alto volumen de tráfico. Es una solución escalable y flexible, capaz de adaptarse al crecimiento sin requerir inversiones adicionales significativas.

Para desplegar este firewall, se requiere una máquina virtual con capacidades específicas que cumplan con los requisitos mínimos y recomendados para su correcto funcionamiento. Los recursos necesarios incluyen: Un procesador con al menos 16 núcleos, una memoria RAM de 56 GB y un almacenamiento de 60 GB. Además, la máquina virtual debe estar alojada en una infraestructura que permita conexiones de red de alto rendimiento, garantizando un funcionamiento óptimo.

Estos lineamientos responden a las buenas prácticas de dimensionamiento de firewalls virtuales definidas por el fabricante, lo que asegura que el desempeño del sistema se mantenga estable y confiable incluso en escenarios de alta concurrencia y demanda de procesamiento. Asimismo, contar con una plataforma virtualizada robusta permite escalar recursos de manera flexible frente a futuros incrementos de tráfico, optimizando así la continuidad operativa de la solución. De igual forma, la ubicación del firewall en un datacenter de alto nivel asegura redundancia eléctrica y de conectividad, lo que reduce significativamente los riesgos de interrupción del servicio.

En términos de funcionalidad y throughput, la VM-700 tiene las siguientes capacidades (Ver Tabla 5):

Tabla 5. Funcionalidades de la VM-700 de PAN.

VM-700 de Palo Alto	
Ancho de Banda	Hasta 10Gbps
Número de usuarios concurrentes	100.000
Funcionalidades de Seguridad	Next Generation Firewall Advanced URL Filtering Threat Prevention Panorama management
Capacidades requeridas para la máquina virtual	
vCPU	16
RAM	56 GB
Almacenamiento	60 GB
Performance	
Throughput APP-ID Firewall	24 Gbps
Throughput Threat Prevention	12 Gbps
Throughput IPSec VPN	5 Gbps
Conexiones por segundo	120.000
Sesiones concurrentes	10.000.000
Zonas de seguridad	200
Reglas de seguridad	20.000
Reglas de NAT	15.000
Perfiles de seguridad	750
Address Objects	40.000
Rutas IPv4 / IPv6	100,000 / 100,000
Políticas QoS	4.000
VPN Site-to-Site	2.000
VPN Site-to-Client	12.000

Fuente. Elaboración propia a partir de Palo Alto Networks (2021), VM-Series Deployment Guide, sección “Components of the VM-Series Firewall on NSX-T (North-South)”.

En conclusión, el dimensionamiento del Palo Alto VM-700 garantiza que la solución de seguridad sea escalable y adecuada para el entorno propuesto, proporcionando protección avanzada y soporte para el tráfico esperado en la red diseñada. Asimismo, asegura la disponibilidad de recursos suficientes para implementar servicios de inspección profunda de paquetes, filtrado de

aplicaciones y gestión de accesos seguros, lo que fortalece la postura de ciberseguridad de la organización.

3.5.2 Implementación del servicio

La etapa de implementación del proyecto se enfoca en llevar a cabo las actividades necesarias para instalar, configurar y poner en operación la infraestructura diseñada en etapas previas. Esta fase incluye el despliegue físico de los enlaces de fibra óptica, la configuración de los equipos de red, la instalación y ajuste del firewall virtual Palo Alto VM-700, y la validación del funcionamiento de la red.

3.5.2.1 Cronograma de Implementación

El proyecto se lleva a cabo siguiendo un cronograma estructurado que asegura el cumplimiento de los plazos establecidos. Este cronograma contempla actividades como la validación de fibra óptica, la instalación y configuración de equipos, la implementación del firewall virtual y la ejecución de pruebas.

Con el fin de facilitar el seguimiento de las tareas y la asignación de recursos, se presenta un cronograma detallado, el cual permite visualizar de manera clara las fechas de inicio y fin de cada actividad, así como los responsables de su ejecución. Dicho cronograma se muestra en el Anexo B.

3.5.2.2 Validación de factibilidad para última milla

Este proceso incluye la inspección física de los enlaces de fibra óptica, para ello se coordinaron visitas técnicas a todas las sedes, revisando visualmente y mediante herramientas especializadas el estado físico de la fibra para asegurar que no haya daños o desgastes que puedan afectar el rendimiento.

Se realizó una evaluación de la pérdida de señal a lo largo de la fibra para asegurar que cumple con los requisitos de rendimiento.

Como parte del proceso, se revisó la información sobre topologías, rutas y características técnicas de la fibra, verificándose que el uso de la infraestructura existente cumple con las normativas locales y sectoriales.

Luego de dichas actividades, se concluyó que la infraestructura existente cumple con los niveles de disponibilidad requeridos para el servicio de Internet Dedicado. Además de las pruebas físicas, se requirió confirmar que la capacidad actual de la fibra soporta las velocidades requeridas.

A continuación, en la tabla 6 se indica el provisionamiento de recursos final para las conexiones de la fibra óptica en los Puntos de Presencia, los cuales soportan las capacidades de 1 Gbps en la sede principal y 200 Mbps en las cuatro (04) sedes remotas.

Tabla 6: Provisionamiento de recursos.

Sede	POP	Switch Proveedor	Puerto	VLAN Gestión	VLAN Servicio
Principal	Pershing	Huawei-11- 10.28.10.178	G0/0/6	1507	3833
Remota 1	Santa Fe	ACC-2- 10.32.237.108	G0/0/16	1525	3831
Remota 2	Los Cipreses	ACCESO-2- 10.32.247.115	G0/0/31	1528	3831
Remota 3	Lince	ACCESO-2- 10.32.247.115	G0/0/6	1528	3831
Remota 4	Rep. Panamá	Huawei 4 - 10.28.8.165	G0/0/3	1525	3825

Fuente. Elaboración propia basada en la provisión de recursos lógicos documentados en la red de WIN Empresas (2024).

3.5.2.3 Instalación y configuración de equipos CPE

Se procedió a la instalación y configuración de los equipos de red en cada sede. Los CPE Cisco seleccionados se configuran según su rol:

- En la sede principal, el Cisco C3560G-24TS-S se ajusta para gestionar las conexiones entrantes de las sedes remotas, con rutas y para priorizar el tráfico crítico (Ver Figura 7).

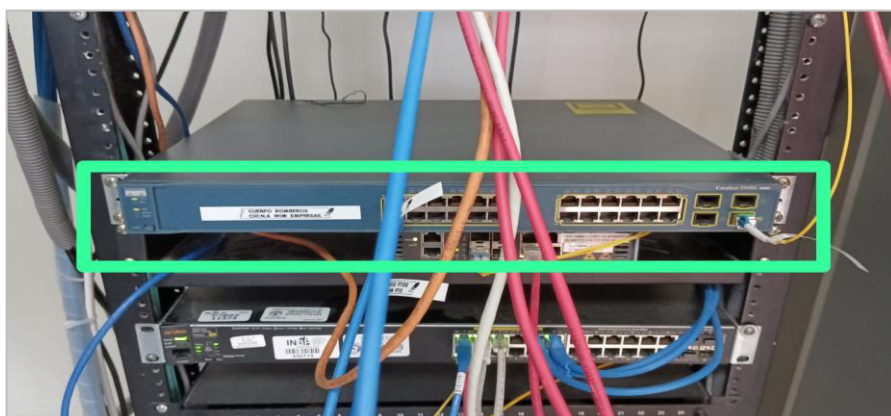


Figura 7: Instalación de CPE Cisco C3560G-24TS-S en la Sede Principal. Fuente. Registro fotográfico de WIN Empresas (2024).

- En las sedes remotas, los Cisco C1121-4P se configuran para soportar un ancho de banda de 200 Mbps. Las imágenes de la instalación de los CPE se encuentran en el anexo C (Ver Figuras del 18 al 21).

Por motivos de confidencialidad, no se revelarán las configuraciones específicas de los equipos utilizados. No obstante, se expondrá la activación de cada uno de ellos en el anexo D (Ver Figuras del 22 al 25), con la finalidad de validar su operatividad dentro del presente trabajo de investigación.

La configuración incluye ajustes de interfaces, asignación de direcciones IP y enrutamiento.

3.5.2.4 Configuración del Firewall Virtual

El firewall Palo Alto VM-700 se despliega en una máquina virtual ubicada en el Data Center de WIN Empresas, siguiendo los requisitos técnicos establecidos en el dimensionamiento. Este proceso asegura que el dispositivo cuente con los recursos necesarios de procesamiento, memoria y almacenamiento para garantizar un funcionamiento óptimo.

El firewall VM-Series se distribuye en formato Open Virtualization Alliance (OVA), que es un método estándar de empaquetado e implementación de máquinas virtuales. La VM-700 se instalará sobre una máquina virtual capaz de ejecutar VMware vSphere Hypervisor (ESXi). Antes de implementar el archivo OVA, se configuran los conmutadores estándar virtuales necesarios para el firewall de la serie VM. En la figura 8, se muestra el tenant de virtualización en vCenter mediante el cliente vSphere.

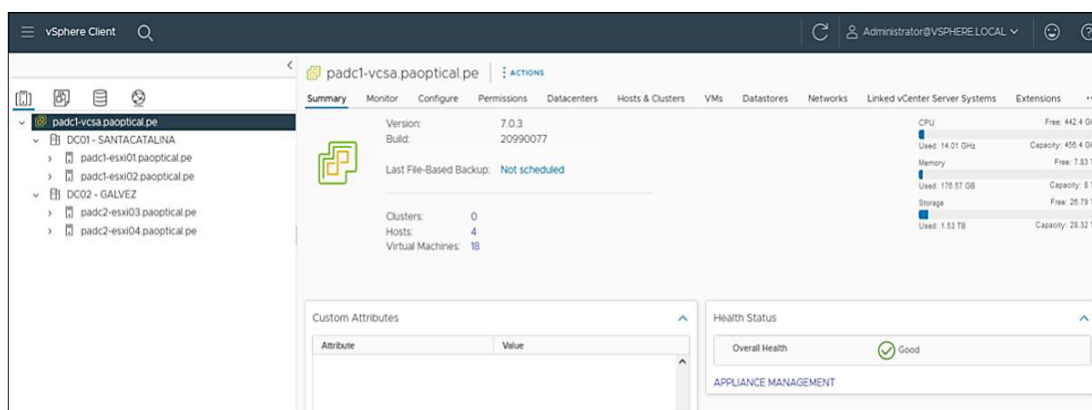


Figura 8: Tenant de Virtualización vSphere de VM-Series. Fuente: Captura de pantalla del Tenant de Virtualización vSphere de VM-Series. WIN Empresas (2024).

Una vez implementada la máquina virtual, se habilita el acceso administrativo al dispositivo a través de su portal web seguro. La Figura 9 muestra el acceso al portar de la VM-700 con la IP de gestión mediante protocolo https. Este mecanismo garantiza la administración segura del dispositivo, evitando

accesos no autorizados y permitiendo configurar de manera centralizada las políticas de seguridad que regirán el tráfico de la red.

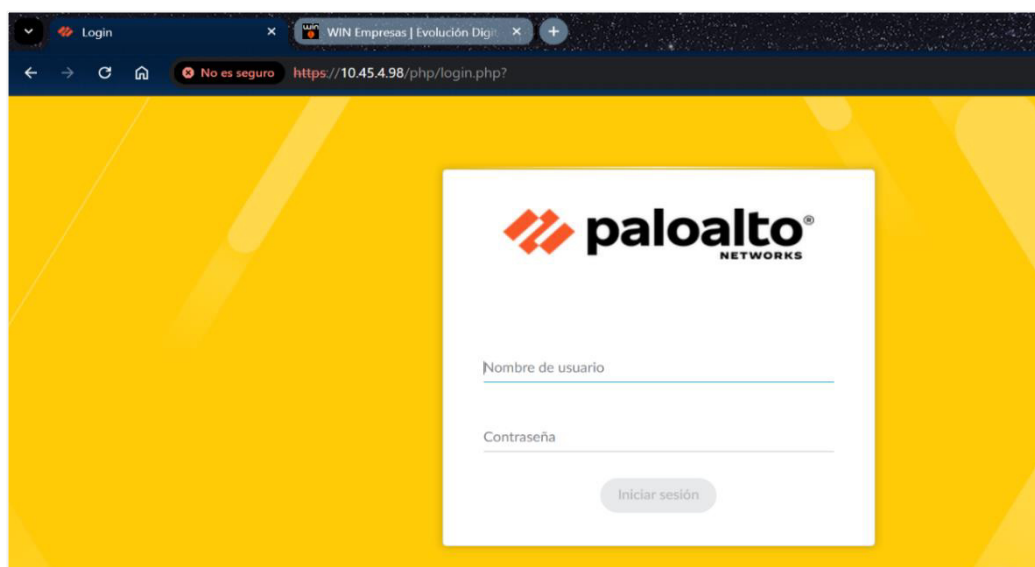


Figura 9: Portal del acceso a Palo Alto VM-700. Fuente. Captura de pantalla proporcionada por WIN Empresas.

Una vez desplegado, se configuran políticas avanzadas de seguridad para proteger el tráfico entre las sedes. Estas políticas incluyen reglas de acceso, detección y prevención de amenazas para mejorar la seguridad y garantizar la continuidad de los servicios críticos.

Dentro de las funcionalidades habilitadas se encuentran las suscripciones de Threat Prevention, que permiten detectar, bloquear y mitigar amenazas conocidas y desconocidas en la red; Advanced URL Filtering, orientada a proteger a los usuarios frente a accesos a sitios web maliciosos o sospechosos; y Panorama for Management, que facilita la administración centralizada de todas las políticas de seguridad.

El uso de estas suscripciones asegura que el firewall no solo actúe como un mecanismo de filtrado básico, sino como una plataforma inteligente capaz de actualizarse constantemente frente a nuevas amenazas. Esto incrementa la

resiliencia de la infraestructura y fortalece la postura de ciberseguridad de la Entidad.

La Figura 10 presenta la evidencia de las suscripciones habilitadas en el VM-700, mostrando cómo se asignan los créditos disponibles y se personalizan las funcionalidades activas según los requerimientos de seguridad definidos para el proyecto.

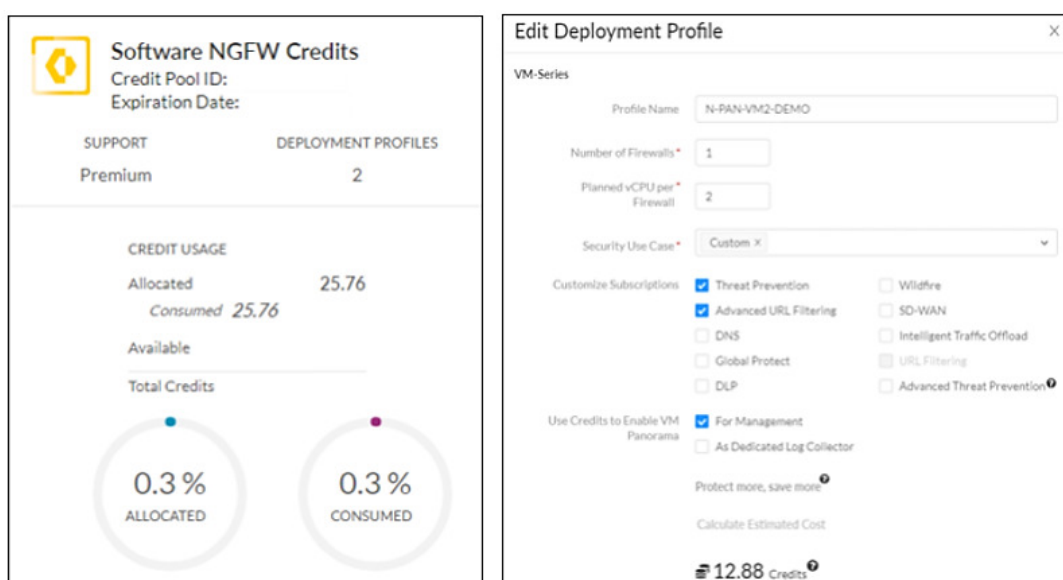


Figura 10: Suscripciones habilitadas en Palo Alto VM-700. Fuente. Captura de pantalla proporcionada por WIN Empresas.

3.5.2.5 Provisionamiento de recursos lógicos

El provisionamiento lógico de recursos constituye un paso esencial en la implementación, ya que define los parámetros que permiten la correcta interacción entre la infraestructura física y la lógica de la red. La asignación de direcciones IP públicas y privadas, así como la configuración de VLANs y puertos, son aspectos que garantizan no solo la conectividad entre la Sede Principal y las sedes remotas, sino también la segmentación adecuada del tráfico para mantener un entorno seguro.

Adicionalmente, estos recursos lógicos facilitan la administración remota de los equipos y aseguran la continuidad de los servicios institucionales, al establecer rutas claras para el enrutamiento y la gestión de la red. La correcta provisión de circuitos, subredes y políticas de seguridad evita conflictos de direccionamiento y reduce el riesgo de interrupciones en la comunicación.

La tabla 7 muestra la provisión de circuito y direcciones IP para la Sede Principal, las cuales serán utilizadas como base para la configuración del servicio de Internet Dedicado. Esta información resulta fundamental para garantizar la continuidad operativa y la correcta integración con el firewall de próxima generación.

Tabla 7: Provisionamiento lógico para Sede Principal.

SEDE PRINCIPAL	
Código de circuito	296051
Pool de IPs Públicas	167.249.11.176/28
Rango de IPs utilizables	167.249.11.178 – 167.249.11.190
IP Router	10.100.4.2
IP Gestión	10.40.171.58
ID de VSI (Intefaz virtual):	294030188
Nombre de VSI (Intefaz virtual):	ISE272086-ELAN

Fuente. Elaboración propia a partir de información de provisionamiento lógico de la red de WIN Empresas para la Sede Principal (2024).

La tabla 8 muestra la provisión de circuito y direcciones IP para la VM-700 que se encuentra en el tenant de Win Empresas. Estos parámetros permiten establecer la conectividad inicial, asegurar la administración remota del equipo y garantizar la correcta segmentación de los recursos.

Tabla 8: Provisionamiento lógico para VM-700.

FIREWALL VM-700	
Código de circuito	296055
Hostname	VM700-ISE272086
IP de Gestión	https://10.45.4.98
IP WAN	10.49.10.196/29
IP LAN	10.42.74.193/26 (62 host disponibles para cada WAN-CPE en sede cliente)
Pool de IP	190.102.144.60/30

Fuente. Elaboración propia a partir de información de provisionamiento lógico de la red de WIN Empresas para el Firewall VM-700 (2024).

Las tablas 9, 10, 11 y 12 muestran la provisión de circuito y direcciones IP para las Sedes Remotas, incluyendo parámetros de gestión y operación. Estos datos son esenciales para asegurar la conectividad con la sede principal y permitir la correcta integración dentro de la red corporativa.

Tabla 9: Provisionamiento lógico para Sede Remota 1.

SEDE REMOTA 1	
Número de Circuito	296052
IP Pública	190.102.144.60/30
IP WAN CPE	10.42.74.197/26
IP LAN CPE	192.168.2.1
IP Gestión	10.40.81.178/30
IP Loopback:	10.34.17.6/32
VSI (Intefaz virtual) ID:	294030188
VSI (Intefaz virtual) NAME:	ISE272086-ELAN

Fuente. Elaboración propia a partir de información de provisionamiento lógico de la red de WIN Empresas para Sede Remota 1 (2024).

Tabla 10: Provisionamiento lógico para Sede Remota 2.

SEDE REMOTA 2	
Código de circuito	296056
IP Pública	190.102.144.61/30
IP WAN CPE	10.42.74.196/26
IP LAN CPE	192.168.3.1
IP Gestión	10.40.73.158/30
IP Loopback:	10.34.27.200/32
VSI (Intefaz virtual) ID:	294030188
VSI (Intefaz virtual) NAME:	ISE272086-ELAN

Fuente. Elaboración propia a partir de información de provisionamiento lógico de la red de WIN Empresas para Sede Remota 2 (2024).

Tabla 11: Provisionamiento lógico para Sede Remota 3.

SEDE REMOTA 3	
Código de circuito	296059
IP Pública	190.102.144.62/30
IP WAN CPE	10.42.74.195/26
IP LAN CPE	192.168.4.1
IP Gestión	10.40.89.42/30
IP Loopback:	10.34.23.232/32
VSI (Intefaz virtual) ID:	294030188
VSI (Intefaz virtual) NAME:	ISE272086-ELAN

Fuente. Elaboración propia a partir de información de provisionamiento lógico de la red de WIN Empresas para Sede Remota 3 (2024).

Tabla 12: Provisionamiento lógico para Sede Remota 4.

SEDE REMOTA 4	
Código de circuito	296050
IP Pública	190.102.144.63/30
IP WAN CPE	10.42.74.194/26
IP LAN CPE	192.168.1.1
IP Gestión	10.40.108.166/30
IP Loopback:	10.34.25.149/32
VSI (Intefaz virtual) ID:	294030188
VSI (Intefaz virtual) NAME:	ISE272086-ELAN

Fuente. Elaboración propia a partir de información de provisionamiento lógico de la red de WIN Empresas para Sede Remota 4 (2024).

3.5.2.6 Validación del Sistema

Con el objetivo de garantizar que la red implementada cumple con los requisitos funcionales y técnicos establecidos en el diseño, se llevaron a cabo pruebas de validación en campo, las cuales se encuentran en el anexo E.

Estas pruebas permitieron verificar la estabilidad de los enlaces, el rendimiento del servicio de Internet Dedicado y la correcta aplicación de las políticas de seguridad implementadas en el firewall virtual Palo Alto VM-700, cuyas validaciones se estructuraron de la siguiente manera:

- Pruebas de conectividad y latencia: Se ejecutaron pruebas de ping entre la sede principal y las sedes remotas (Ver Figuras del 27 al 31), con el fin de comprobar la estabilidad de los enlaces y validar que la latencia no superara los 10 milisegundos, límite máximo definido para enlaces sobre fibra óptica según los criterios de diseño.
- Pruebas de ancho de banda: Mediante la herramienta Speed Test, se midieron las velocidades de carga y descarga en todas las sedes, verificando que el proveedor garantice al menos el 90% del ancho de banda contratado (1 Gbps para la sede principal y 200 Mbps para sedes remotas), en condiciones de carga normales (Ver Figuras del 32 al 36).

- Validación de configuración de políticas de seguridad: Se revisó la configuración del firewall Palo Alto VM-700 en la nube, comprobando la asignación de interfaces y zonas de seguridad, rutas estáticas, reglas de acceso (permitir/denegar), perfiles de filtrado web y provisionamiento de direcciones IP públicas y privadas (Ver Figuras del 37 a 42).

Estas validaciones fueron fundamentales para asegurar que la red estuviera preparada para operar en un entorno real, bajo parámetros de calidad, seguridad y disponibilidad.

3.6 Resultado de la actividad

Con el objetivo de garantizar el correcto funcionamiento de la red implementada, se realizaron pruebas técnicas de conectividad, rendimiento y seguridad, orientadas a validar el cumplimiento de los parámetros definidos en la fase de diseño. Estas pruebas incluyeron:

- Latencia y estabilidad de los enlaces: Las pruebas realizadas mostraron una latencia promedio de 4 ms y una pérdida de paquetes del 0% entre la sede principal y las sedes remotas, cumpliendo satisfactoriamente el límite establecido de 10 ms. Esto demuestra una conectividad estable y de baja latencia, ideal para servicios de misión crítica. (Ver Tablas del 16 a 20 del Anexo E).
- Ancho de banda garantizado: Los enlaces presentaron velocidades simétricas en la carga y descarga, superando el 90% del ancho de banda contratado. En la sede principal, se alcanzaron 918 Mbps de descarga y 933 Mbps de subida. En las sedes remotas, se reportaron promedios de hasta 197 Mbps de bajada y 201 Mbps de subida. Estos resultados evidencian que la red puede soportar el tráfico esperado con

un margen suficiente para garantizar continuidad operativa y escalabilidad futura. (Ver Figuras del 32 al 36 del Anexo E).

- Configuración del firewall: Se comprobó la correcta aplicación de políticas de seguridad en el firewall VM-700. Las Figuras del 37 a 42 del Anexo E evidencian la creación de reglas que abarcan la configuración adecuada de interfaces y zonas (WAN, LAN y públicas), la definición de rutas estáticas hacia cada sede, la implementación de reglas de acceso para permitir únicamente servicios legítimos como HTTP, HTTPS y DNS, bloqueo de tráfico hacia direcciones IPs maliciosas o de alto riesgo y de perfiles de filtrado web que contemplan categorías críticas como malware, phishing, command and control y adult content, entre otras.

Estos resultados confirman que la infraestructura de red desplegada no solo cumple con los estándares de calidad y seguridad establecidos, sino que también está preparada para una operación continua y confiable en el entorno operativo de la Entidad.

CAPITULO IV

DISCUSION DE RESULTADOS

4.1 Descripción de la implementación

La implementación del proyecto se llevó a cabo en tres fases principales: La validación del despliegue existente de fibra óptica, la configuración de equipos de red y la integración del firewall virtual Palo Alto VM-700. Cada una de estas fases se ejecutó de acuerdo con el diseño establecido.

En la primera fase, se validaron un total de 3.197 metros de fibra óptica desde el Punto de Presencia (POP) hasta las cinco sedes. El proceso incluyó la identificación de rutas óptimas previamente analizadas en estudio de factibilidad. Se logró culminar la validación de operatividad de los enlaces dentro del tiempo planificado, determinándose que la fibra óptica garantiza la continuidad del servicio.

En la segunda fase, los equipos de red fueron configurados e instalados. En la sede principal, el router Cisco C3560G-24TS-S se ajustó para gestionar múltiples conexiones entrantes y salientes, con un ancho de banda de 1 Gbps y políticas de calidad de servicio (QoS) para priorizar el tráfico crítico. En las sedes remotas, los routers Cisco C1121-4P se configuraron para establecer una conexión confiable hacia la sede principal, con un ancho de banda de 200 Mbps en cada sede.

De las mediciones de ancho de banda en cada sede, se resalta que las pérdidas pueden darse por sobrecarga de protocolos y otros factores, los cuales son comunes y aceptables en entornos de red reales.

La tercera fase incluyó el despliegue y configuración del firewall virtual Palo Alto VM-700 en la nube. Se configuraron políticas avanzadas de seguridad

para controlar el tráfico entrante y saliente. El firewall brinda una herramienta de monitoreo en tiempo real, permitiendo supervisar métricas como el ancho de banda y detectar intentos de acceso no autorizado a la red.

Las pruebas de validación demostraron que los enlaces entre las sedes son estables, comprobándose los siguientes indicadores:

- De Sede Principal a Sedes Remotas: La latencia promedio de 4 ms y una pérdida de paquetes de 0%.
- De Sedes Remotas hacia Sede Principal: La latencia promedio es de 4 ms y una pérdida de paquetes de 0%

Con ello, se cumplen los parámetros de calidad definidos en el diseño (latencia máx de 10 ms). Además, las políticas de seguridad implementadas bloquearán exitosamente los intentos de acceso no autorizado y ataques de malware.

En conclusión, la implementación se completó satisfactoriamente, cumpliendo con los objetivos establecidos y proporcionando una infraestructura robusta, segura y escalable. La red implementada no solo satisface las necesidades actuales, sino que también está preparada para soportar expansiones futuras.

4.2 Evaluación Económica

A continuación, se presenta la evaluación económica, la cual se centra en analizar la viabilidad financiera y la rentabilidad de la inversión asumida por la empresa, considerando tanto los gastos de capital (Capex) como los gastos operativos (Opex) y los beneficios tangibles obtenidos.

Para la inversión, se asume la totalidad de los costos de implementación y soporte, estableciendo un convenio con la entidad gubernamental por 5 años que no implica desembolso financiero directo por parte de la entidad.

4.2.1 Identificación de costos y plan de inversión

- Capital Expenditure (Capex): Los capex representan los costos iniciales necesarios para adquirir y establecer la infraestructura del proyecto. A continuación, en la Tabla 13, se detallan los principales componentes:

Tabla 13: Gastos de capital del proyecto.

Descripción	Cant.	Costo Unitario (\$)	Costo Total (\$)
Router Cisco C3560G-24TS-S	1	3,180.00	3,180.00
Router Cisco 1121-4P	4	190.00	760.00
Implementación de Firewall Virtual	1	20,928.04	20,928.04
Validación de fibra óptica	1	1,500.00	1,500.00
Traslado de equipos a cada sede	5	20.00	100.00
Instalación y Configuración de equipos	5	100.00	500.00
Total Capex (\$)			26,968.04

Fuente: Elaboración propia basada en la estimación de gastos de capital del proyecto, con información de costos proporcionada por WIN Empresas (2024).

- Operational Expenditure (OpEx): Los Opex son los costos recurrentes asociados al funcionamiento y mantenimiento de la infraestructura a lo largo de su vida útil (Ver Tabla 14).

Tabla 14: Gastos operativos del proyecto.

Descripción	Costo Anual (\$)	Costo Total 5 años (\$)
Transporte Internacional de Datos	4,320.00	21,600.00
Mantenimiento de Equipos	3,000.00	15,000.00
Mantenimiento de Firewall Virtual	1,500.00	7,500.00
Soporte Técnico y Mano de Obra Calificada	3,000.00	15,000.00
Total Opex	11,820.00	59,100.00

Fuente: Elaboración propia basada en la estimación de gastos operativos del proyecto, con información de costos proporcionada por WIN Empresas (2024).

4.2.2 Identificación y clasificación de beneficios

- **Beneficios Tangibles:** Son aquellos que se pueden cuantificar económicamente y se derivan directamente de la implementación del proyecto. A continuación, en la Figura 11, se presenta una gráfica que muestra la comparativa de costos de implementación entre el Firewall Virtual Centralizado y un Firewall físico por cada sede, tomando el dimensionamiento de 54 sede remotas totales. La finalidad de esta comparativa es justificar la decisión financiera de la elección del firewall virtual centralizado frente a una alternativa tradicional de firewall físico.

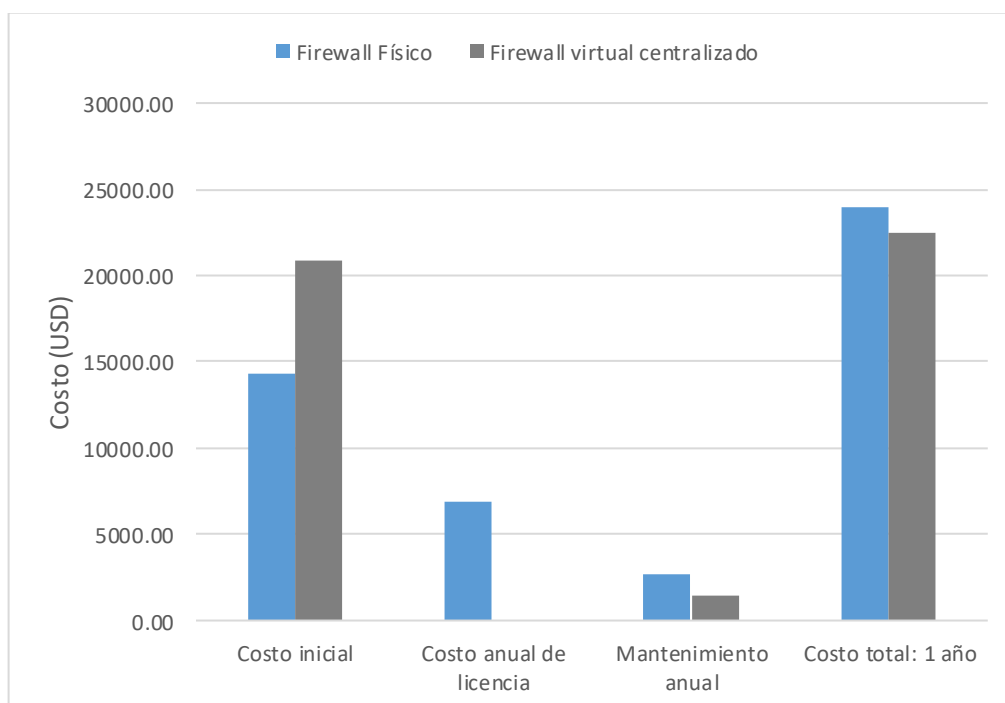


Figura 11: Comparativa de Costos: Firewall virtual vs Firewall físicos en cada sede por 1 año. Fuente. Elaboración propia basada en la estimación comparativa de costos de firewall físico y virtual, con información de WIN Empresas (2024).

En referencia al costo inicial, el firewall virtual centralizado tiene un costo inicial mayor que el firewall físico, esto se debe a la inversión de infraestructura en la nube y licencias.

Por otro lado, el firewall físico tiene un costo anual de licencias por cada equipo, a diferencia del firewall virtual que maneja las licencias en la inversión inicial.

Respecto al mantenimiento anual, el firewall físico requiere más gastos de mantenimiento que el firewall virtual, debido al hardware dedicado, soporte técnico y actualizaciones.

Se concluye que, a pesar del alto costo inicial del firewall virtual, su costo total es ligeramente menor que el del firewall físico, por lo que, a largo plazo, la solución virtual centralizada es más rentable. Ello se valida en la Figura 12, la cual muestra el ahorro acumulado por 5 años.

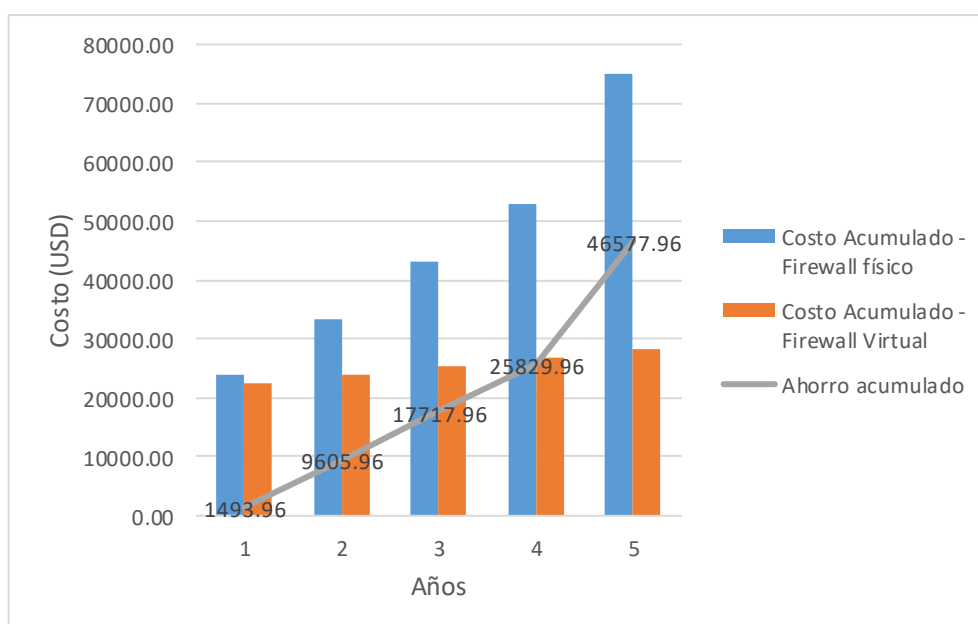


Figura 12: Análisis de Costos y Beneficios Acumulados en 5 Años: Firewall físico vs Firewall virtual Centralizado. Fuente. Elaboración propia basada en la proyección comparativa de costos de firewall físico y virtual, utilizando información de WIN Empresas (2024).

La gráfica confirma que la implementación del firewall virtual centralizado ofrece mayores ahorros en comparación con un firewall físico. A lo largo de 5 años, la diferencia en costos se vuelve

significativa, validando la decisión de optar por la solución virtual para garantizar una infraestructura de seguridad más eficiente y rentable.

- **Beneficios Intangibles:** Son resultados que no se pueden cuantificar monetariamente; sin embargo, aportan un valor significativo al proyecto. Dentro de estos beneficios se encuentra la mejora en la satisfacción del usuario al tener mayor eficiencia y estabilidad en las comunicaciones. También se encuentra el incremento en la seguridad de la información y la capacidad para adaptarse a futuras necesidades tecnológicas sin costos adicionales significativos.

CAPITULO V

CONCLUSIONES

- La migración de una arquitectura centralizada a un esquema de conectividad basado en internet dedicado y firewall virtual para cinco sedes de una entidad gubernamental ha demostrado ser una solución efectiva y viable. Esta implementación ha mejorado significativamente el ancho de banda y la seguridad de las comunicaciones, además de optimizar la operatividad de la entidad, alineándose con las demandas de entornos tecnológicos modernos y contribuyendo a una mayor eficiencia y resiliencia organizacional.
- La implementación de enlaces de internet dedicados en cada una de las cinco sedes de la entidad gubernamental ha garantizado una notable mejora en la conectividad y el rendimiento de la red. Se observó una latencia menor a 5ms y una optimización del uso del ancho de banda disponible, lo cual permite una transmisión de datos más rápida y estable. Estos avances han facilitado una comunicación más eficiente entre las sedes.
- La adopción de una solución de seguridad perimetral virtualizada ha fortalecido significativamente la protección de las sedes remotas contra amenazas externas e internas, alineándose con estándares internacionales como ISO/IEC 27001 para la gestión de la seguridad de la información y ISO/IEC 27032 para la ciberseguridad. La virtualización del firewall ha permitido una aplicación centralizada de las políticas de seguridad, garantizando el cumplimiento de buenas prácticas y reduciendo las vulnerabilidades. Esto contribuye a la integridad, confidencialidad y disponibilidad de la información. Además, esta implementación ha facilitado la supervisión y el control de accesos,

incrementando la capacidad de respuesta ante incidentes de seguridad conforme a los lineamientos de ISO/IEC 22301 para la continuidad del negocio, garantizando que la entidad pueda operar y recuperarse de interrupciones inesperadas, como ciberataques, fallos tecnológicos o incidentes de seguridad.

- La transición a una infraestructura de conectividad basada en internet dedicado y firewalls virtuales ha resultado en una evaluación económica que revela que, aunque los indicadores financieros tradicionales no soportan la viabilidad del proyecto, los beneficios intangibles y las mejoras operativas justifican la inversión asumida por la empresa. Además, los beneficios económicos indirectos, como la capacidad de respuesta ante emergencias, han contribuido a una mayor productividad y resiliencia organizacional, justificando la inversión realizada en la nueva infraestructura.

CAPITULO VI

RECOMENDACIONES

- Fortalecer las Medidas de Seguridad Interna: Se recomienda complementar la solución de firewall virtualizada con protección de endpoints haciendo el sistema más redundante. Esto garantizará una seguridad integral de la red, protegiendo tanto el perímetro como los dispositivos finales contra amenazas internas y avanzadas.
- Desarrollar normativas de Respaldo y Recuperación ante Desastres basadas en los estándares nacionales e internacionales: Es esencial establecer procedimientos detallados para la recuperación rápida de la infraestructura de red en caso de fallos críticos o desastres. Un plan de recuperación bien definido asegurará la continuidad operativa de la entidad gubernamental, minimizando el tiempo de inactividad y manteniendo la disponibilidad de servicios esenciales.
- Implementar Redundancia en Componentes Críticos: Se recomienda establecer sistemas redundantes para routers, switches y enlaces de internet dedicado, garantizando la continuidad operativa en caso de fallos de hardware o interrupciones en los enlaces principales. Esto se puede llevar a cabo mediante el despliegue de rutas de contingencia para los enlaces de fibra óptica y/o implementación tecnología de SD-WAN (Software Defined Wide Area Network).
- Fomentar la Capacitación Continua del Personal de TI: Para mantener la eficiencia y seguridad de la infraestructura a largo plazo, es fundamental implementar programas de formación continua y certificaciones para el personal de TI. Esto asegurará que el equipo esté actualizado con las últimas tecnologías, mejores prácticas y estrategias de mitigación de riesgos, contribuyendo a una gestión y

mantenimiento efectivos de la red. Además, considerando la rotación del personal y la incorporación de nuevos profesionales, es esencial establecer planes de capacitación inicial y transferencia de conocimientos para garantizar la continuidad operativa y evitar brechas en la gestión de la seguridad.

CAPITULO VII

BIBLIOGRAFÍA

Ardila, N. (27 de Agosto de 2019). Seguridad en las VPN'S. Colombia: Universidad Piloto de Colombia. Obtenido de <http://repository.unipiloto.edu.co/handle/20.500.12277/6435>

AscentOptics. (18 de Septiembre de 2023). *Comprender las diferencias: fibra multimodo OM1, OM2, OM3, OM4 y OM5*. Obtenido de <https://ascentoptics.com/blog/pt/understanding-the-differences-om1-vs-om2-vs-om3-vs-om4-vs-om5-multimode-fiber/>

Cabello, L. M. (2017). Geolocalización a través de direcciones IP. Obtenido de <https://dialnet.unirioja.es/servlet/articulo?codigo=6097027>

Camacho Contreras, A. F., & Lopez Rodriguez, J. S. (2017). Diseño de un Sistema de Seguridad Perimetral e Interna para la empresa American Business Process Services, en Bogotá D.C. Universidad Distrital Francisco Jose de Caldas. Facultad de Ingeniería.

De la Cruz, S. & Vera, J. (2020). Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo.

Diaz, L. (Julio de 2023). Análisis y Diseño de Seguridad Perimetral Basado en Software de Código Abierto para una Compañía en Crecimiento. Bogotá, Colombia.

Feknous, M., Guyader, B., Varga, P., Gravey, A., Gosselin, S., & Torrijos, J. (2015). Multi-Criteria Comparison Between Legacy and Next Generation Point of Presence Broadband Network Architectures.

- Flores, J. (Septiembre de 2023). *Internet Dedicado: Mitos y realidades*.
Obtenido de <https://winempresas.pe/blog/internet-dedicado-mitos-y-realidades>
- González, C. (2015). *Análisis de Vulnerabilidades DNS*. Universidad Politécnica de Madrid.
- Hubbard, B. (25 de Julio de 2022). *¿Qué es la seguridad perimetral informática?* Obtenido de <https://blog.invgate.com/es/seguridad-perimetral-informatica>
- Kurose, J., & Ross, K. (2017). *Computer Networking: A Top-Down approach*.
Lederkremer, M. (2019). *Redes Informáticas*. RedUsers.
- Manage Engine. (2024). *Topología de red: tipos e importancia*. Obtenido de <https://www.manageengine.com/latam/network-monitoring/tech-topics/topologia-de-red.html>
- Marín Valencia, J. J., Patiño Valencia, A., & Acevedo Bedoya, J. C. (2020). Implementación de un sistema de seguridad perimetral informático usando vpn, firewall e IDS. *Revista Universidad Católica de Oriente*. doi:<https://doi.org/10.47286/01211463.284>
- Morales, F., Toapanta, S., & Toasa, R. (2019). Implementación de un Sistema de Seguridad Perimetral como Estrategia de Seguridad de la Información. Ecuador.
- Muhammad, U., Nor, N., Ramli, A., & Ahmad, N. (Febrero de 2022). Effect of Ground Electrodes on the Susceptibility to Damage of Customer Premises Equipment (CPE) under Impulse Conditions. doi:<https://doi.org/10.3390/en15031247>
- Mújica, J. (2008). *Origen, desarrollo y perspectivas éticas de Internet*. Roma, Italia: Ecclesia del Ateneo Pontificio Regina Apostolorum.
- Norton, W. (Mayo de 2001). *Internet Service Providers and Peering*.

Nur, A., & Tozal, M. (2024). Inferring Internet Topology at Point of Presence Level. doi:10.1109/SysCon61195.2024.10553435

Ñacato Gualotuña, M. A. (Enero de 2007). Diseño e implementación de una red privada virtual (VPN) para la empresa Hato telecomunicaciones. Obtenido de <http://bibdigital.epn.edu.ec/handle/15000/1309>

Palo Alto Networks. (2017). VM-Series on VMware NSX-T. Obtenido de <https://www.paloaltonetworks.lat/resources/datasheets/vm-series-for-vmware>

Palo Alto Networks. (19 de Mayo de 2021). *Panorama datasheet*. Obtenido de <https://www.paloaltonetworks.com/resources/datasheets/panorama-centralized-management-datasheet>

Palo Alto Networks. (2024). *VM-Series*. Obtenido de <https://docs.paloaltonetworks.com/vm-series>

Palo Alto Networks. (Noviembre de 2024). *VM-Series Deployment Guide*. Obtenido de <https://docs.paloaltonetworks.com/vm-series/11-1/vm-series-deployment/license-the-vm-series-firewall/vm-series-models>

Palo Alto Networks. (Agosto de 2024). *VM-Series Spec Sheet*. Obtenido de <https://www.paloaltonetworks.com/resources/datasheets/vm-series-spec-sheet>

Paredes, L. (2020). Modelo de infraestructura de red VPN para interconexión segura de datos en la Universidad Nacional del Altiplano. Puno, Perú.

Parziale, L., Britt, D., Davis, C., Forrester, J., & Liu, W. (2006). *TCP/IP Tutorial and Technical Overview*. IBM Corp.

Pomar, R. (Junio de 2019). Implementación de una red privada virtual de software libre en una empresa. Barcelona, España. Obtenido de <http://hdl.handle.net/10609/94606>

- Quintana, J. & Gallardo, E. (2021). Diseño de una red VPN full mesh para mejorar la comunicación y seguridad en una empresa metalmecánica de Lima. Lima.
- Rodriguez, Y. (2009). Fibra Óptica. Obtenido de <http://ebookcentral.proquest.com>
- Santhanamahalingam, S., Saravanan, A., & Karthikeyan, S. (2022). A study of cloud-based VPN establishment using network function virtualization technique. doi:<https://doi.org/10.1109/ICOSEC54921.2022.9951894>
- Schifani, A. (2022). Climate, infrastructure and the mediation of Miami: The spatial and discursive politics of the Network Access Point of the Americas. *Environmental Science, Political Science, Geography*.
- Tanenbaum, A., & Wetherall, D. (2012). *Redes de Computadoras*. Pearson Education, Inc.
- Telecom, C. (28 de Marzo de 2023). *Internet dedicado para empresas. ¿Por qué es esencial?* Obtenido de <https://www.c3ntro.com/es-mx/blog/internet-dedicado-por-que-es-esencial-para-las-empresas>
- Vargas, I. A. (2014). *Sistemas de Fibra óptica*. Mexico: Prenti Hall.
- Zapata, C. (2022). *¿Qué es internet dedicado y todas sus características?* Obtenido de <https://blog.internexa.com/es/empresas/que-es-internet-dedicado>

CAPITULO IX

ANEXOS

ANEXO A UBICACIÓN DE LAS SEDES



Figura 13: Ubicación de la Sede Principal. Fuente. Tomado de Google Earth como parte del estudio de factibilidad.



Figura 14: Ubicación de la Sede Remota 1. Fuente. Tomado de Google Earth como parte del estudio de factibilidad.

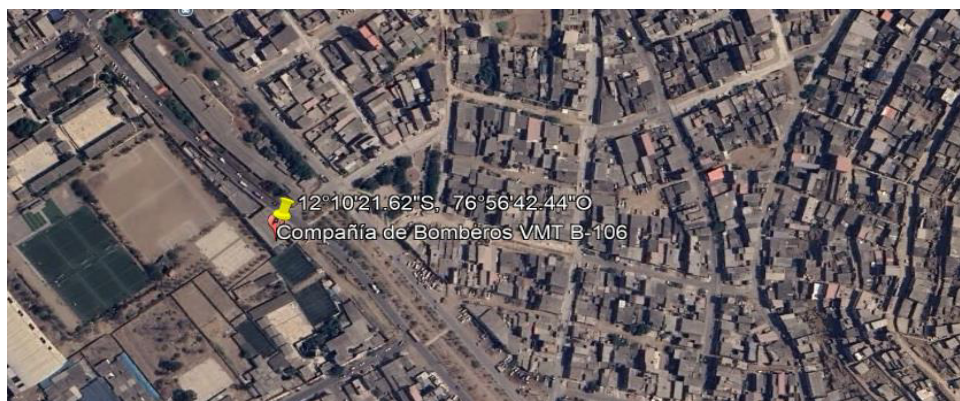


Figura 15: Ubicación de la Sede Remota 2. Fuente. Tomado de Google Earth como parte del estudio de factibilidad.



Figura 16: Ubicación de la Sede Remota 3. Fuente. Tomado de Google Earth como parte del estudio de factibilidad.



Figura 17: Ubicación de la Sede Remota 4. Fuente. Tomado de Google Earth como parte del estudio de factibilidad.

ANEXO B

CRONOGRAMA DE IMPLEMENTACIÓN

Tabla 15: Detalle de actividades, tiempos y responsables en la fase de implementación de la solución. propuesta.

CRONOGRAMA	TIEMPO	INICIO	FIN	Nombres de los recursos
FASE: IMPLEMENTACIÓN	45 días	10-10-24	11-12-24	
Sede Principal	25 días	10-10-24	16-11-24	
Visita técnica a sedes / Aprobación de Informes	5 días	10-10-24	16-10-24	Cliente, WIN
Revisión de despliegue de fibra óptica outdoor (desde nodo hasta sede)	8 días	17-10-24	28-10-24	WIN; Cliente
Validación de fibra indoor (dentro de la sede)	6 días	29-10-24	05-11-24	WIN
Instalación de equipos CPE y puesta en operación	3 días	06-11-24	08-11-24	WIN
Pruebas de conectividad y validación de servicio.	2 días	11-11-24	12-11-24	WIN
Firma de acta de implementación	1 días	15-11-24	16-11-24	Cliente, WIN
Sede Remota 1	25 días	23-10-24	29-11-24	
Visita técnica a sedes / Aprobación de Informes	5 días	23-10-24	29-10-24	Cliente, WIN
Revisión de despliegue de fibra óptica outdoor (desde nodo hasta sede)	8 días	30-11-24	11-11-24	WIN; Cliente
Validación de fibra indoor (dentro de la sede)	6 días	12-11-24	19-11-24	WIN
Instalación de equipos CPE y puesta en operación	3 días	20-11-24	22-11-24	WIN
Pruebas de conectividad y validación de servicio.	2 días	25-11-24	26-11-24	WIN
Firma de acta de implementación	1 días	28-11-24	29-11-24	Cliente, WIN
Sede Remota 2	25 días	18-10-24	24-11-24	
Visita técnica a sedes / Aprobación de Informes	5 días	18-10-24	24-10-24	Cliente, WIN
Revisión de despliegue de fibra óptica outdoor (desde nodo hasta sede)	8 días	25-10-24	06-11-24	WIN; Cliente
Validación de fibra indoor (dentro de la sede)	6 días	07-11-24	14-11-24	WIN
Instalación de equipos CPE y puesta en operación	3 días	15-11-24	19-11-24	WIN
Pruebas de conectividad y validación de servicio.	2 días	20-11-24	21-11-24	WIN
Firma de acta de implementación	1 días	23-11-24	24-11-24	Cliente, WIN
Sede Remota 3	25 días	10-10-24	14-11-24	
Visita técnica a sedes / Aprobación de Informes	5 días	10-10-24	16-10-24	Cliente, WIN
Revisión de despliegue de fibra óptica outdoor (desde nodo hasta sede)	8 días	17-10-24	28-10-24	WIN; Cliente
Validación de fibra indoor (dentro de la sede)	6 días	29-10-24	05-11-24	WIN
Instalación de equipos CPE y puesta en operación	3 días	06-11-24	08-11-24	WIN
Pruebas de conectividad y validación de servicio.	2 días	11-11-24	12-11-24	WIN
Firma de acta de implementación	1 días	13-11-24	14-11-24	Cliente, WIN
Sede Remota 4	25 días	05-11-24	11-12-24	
Visita técnica a sedes / Aprobación de Informes	5 días	05-11-24	11-11-24	Cliente, WIN
Revisión de despliegue de fibra óptica outdoor (desde nodo hasta sede)	8 días	12-11-24	21-11-24	WIN; Cliente
Validación de fibra indoor (dentro de la sede)	6 días	22-11-24	29-11-24	WIN
Instalación de equipos CPE y puesta en operación	3 días	02-12-24	4-12-24	WIN
Pruebas de conectividad y validación de servicio.	2 días	05-12-24	06-12-24	WIN
Firma de acta de implementación	1 días	10-12-24	11-12-24	Cliente, WIN

Fuente: Elaboración propia a partir del cronograma de implementación del proyecto (2024).

ANEXO C

INSTALACIÓN DE EQUIPOS EN SEDES REMOTAS



Figura 18: Instalación de CPE Cisco 1121-4P en Sede Remota 1. Fuente. Imagen tomada durante la implementación del proyecto en la sede Remota 1, con equipo CPE Cisco 1121-4P. WIN Empresas (2024).

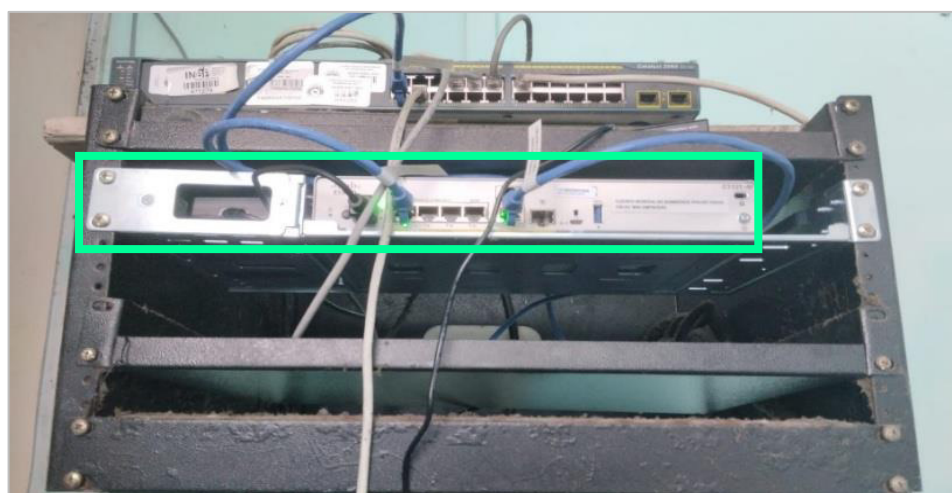


Figura 19: Instalación de CPE Cisco 1121-4P en la Sede Remota 2. Fuente. Imagen tomada durante la implementación del proyecto en la sede Remota 2, con equipo CPE Cisco 1121-4P. WIN Empresas (2024).

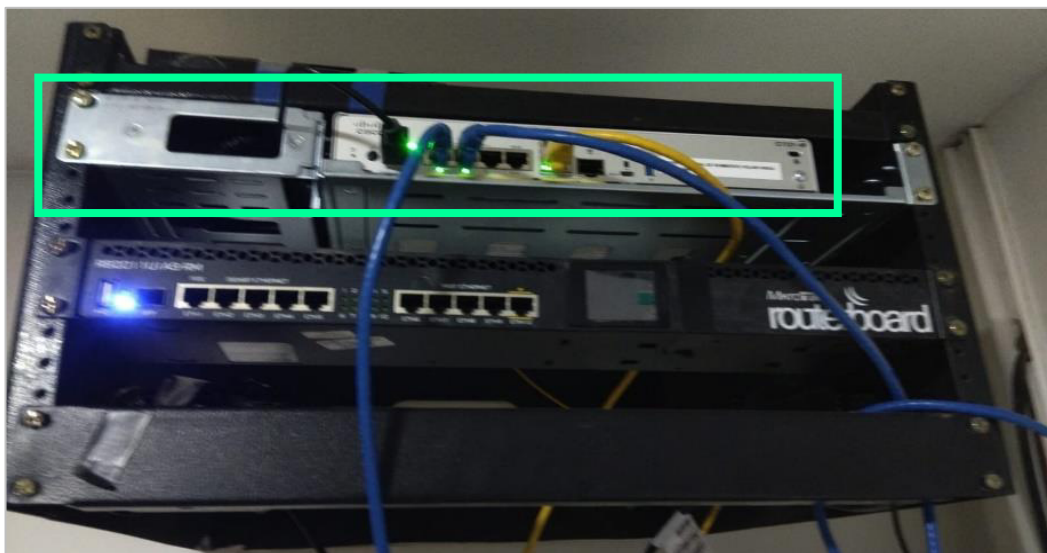


Figura 20: Instalación de CPE Cisco 1121-4P en la Sede Remota 3. Fuente. Imagen tomada durante la implementación del proyecto en la sede Remota 3, con equipo CPE Cisco 1121-4P. WIN Empresas (2024).



Figura 21: Instalación de CPE Cisco 1121-4P en la Sede Remota 4. Fuente. Imagen tomada durante la implementación del proyecto en la sede Remota 4, con equipo CPE Cisco 1121-4P. WIN Empresas (2024).

ANEXO D

VALIDACIÓN DE ACTIVACIÓN DE EQUIPOS CPE

```

10.40.171.58 - PuTTY

CID011190 uptime is 5 weeks, 4 days, 3 hours, 58 minutes
System returned to ROM by power-on
System restarted at 13:17:14 pet Thu Nov 28 2024
System image file is "flash:/c3560-ipervicesk9-mz.122-58.SE2.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco WS-C3560G-24TS (PowerPC405) processor (revision A0) with 131072K bytes of memory.
Processor board ID FOC0909U0UB
Last reset from power-on
5 Virtual Ethernet interfaces
28 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address      : 00:13:7F:13:DE:00
Motherboard assembly number    : 73-9708-03
Power supply part number       : 341-0098-01
Motherboard serial number      : FOC09084S7H
Power supply serial number      : DCA085105SC
Model revision number          : A0
Motherboard revision number    : A0
Model number                   : WS-C3560G-24TS-S
System serial number           : FOC0909U0UB
SFP Module assembly part number : 73-7757-02
SFP Module revision Number     : A0
SFP Module serial number       : CAT09070LM8
Top Assembly Part Number       : 800-25864-01
Top Assembly Revision Number   : A0
Version ID                     : 01
CLEI Code Number               : CNMW200ARA
Hardware Board Revision Number : 0x05

Switch Ports Model          SW Version  SW Image
-----
*    1 28 WS-C3560G-24TS  12.2 (58) SE2  C3560-IPSERVICESK9-M

Configuration register is 0xF

```

Figura 22: Activación de Router Cisco C3560G-24TS en Sede Principal.
Fuente. Fotografía proporcionada por Win Empresas durante la etapa de implementación en la Sede Principal.

```

10.40.81.178 - PuTTY
CPE-MULTISERVICE uptime is 4 weeks, 3 days, 21 hours, 1 minute
Uptime for this control processor is 4 weeks, 3 days, 21 hours, 2 minutes
System returned to ROM by Reload Command at 18:54:18 pet Thu Dec 5 2024
System restarted at 18:57:55 pet Thu Dec 5 2024
System image file is "bootflash:c1100-universalk9.17.06.06a.SPA.bin"
Last reload reason: Reload Command

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Suite License Information for Module:'esg'

-----
Suite                Suite Current      Type                Suite Next reboot
-----
FoundationSuiteK9    None                Smart License      None

securityk9
appxk9

Technology Package License Information:

-----
Technology            Technology-package      Technology-package
Current              Type                  Next reboot
-----
appxk9                None                  Smart License      None
uck9                  None                  Smart License      None
securityk9            None                  Smart License      None
ipbase                ipbasek9              Smart License      ipbasek9

The current throughput level is unthrottled

Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco C1121-4P (1RU) processor with 1400294K/6147K bytes of memory.
Processor board ID FGL2827LDTL
Router operating mode: Autonomous
3 Virtual Ethernet interfaces
6 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
2945023K bytes of flash memory at bootflash:..

```

Figura 23: Activación de Router Cisco 1121-4P en la Sede Remota 1.
Fuente. Fotografía proporcionada por Win Empresas durante la etapa de implementación en la Sede Remota 1.

```

10.40.73.158 - PuTTY
CPE-MULTISERVICE uptime is 4 days, 11 hours, 8 minutes
Uptime for this control processor is 4 days, 11 hours, 9 minutes
System returned to ROM by PowerOn at 17:36:02 pet Fri Dec 6 2024
System restarted at 05:10:28 pet Thu Jan 2 2025
System image file is "bootflash:cll100-universalk9.17.06.06a.SPA.bin"
Last reload reason: PowerOn

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Suite License Information for Module:'esg'

-----
Suite                Suite Current      Type                Suite Next reboot
-----
FoundationSuiteK9    None                Smart License      None
securityk9
appxk9

Technology Package License Information:

-----
Technology    Technology-package    Technology-package
              Current           Type                Next reboot
-----
appxk9        None                Smart License      None
uck9          None                Smart License      None
securityk9    None                Smart License      None
ipbase        ipbasek9            Smart License      ipbasek9

The current throughput level is unthrottled

Smart Licensing Status: Registration Not Applicable/Not Applicable
cisco C1121-4P (1RU) processor with 1400294K/6147K bytes of memory.
Processor board ID FGL2827LDQ5
Router operating mode: Autonomous
3 Virtual Ethernet interfaces
6 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
2945023K bytes of flash memory at bootflash:.

Configuration register is 0x2102

```

Figura 24: Activación de Router Cisco 1121-4P en la Sede Remota 2.
Fuente. Fotografía proporcionada por Win Empresas durante la etapa de implementación en la Sede Remota 2.

```

10.40.89.42 - PuTTY
CPE-MULTISERVICE uptime is 1 day, 5 hours, 0 minutes
Uptime for this control processor is 1 day, 5 hours, 2 minutes
System returned to ROM by PowerOn
System restarted at 11:38:23 pet Sun Jan 5 2025
System image file is "bootflash:c1100-universalk9.17.06.06a.SPA.bin"
Last reload reason: PowerOn

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Suite License Information for Module:'esg'

-----
Suite                Suite Current      Type                Suite Next reboot
-----
FoundationSuiteK9    None                Smart License      None

securityk9
appxk9

Technology Package License Information:

-----
Technology    Technology-package    Technology-package
              Current          Type                Next reboot
-----
appxk9        None                Smart License      None
uck9          None                Smart License      None
securityk9    None                Smart License      None
ipbase        ipbasek9            Smart License      ipbasek9

The current throughput level is unthrottled

Smart Licensing Status: Registration Not Applicable/Not Applicable
cisco C1121-4P (1RU) processor with 1400294K/6147K bytes of memory.
Processor board ID FGL2827LDRP
Router operating mode: Autonomous
3 Virtual Ethernet interfaces
6 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
2945023K bytes of flash memory at bootflash:.

```

Figura 25: Activación de Router Cisco 1121-4P en la Sede Remota 3.
Fuente. Fotografía proporcionada por Win Empresas durante la etapa de implementación en la Sede Remota 3.

```

10.40.108.166 - PuTTY
CPE-MULTISERVICE uptime is 2 weeks, 6 days, 3 hours, 4 minutes
Uptime for this control processor is 2 weeks, 6 days, 3 hours, 6 minutes
System returned to ROM by PowerOn at 15:31:13 pet Tue Dec 3 2024
System restarted at 13:52:19 pet Tue Dec 17 2024
System image file is "bootflash:cll00-universalk9.17.06.06a.SPA.bin"
Last reload reason: PowerOn

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Suite License Information for Module:'esg'

-----
Suite                Suite Current      Type                Suite Next reboot
-----
FoundationSuiteK9    None                Smart License      None
securityk9
appxk9

Technology Package License Information:

-----
Technology            Technology-package      Technology-package
Current              Type                    Next reboot
-----
appxk9                None                    Smart License      None
uck9                  None                    Smart License      None
securityk9            None                    Smart License      None
ipbase                ipbasek9                Smart License      ipbasek9

The current throughput level is unthrottled

Smart Licensing Status: Registration Not Applicable/Not Applicable
cisco C1121-4P (1RU) processor with 1400294K/6147K bytes of memory.
Processor board ID FGL2827LE5M
Router operating mode: Autonomous
3 Virtual Ethernet interfaces
6 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
2945023K bytes of flash memory at bootflash:.

Configuration register is 0x2102

```

Figura 26: Activación de Router Cisco 1121-4P en la Sede Remota 4.
Fuente. Fotografía proporcionada por Win Empresas durante la etapa de implementación en la Sede Remota 4.

ANEXO E: PRUEBAS DE VALIDACIÓN DEL SISTEMA EN CAMPO

- Pruebas de ping y latencia para verificar la estabilidad de los enlaces.
 - i. Desde sede principal a sedes remotas:

```

10.40.171.58 - PuTTY
CID011190>ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
CID011190>ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
CID011190>ping 192.168.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
CID011190>ping 192.168.4.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
CID011190>
  
```

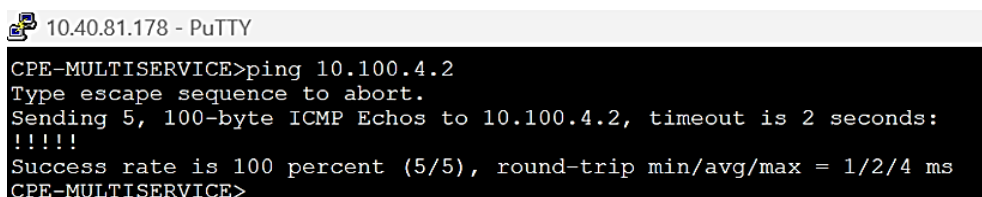
Figura 27: Prueba de Ping y Round Trip Time (RTT) de Sede Principal a Sedes Remotas. Fuente. Imagen proporcionada por Win Empresas durante la fase de validación de enlaces.

Tabla 16: Valores de pruebas realizadas en Sede Principal.

Nº	Destino	Pérdida de paquetes	RTT min (ms)	RTT max (ms)	RTT avg (ms)
1	192.168.1.1	0%	1	8	3
2	192.168.2.1	0%	1	9	5
3	192.168.3.1	0%	1	9	4
4	192.168.4.1	0%	1	9	4

Fuente: Elaboración propia

ii. Desde Sede Remota 1 a Sede Principal



```

10.40.81.178 - PuTTY
CPE-MULTISERVICE>ping 10.100.4.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
CPE-MULTISERVICE>

```

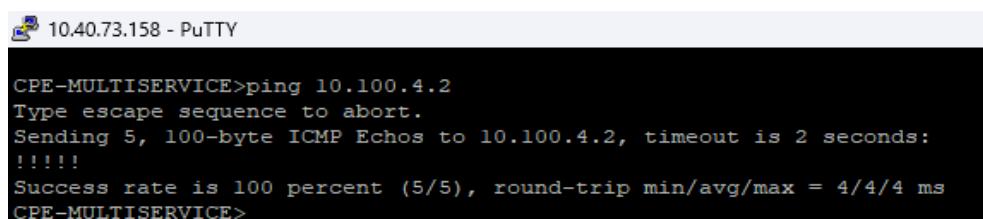
Figura 28: Prueba de Ping y RTT desde Sede Remota 1 a Sede Principal. Fuente. Imagen proporcionada por Win Empresas durante la fase de validación de enlaces.

Tabla 17: Valores de pruebas realizadas en sede Remota 1.

Nº	Destino	Pérdida de paquetes	RTT min (ms)	RTT max (ms)	RTT avg (ms)
1	10.100.4.2	0%	1	2	4

Fuente. Elaboración Propia.

iii. Desde Sede Remota 2 a Sede Principal:



```

10.40.73.158 - PuTTY
CPE-MULTISERVICE>ping 10.100.4.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
CPE-MULTISERVICE>

```

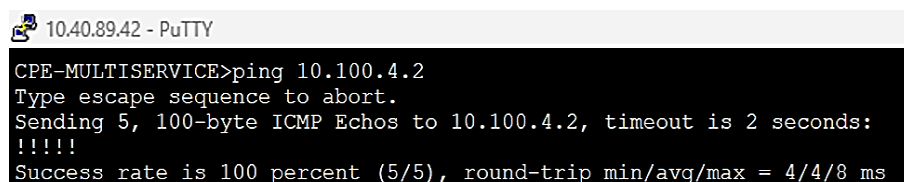
Figura 29: Prueba de Ping y RTT desde Sede Remota 2 a Sede Principal. Fuente. Imagen proporcionada por Win Empresas durante la fase de validación de enlaces.

Tabla 18: Valores de pruebas realizadas en sede Remota 2

Nº	Destino	Pérdida de paquetes	RTT min (ms)	RTT max (ms)	RTT avg (ms)
1	10.100.4.2	0%	4	4	4

Fuente: Elaboración Propia.

iv. Desde Sede Remota 3 a Sede Principal



```

10.40.89.42 - PuTTY
CPE-MULTISERVICE>ping 10.100.4.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

```

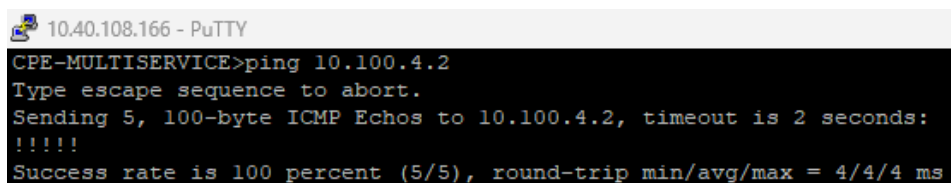
Figura 30: Prueba de Ping y RTT desde Sede Remota 3 a Sede Principal Fuente. Imagen proporcionada por Win Empresas durante la fase de validación de enlaces.

Tabla 19: Valores de pruebas realizadas en sede Remota 3.

N°	Destino	Pérdida de paquetes	RTT min (ms)	RTT max (ms)	RTT avg (ms)
1	10.100.4.2	0%	4	4	8

Fuente. Elaboración propia.

v. Desde Sede Remota 4 a Sede Principal



```

10.40.108.166 - PuTTY
CPE-MULTISERVICE>ping 10.100.4.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

```

Figura 31: Prueba de Ping y RTT desde Sede Remota 4 a Sede Principal. Fuente. Imagen proporcionada por Win Empresas durante la fase de validación de enlaces.

Tabla 20: Valores de pruebas realizadas en Sede Remota 4

N°	Destino	Pérdida de paquetes	RTT min (ms)	RTT max (ms)	RTT avg (ms)
1	10.100.4.2	0%	4	4	4

Fuente. Elaboración propia.

- **Medición del ancho de banda en cada enlace**

A continuación, se valida la medición de ancho de banda en todas las sedes mediante la Herramienta Speed Test, la cual permite evaluar aspectos clave como la velocidad de descarga, la velocidad de carga y la latencia (ping) de conexión.

- i. **Sede Principal:** Se valida que tanto las velocidades de subida y de bajada son simétricas. La latencia hacia el servidor de WIN Empresas es de 1ms, lo cual valida que la conexión es eficiente.

El ancho de banda de esta sede es de 1Gbps. De acuerdo con la medición, se está garantizado un 91.8% en la descarga y 93.3% en la carga, lo cual es una excelente tasa de utilización en condiciones óptimas.



Figura 32: Medición de ancho de banda en la Sede Principal.
Fuente. Imagen proporcionada por Win Empresas durante la fase de validación de ancho de banda.

- ii. **Sede Remota 1:** Se valida que tanto las velocidades de subida y de bajada son simétricas. La latencia hacia el servidor de WIN Empresas es de 2ms, lo cual valida que la conexión es eficiente.

El ancho de banda de esta sede es de 200 Mbps. De acuerdo con la medición, se está garantizado un 96.0% en la carga y 97.7% en la descarga, lo cual es una excelente tasa de utilización en condiciones óptimas.

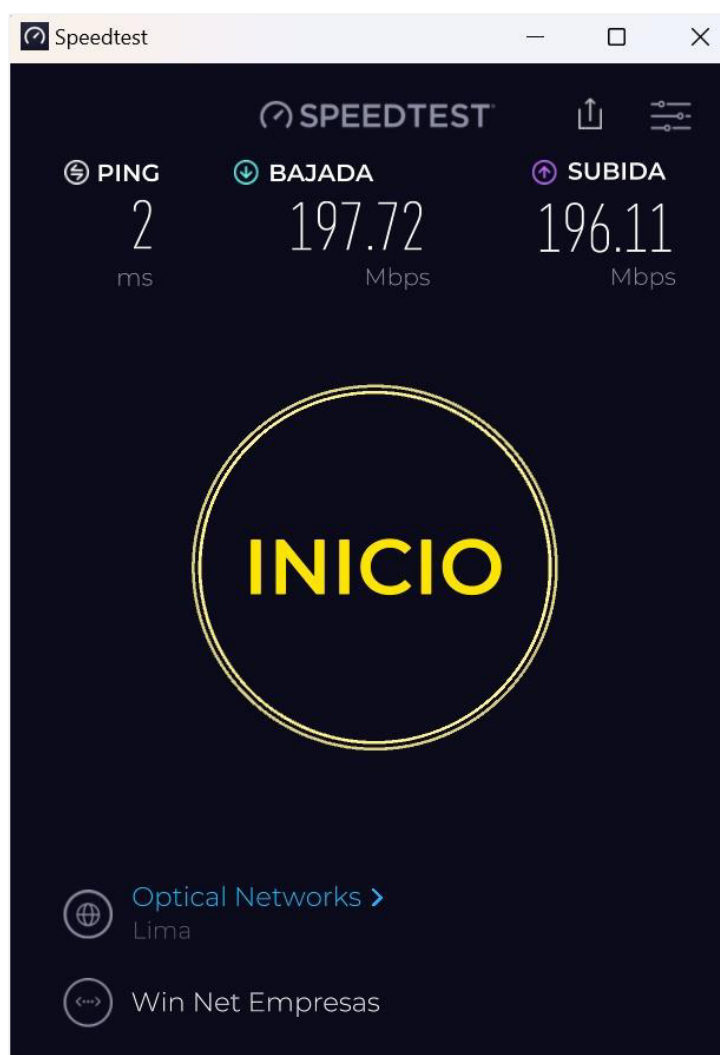


Figura 33: Medición de ancho de banda en la Sede Remota 1.
Fuente. Imagen proporcionada por Win Empresas durante la fase de validación de ancho de banda.

iii. **Sede Remota 2:** Se valida que tanto las velocidades de subida y de bajada son simétricas. La latencia hacia el servidor de WIN Empresas es de 2ms, lo cual valida que la conexión es eficiente.

El ancho de banda de esta sede es de 200 Mbps. De acuerdo con la medición, se está garantizado un 93.0% en la descarga y 91.5% en la carga, lo cual es una excelente tasa de utilización en condiciones óptimas.

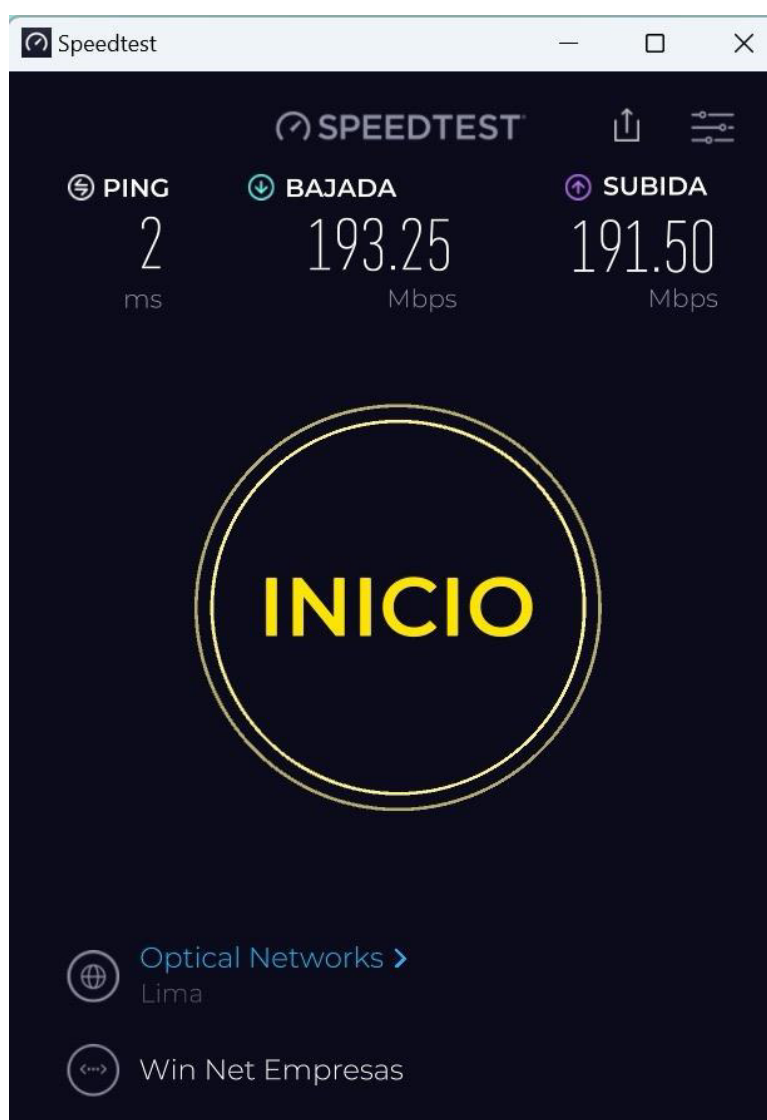


Figura 34: Medición de ancho de banda en la Sede Remota 2.
Fuente. Imagen proporcionada por Win Empresas durante la fase de validación de ancho de banda.

iv. Sede Remota 3: Se valida que tanto las velocidades de subida y de bajada son simétricas. La latencia hacia el servidor de WIN Empresas es de 2ms, lo cual valida que la conexión es eficiente.

El ancho de banda de esta sede es de 200 Mbps. De acuerdo con la medición, se está garantizado un 97.0% en la descarga y 101.78% en la carga, lo cual es una excelente tasa de utilización en condiciones óptimas.

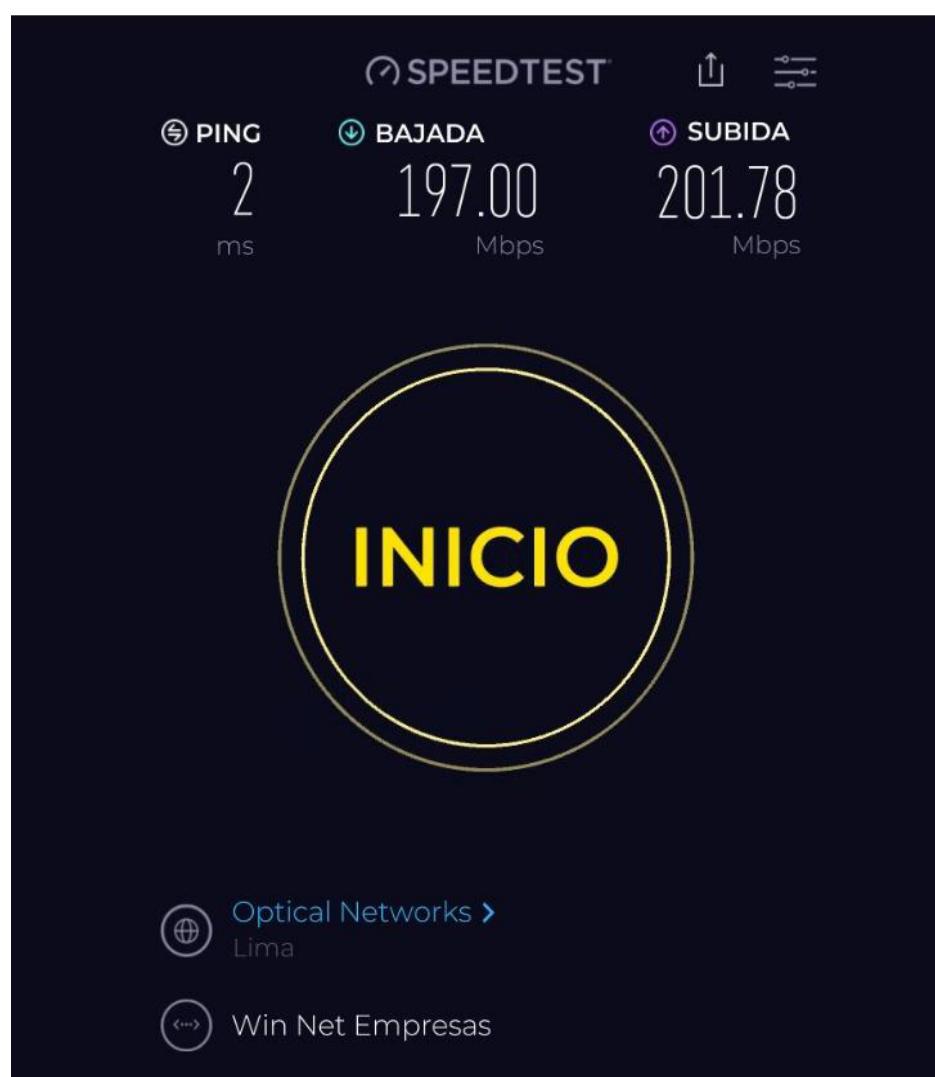


Figura 35: Medición de ancho de banda en la Sede Remota 3. Fuente. Imagen proporcionada por Win Empresas durante la fase de validación de ancho de banda.

- v. **Sede Remota 4:** Se valida que tanto las velocidades de subida y de bajada son simétricas. La latencia hacia el servidor de WIN Empresas es de 2ms, lo cual valida que la conexión es eficiente.

El ancho de banda de esta sede es de 200 Mbps. De acuerdo con la medición, se está garantizado un 104% en la descarga y 114% en la carga, lo cual es una excelente tasa de utilización en condiciones óptimas.

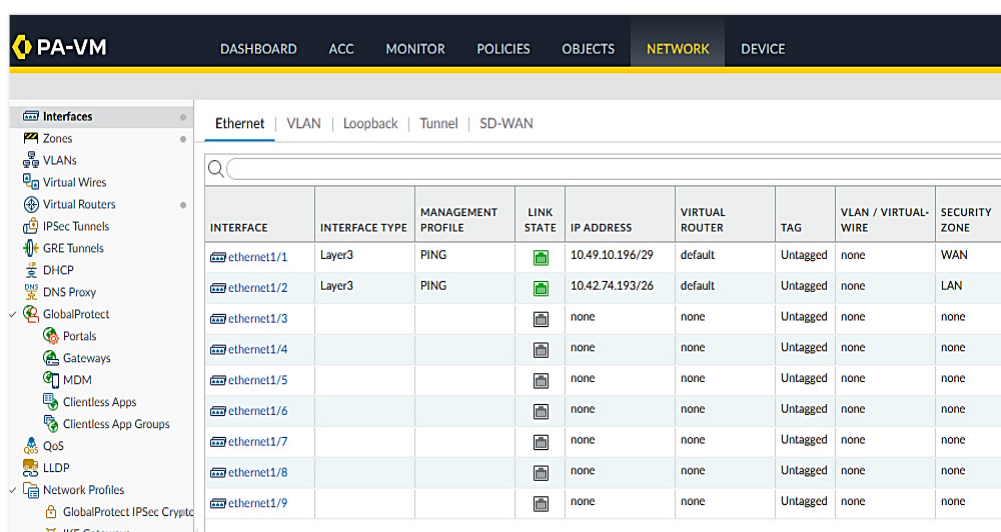


Figura 36: Medición de ancho de banda en la Sede Remota 4.
Fuente. Imagen proporcionada por Win Empresas durante la fase de validación de ancho de banda.

- **Validación de configuración de las políticas de seguridad implementadas en el firewall.**

Las siguientes configuraciones corresponden a la implementación en el firewall VM-700, donde se validan parámetros críticos como interfaces, direcciones IP, rutas y reglas de seguridad, con el fin de garantizar la operación segura y confiable de la red.

- Configuración de Interfaces WAN/LAN en VM-700:** Se valida la configuración de direcciones IP de acuerdo con el provisionamiento de recursos indicado en la tabla 8.



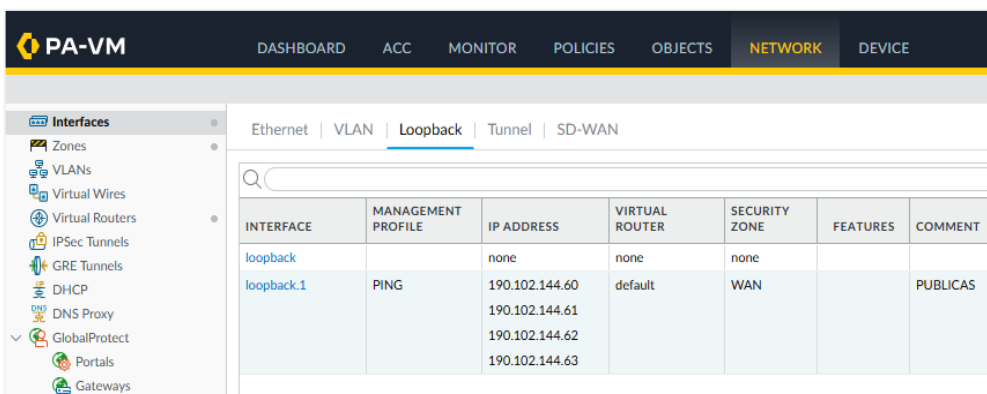
The screenshot shows the Palo Alto VM-700 configuration interface. The top navigation bar includes 'PA-VM', 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK' (highlighted), and 'DEVICE'. The left sidebar lists various configuration categories, with 'Network Profiles' and 'GlobalProtect IPsec Cryptic' checked. The main content area is titled 'Ethernet' and displays a table of interface configurations.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL WIRE	SECURITY ZONE
ethernet1/1	Layer3	PING		10.49.10.196/29	default	Untagged	none	WAN
ethernet1/2	Layer3	PING		10.42.74.193/26	default	Untagged	none	LAN
ethernet1/3				none	none	Untagged	none	none
ethernet1/4				none	none	Untagged	none	none
ethernet1/5				none	none	Untagged	none	none
ethernet1/6				none	none	Untagged	none	none
ethernet1/7				none	none	Untagged	none	none
ethernet1/8				none	none	Untagged	none	none
ethernet1/9				none	none	Untagged	none	none

Figura 37: Configuración WAN/LAN en Palo Alto VM-700. Fuente. Registro técnico de la configuración de interfaces WAN/LAN en el firewall VM-700, correspondiente a la implementación del proyecto en WIN Empresas (2024).

Esta validación permitió comprobar que las direcciones IP aprovisionadas en el firewall coinciden con las asignadas en el diseño lógico de la red, garantizando coherencia en la configuración. Asimismo, se evidencia que la implementación cumple con las buenas prácticas de seguridad y facilita la trazabilidad del proceso de instalación.

- ii. **Configuración de IPs Públicas:** Se valida la configuración del pool de IPs asignado de acuerdo con el provisionamiento de recursos indicado en la tabla 8.

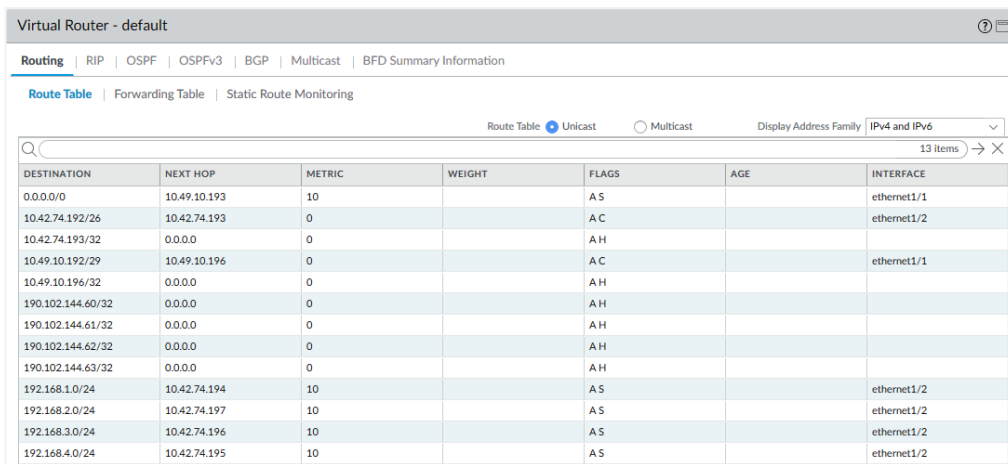


The screenshot shows the Palo Alto VM-700 Network configuration page. The 'Loopback' tab is selected under the 'Interfaces' section. The configuration table shows the following details:

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FEATURES	COMMENT
loopback		none	none	none		
loopback.1	PING	190.102.144.60	default	WAN		PUBLICAS
		190.102.144.61				
		190.102.144.62				
		190.102.144.63				

Figura 38: Configuración de pool de IPs en Palo Alto VM-700. Fuente. Registro técnico de la implementación realizada en WIN Empresas (2024).

- iii. **Configuración de Routing:** Se valida la configuración de rutas con direccionamiento hacia las IPs asignadas en cada sede de acuerdo con el provisionamiento de recursos lógicos



The screenshot shows the Palo Alto VM-700 Routing configuration page for the 'Virtual Router - default'. The 'Route Table' tab is selected. The configuration shows the following details:

DESTINATION	NEXT HOP	METRIC	WEIGHT	FLAGS	AGE	INTERFACE
0.0.0.0/0	10.49.10.193	10		A S		ethernet1/1
10.42.74.192/26	10.42.74.193	0		A C		ethernet1/2
10.42.74.193/32	0.0.0.0	0		A H		
10.49.10.192/29	10.49.10.196	0		A C		ethernet1/1
10.49.10.196/32	0.0.0.0	0		A H		
190.102.144.60/32	0.0.0.0	0		A H		
190.102.144.61/32	0.0.0.0	0		A H		
190.102.144.62/32	0.0.0.0	0		A H		
190.102.144.63/32	0.0.0.0	0		A H		
192.168.1.0/24	10.42.74.194	10		A S		ethernet1/2
192.168.2.0/24	10.42.74.197	10		A S		ethernet1/2
192.168.3.0/24	10.42.74.196	10		A S		ethernet1/2
192.168.4.0/24	10.42.74.195	10		A S		ethernet1/2

Figura 39: Tabla de rutas en Palo Alto VM-700. Registro técnico de la implementación realizada en WIN Empresas (2024).

- iv. **Configuración de Políticas de Firewall:** Se validó la correcta aplicación de las políticas de seguridad para proteger el perímetro de la red. Dentro de estas, se establecieron reglas específicas para bloquear direcciones IP asociadas a actividades maliciosas, tales como aquellas utilizadas para distribuir malware, lanzar ataques de comando y control o alojar contenido ilícito. Asimismo, se configuró la denegación de IPs de alto riesgo incluidas en listas de reputación de amenazas compiladas por Palo Alto.

En adición, se aplicaron filtros para bloquear el tráfico proveniente de direcciones IP vinculadas a la red Tor, debido a su alta asociación con comportamientos maliciosos en entornos corporativos.

Finalmente, se habilitaron únicamente los servicios seguros y autorizados de DNS, HTTP y HTTPS, garantizando así la disponibilidad de los recursos legítimos y la protección de la infraestructura crítica.

PA-VM

DASH-BOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICE

Log Connect

Security

NAT

QoS

Policy Based Forwarding

Deserialization

Tunnel Inspection

Application Overwrite

Authentication

DoS Protection

IDS-VM

1

BLOCK-ETH-IN

Block

Nonpassive

Universal

LAN

Palo Alto Networks - Bulkyhost IP addresses

Palo Alto Networks - High risk IP addresses

Palo Alto Networks - Known malicious IP addresses

Palo Alto Networks - Tor exit IP addresses

any

any

LAN

any

any

any

any

application-default

deny

None

2

BLOCK-ETH-OUT

Nonpassive

Block

Universal

LAN

any

Palo Alto Networks - Subnet of IP addresses

Palo Alto Networks - High risk IP addresses

Palo Alto Networks - Known malicious IP addresses

Palo Alto Networks - Tor exit IP addresses

any

any

YUAN

any

any

any

any

application-default

deny

None

3

DNS

Nonpassive

Universal

LAN

LAN-SUBNETS

any

any

YUAN

any

any

any

dns

DNS

Allow

Log

Alert

Generate Report

4

WEB-BROWSING

Nonpassive

Universal

LAN

LAN-SUBNETS

any

any

YUAN

any

any

any

web-browsing

HTTP

Allow

Log

Alert

Generate Report

5

PERMIT-ALL

Nonpassive

Universal

LAN

LAN-SUBNETS

any

any

YUAN

any

any

any

any

any

Allow

Log

Alert

Generate Report

Figura 40: Configuración de políticas de firewall en Palo Alto VM-700. Registro técnico de la implementación realizada en WIN Empresas (2024).

Para una mejor comprensión, la Tabla 21 resume estas configuraciones de seguridad implementadas en el firewall VM-700, complementando la evidencia mostrada en la Figura 40.

Tabla 21: Resumen de las políticas de seguridad configuradas en el firewall VM-700.

Nombre de la Regla	Tipo	Zona Origen	Zona Destino	Servicio	Acción	Observación
Block-Bulk-In	Virtual IP	LAN	WAN	Any	Deny	Bloqueo de IPs sospechosas (lista negra de Palo Alto).
Block-Kix Out	Virtual IP	LAN	WAN	Any	Deny	Bloqueo de tráfico saliente hacia IPs maliciosas (Tor, C2).
DNS	Virtual IP	LAN SUBNETS	WAN	DNS	Allow	Permite consultas DNS seguras.
Web Browsing	Virtual IP	LAN SUBNETS	WAN	HTTP HTTPS	Allow	Permite navegación web legítima.
Permit All	Virtual IP	LAN SUBNETS	WAN	Any	Allow	Permite acceso general a la red para tráfico autorizado

Fuente. Elaboración propia a partir de configuración realizada en el firewall VM-700 de WIN Empresas (2024).

- v. Configuración de filtros de páginas web:** Se valida la correcta configuración del perfil de filtros URL para proteger la navegación de los usuarios de la Entidad. Las siguientes categorías se encuentran bloqueadas: Contenido para adultos, comando y

control, extremism, grayware, high-risk, malware, phishing, ransomware.

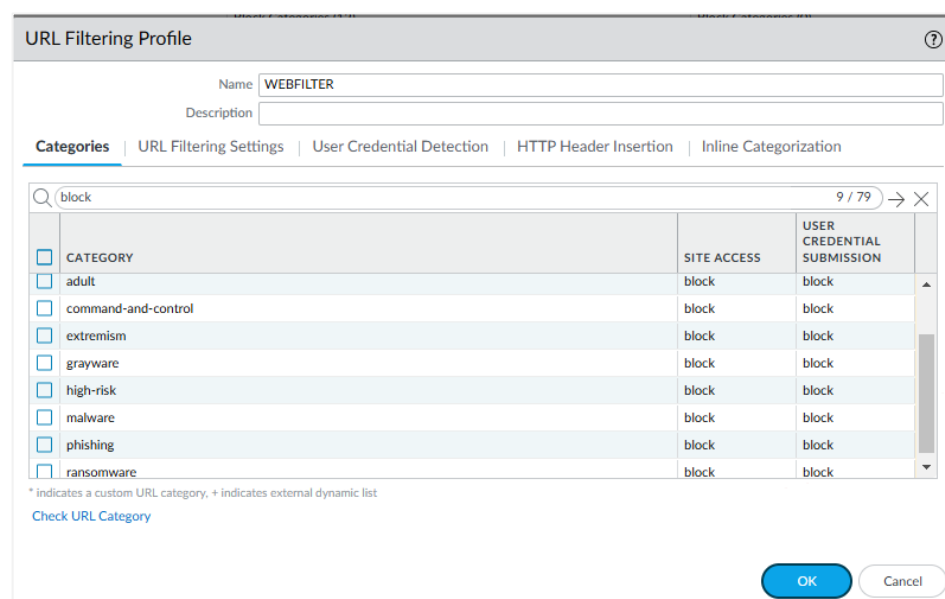


Figura 41: Categoría de webfilter bloqueadas en Palo Alto VM-700. Fuente. Registro técnico de la implementación realizada en WIN Empresas (2024).

- vi. **Reporte de tráfico:** El análisis de tráfico constituye una herramienta fundamental para detectar anomalías en tiempo real, ya que permite advertir comportamientos inusuales que podrían estar vinculados a incidentes de seguridad, como intentos de intrusión o transferencia no autorizada de información.

En la Figura 42 se puede observar el monitoreo de tráfico de los últimos 7 días referente al Uso de Aplicaciones, donde se muestran las aplicaciones más visitadas, el consumo de datos en bytes, la cantidad de sesiones, los intentos de ataque, la cantidad de direcciones URLs accedidas y el número de usuarios que utilizaron cada aplicación. Esta información resulta esencial para identificar patrones de comportamiento, detectar posibles abusos de recursos y establecer prioridades de gestión del ancho de banda.

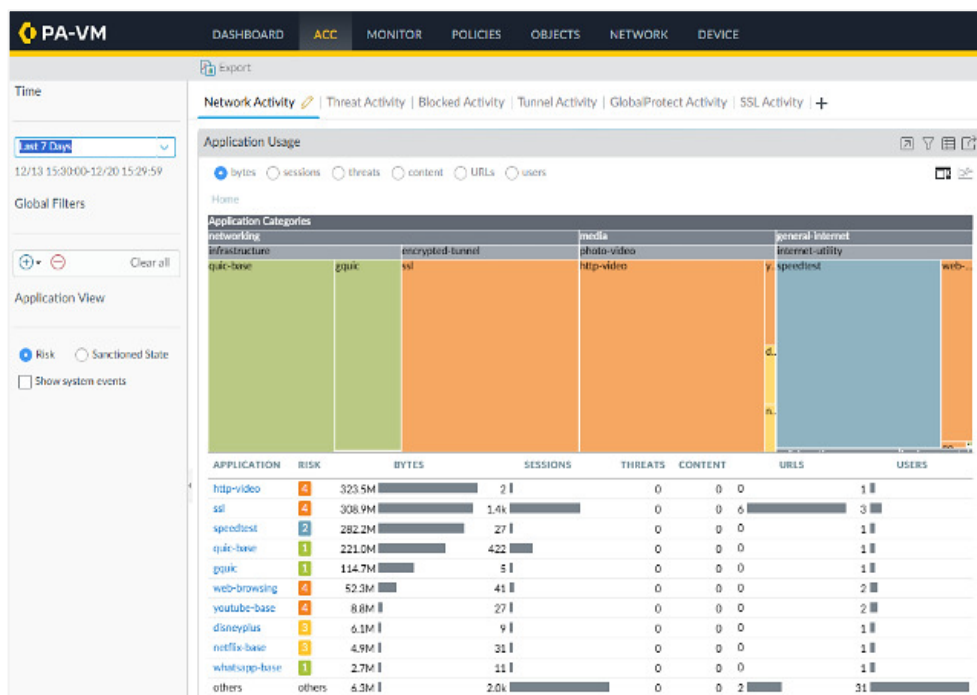


Figura 42: Portal de Monitoreo en Palo Alto VM-700 para uso de aplicaciones. Fuente: Registro técnico de la implementación realizada en WIN Empresas (2024).

En la Figura 43 se puede observar el monitoreo de tráfico de los últimos 7 días referente a la Actividad de Usuarios. Esto permite validar el volumen de datos transmitidos y recibidos, correlacionando esta información con políticas de uso aceptable de la red.

Esto no solo ayuda a optimizar los recursos de conectividad, sino que también permite detectar conductas inusuales, como consumos excesivos de datos por parte de un único usuario o intentos de acceder a aplicaciones no autorizadas.

Finalmente, la integración de estos reportes dentro del sistema de gestión de seguridad fortalece la toma de decisiones estratégicas, ya que aporta evidencia objetiva para priorizar inversiones en infraestructura, aplicar controles adicionales de seguridad y garantizar la continuidad operativa de los servicios críticos de la Entidad.

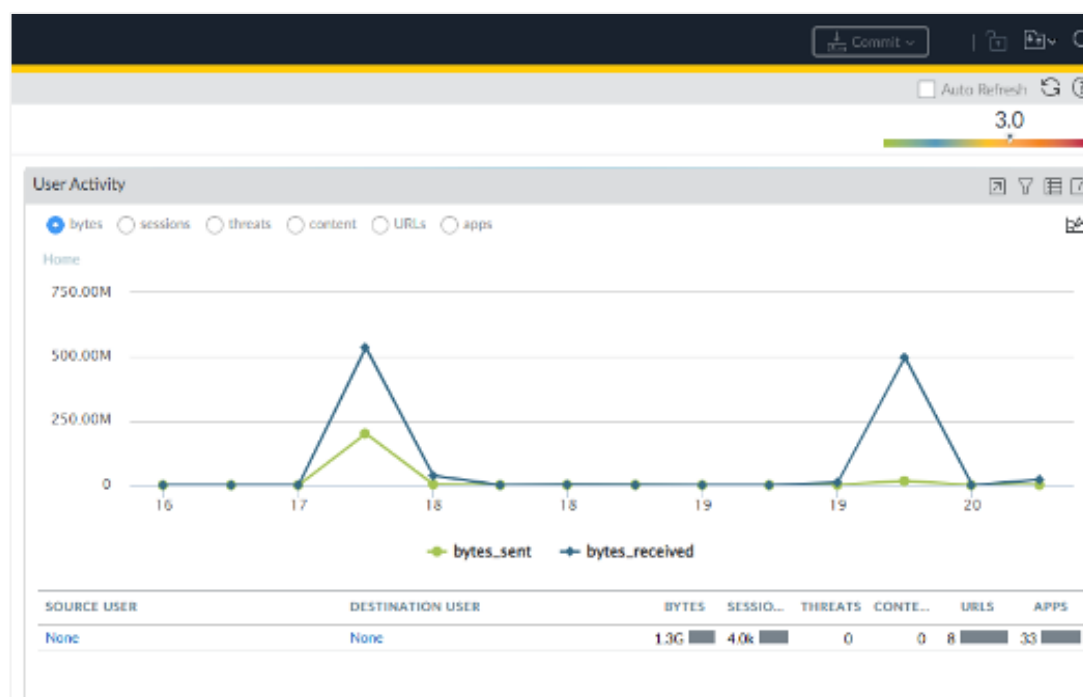


Figura 43: Portal de Monitoreo en Palo Alto VM-700 para la actividad de usuarios. Fuente: Registro técnico de la implementación realizada en WIN Empresas (2024).