

SERVICIO DE SOLUCIÓN INTEGRAL DE SEGURIDAD PERIMETRAL PARA EL OEFA**1. DENOMINACIÓN DE LA CONTRATACIÓN**

SERVICIO DE SOLUCIÓN INTEGRAL DE SEGURIDAD PERIMETRAL PARA EL OEFA

2. AREA USUARIA

Oficina de Tecnologías de la Información

3. FINALIDAD PÚBLICA

El presente servicio permitirá contar con el servicio de soporte y mantenimiento para garantizar la Operatividad y Seguridad de la red de datos del Organismo de Evaluación y Fiscalización Ambiental (En adelante OEFA), en beneficio de los colaboradores de la Institución, Administrados y Público en General.

3.1. OBJETIVO/META DEL POI VINCULADO

Mantener la operatividad, soporte y mantenimiento del equipamiento de seguridad Check Point del OEFA.

Tabla 01: Objetivo POI vinculado

Unidad Orgánica	Actividad presupuestal	Actividad Operativa	Tarea del POI
OTI	5000276 - gestión del programa	Implementación de Proyectos de Tecnologías de la Información y Comunicación	OTI 014254 - GESTIÓN DE INFRAESTRUCTURA Y SERVICIOS DE TI

4. ANTECEDENTES

El **11 de enero de 2016**, mediante Contrato N° 001-2016-OEFA derivado de una licitación pública N° 008- 2015-OEFA – Primera Convocatoria, se realizó la **“Adquisición de una solución de firewall”** con la empresa **VILSOL S.A.C** por un período de tres (03) años, contabilizados a partir del día calendario siguiente de suscrito el contrato, por un monto de S/. 3,280,000.00, tanto para la prestación principal como la prestación accesoria.

El **26 de noviembre de 2018**, mediante la Resolución N° 222-2018-OEFA/OAD, se aprobó la estandarización del **“Servicio de Soporte y Mantenimiento del Equipamiento de Seguridad Check Point del OEFA”**, cuya vigencia finalizó el 25 de noviembre de 2021.

El **05 de julio de 2019**, mediante Contrato N° 022-2019-OEFA derivado del concurso público N° 005- 2019-OEFA – Primera Convocatoria, se realizó la contratación del **“Servicio de soporte y mantenimiento al equipamiento de seguridad firewall checkpoint”**, con la empresa **GRUPO ELECTRODATA S.A.C** por un período de trescientos sesenta y cinco (365) días calendario, contabilizados a partir del día calendario siguiente de suscrito el contrato y cuya fecha fin del servicio se cumple el 05 de julio de 2020, por un monto de S/. 1,462,350.22, tanto para la prestación principal como la prestación accesoria.

El **05 de julio de 2020**, mediante Contrato N° 022-2019-OEFA se realizó la contratación COMPLEMENTARIA del **“Servicio de soporte y mantenimiento al equipamiento de seguridad firewall checkpoint”**, con la empresa **GRUPO ELECTRODATA S.A.C** por un período de noventa (90) días calendario o hasta que se inicie la ejecución del nuevo contrato proveniente del Concurso Público N° 002-2020-OEFA, contados a partir del 06 de julio de 2020 por un monto de S/. 438,705.07, tanto para la prestación principal como la prestación accesoria.

El **31 de agosto de 2020**, mediante el contrato N° 038-2020-OEFA derivado del concurso público N° 002- 2020-OEFA – Primera Convocatoria, se realizó la contratación del – **“Servicio de soporte y mantenimiento al equipamiento de seguridad firewall checkpoint o**

equivalente” incluyó nuevos equipos, con la empresa **GRUPO ELECTRODATA S.A.C** por un periodo de setecientos treinta (730) días calendario, contabilizados a partir del día calendario siguiente de finalizado el contrato vigente, por un monto de S/. 3,233,339.00, tanto para la prestación principal como la prestación accesoria.

Modelo	Uso	Fin de soporte de fábrica ¹
15600 Appliance – R81.10	Lima	Diciembre 2025
Serie 1500 – R81.10	Provincia	Julio 2026

El **14 de junio de 2022**, mediante el contrato N° 018-2022-OEFA derivado del concurso público N° 018- 2022-OEFA – Primera Convocatoria, se realizó la contratación del – **“Servicio de soporte y mantenimiento al equipamiento de seguridad firewall checkpoint o equivalente”**, con la empresa **GRUPO ELECTRODATA S.A.C** por un periodo de mil noventa y cinco (1095) días calendario, contabilizados a partir del día calendario siguiente de finalizado el contrato vigente, por un monto de S/. 3,297,505.80, tanto para la prestación principal como la prestación accesoria.

Asimismo, en la actualidad existen **soluciones integrales para la seguridad perimetral** necesarias para el OEFA:

- **Equipos firewall:** Monitorea y filtra a través de políticas de seguridad el tráfico de red entrante y saliente, permitiendo ser una barrera que se encuentra entre la red interna privada del OEFA y la internet pública que permita la entrada de tráfico no amenazante y mantener fuera el tráfico peligroso.
- **Detección y prevención contra amenazas (XDR):** Analiza los datos de diferentes herramientas de seguridad permitiendo detectar/identificar rápidamente las amenazas y responder a los incidentes con mayor eficacia.
- **Protección de las aplicaciones (WAF):** Protege las aplicaciones web filtrando, vigilando y bloqueando todo el tráfico HTTP/S malicioso que se dirija hacia ellas e impide que salga de ellas cualquier dato no autorizado.
- **Protección de las herramientas de colaboración y correo electrónico en la nube:** Protege las amenazas sofisticadas, como el phishing y el ransomware para al correo electrónico, las aplicaciones de colaboración, los navegadores.

Por ello, es necesario contratar un **SERVICIO DE SOLUCIÓN INTEGRAL DE SEGURIDAD PERIMETRAL PARA EL OEFA**, con el objetivo de minimizar los riesgos asociados a la intrusión no autorizada, el secuestro de información y otras amenazas externas, como los ciberataques.

5. OBJETIVO DE LA CONTRATACIÓN

- ✓ Asegurar la continuidad y disponibilidad operativa de los servicios que brinda el OEFA a nivel nacional

6. OBJETIVO ESPECIFICO

- ✓ Controlar el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas.
- ✓ Proteger de forma automatizada las aplicaciones web y API.
- ✓ Brindar solución de seguridad para el correo electrónico institucional la nube².
- ✓ Brindar solución de inteligencia de amenazas.
- ✓ Monitorear y correlacionar eventos de seguridad.

¹ <https://www.checkpoint.com/support-services/support-life-cycle-policy/>

² Contrato N° 13-2023-OEFA – Servicio de suscripción del software de mensajería electrónica Google Workspace Enterprise Estándar o equivalente, vigente hasta el 15 de junio de 2026.

7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO

Mediante el presente **SERVICIO DE SOLUCIÓN INTEGRAL DE SEGURIDAD PERIMETRAL PARA EL OEFA** se requiere garantizar el adecuado funcionamiento y gestión de los equipos de seguridad, **los cuales pasamos a detallar en el Tabla 02:**

Tabla 02: Resumen

DESARROLLO DEL SERVICIO			Medida	
			Bien	Servicio
	PRESTACIÓN PRINCIPAL			
7.1	SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALLS			
	7.1.1	Solución de Seguridad Next Generation Firewall Tipo I	4	-
	7.1.2	Solución de Seguridad Next Generation Firewall Tipo II	2	-
	7.1.3	Solución de Seguridad Next Generation Firewall Tipo III	2	-
	7.1.4	Solución de Seguridad Next Generation Firewall Tipo IV	31	-
	7.1.5	Consola de Administración de Firewalls	-	1
	7.1.6	Correlación de Eventos, Logs y Reportes de Firewalls	-	1
7.2	SOLUCIÓN DE FIREWALL DE APLICACIONES WEB - WAF			
	7.2.1	Características Generales	-	1
	7.2.2	Funcionalidades para la seguridad WEB		
	7.2.3	Funcionalidades para la seguridad de archivos (File Security o Antimalware)		
	7.2.4	Funcionalidades para la seguridad de API		
	7.2.5	Funcionalidades para la protección Anti-bot		
	7.2.6	Gestión Certificados SSL/TLS		
	7.2.7	Configuración e implementación		
7.3	SOLUCIÓN DE SEGURIDAD DE NUBE GOOGLE WORKSPACE			
	7.3.1	Requerimientos generales de la solución requerida	-	1
	7.3.2	Funcionalidades generales requeridas de la solución de seguridad para Google Workspace		
	7.3.3	Capacidades requeridas de prevención de malware y phishing en Google Workspace		
	7.3.4	Capacidades requeridas de detección de comportamiento anómalo para identificar robo o compromiso de cuentas en Google Workspace		
	7.3.5	Compromiso de Partner y uso de aplicaciones terceras		
	7.3.6	Prevención de Fuga de Información – DLP		
	7.3.7	Consola de Administración		
	7.3.8	Implementación		
7.4	SOLUCIÓN DE INTELIGENCIA DE AMENAZAS Y AUTOMATIZACIÓN			
	7.4.1	Requerimientos generales de la solución requerida	-	1
	7.4.2	Implementación		
	PRESTACIÓN ACCESORIA			
7.5	SERVICIO DE CYBERSOC			1
	7.5.1.	Servicio de Monitoreo y correlación de Eventos de seguridad		
	7.5.2.	Servicio de Detección y Prevención de Ciberataques		
	7.5.3.	Servicio de Soporte a Incidentes		
7.6	SERVICIO GESTIONADO PROACTIVO			1
7.7	NIVELES DE SERVICIO (SLA)			1

A continuación, se detallan las características técnicas que deben cumplir cada uno de los componentes de la solución de seguridad:-

➤ PRESTACIÓN PRINCIPAL

7.1. SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALLS

- El fabricante de la solución de seguridad debe estar presente en los últimos 08 reportes de Gartner (Magic Quadrant), en el cuadrante de Líderes para Network Enterprise Firewalls.

- b) El fabricante de la solución de seguridad debe tener un porcentaje igual o superior al 96% de ratio de protección, en la última evaluación de Enterprise Firewall Report de CyberRatings para el año 2024.

7.1.1. SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALL TIPO I:

- a) Cantidad: 04 appliance
- b) Tamaño: Altura máxima de 01 RU, para ser instalado en bandeja para gabinete de 19"
- c) Rendimiento (throughput) en prevención de amenazas de 16 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, URL Filtering (opcional), IPS, Antivirus y/o Antimalware, DNS Security y Emulación Malware día-cero con log habilitado.
- d) Rendimiento (throughput) en NGFW de 50 Gbps (medido con Capacidades habilitadas de: Firewall y Control de Aplicaciones.
- e) Conexiones Concurrentes: 28'000,000 sesiones o conexiones concurrentes, o 5'000,000 de sesiones o conexiones concurrentes en caso se analice a través de transacciones HTTP.
- f) Conexiones por segundo: 530,000 conexiones o sesiones por segundo, o 270,000 de conexiones o sesiones por segundo en caso se analice a través de transacciones HTTP.
- g) 02 Fuentes redundantes.
- h) Interfaces:
 - a. 08 puertos de red 1GB (RJ45)
 - b. 04 puerto de red 10G SFP+ (inc. Transceivers 10G Base-SR).
 - c. 01 puerto de Sincronización
 - d. 01 puerto de Gestión RJ45
 - e. 01 puerto de consola tipo: USB Type-C o Micro USB
 - f. 01 puerto USB

7.1.1.1. Consideraciones Generales

- c) El sistema operativo deberá ser del fabricante de la solución de firewall ofertado, el mismo deberá venir de fábrica con el "hardening" necesario para no tener componentes y/o configuraciones que puedan causar vulnerabilidades.
- d) En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan publicado y/o anunciado el "End-of-life" y/o "End-of-Support", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos. Este requerimiento deberá ser respaldado con una carta del fabricante adjuntando la documentación publica de Internet que la respalde.
- e) Las versiones de sistema operativo y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) altas o críticas (acumuladas entre sus diferentes versiones) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas.
- f) La solución de seguridad debe soportar la configuración de clúster en modo de operación en alta disponibilidad (HA).
- g) Debe soportar redundancia de enlaces WAN o de ISP (Internet Service Provider) redundantes, sin la necesidad de una licencia adicional o software/hardware de terceros.
- h) La redundancia de ISP emplea la detección de falla enlace para conmutación automática.
- i) Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster.
- j) Administración accesible a través de SSH y de interfaz Web segura (HTTPS).
- k) La herramienta debe ser capaz de realizar backup/restore de la configuración, permitiendo al administrador programar la realización de los backups en periodos diario, semanal y mensual.
- l) Los backups pueden ser generados transferidos vía SFTP, SCP, FTP y localmente. El backup debe tener capacidad de ser cifrado.

- m) La comunicación entre la consola de gestión y los equipos de seguridad (firewall), debe ser cifrada y autenticada.

7.1.1.2. Funcionalidades de Red

- a) La solución debe ser capaz de operar en modalidad Layer 3 (routing), modalidad in-line (bridge) y L2 (port mirroring y/o monitor mode).
- b) Deben soportar inspección del tráfico cifrado (SSL/HTTPS).
- c) Debe soportar enrutamiento con IPv4 e IPv6.
- d) Debe soportar DHCP en modos: Servidor DHCP y DHCP Relay (reenvío) en IPv4 e IPv6.
- e) Debe contar con un módulo de control QoS basado en prioridades y pesos para el control de: porcentaje del ancho de banda disponible, basado en prioridad de regla, ancho de banda mínimo garantizado y ancho de banda máximo, basado en límites.
- f) Debe contar con un módulo de control QoS garantizar el ancho de banda y controlar la latencia para aplicaciones de transmisión, como son Voz sobre IP (VoIP) y videoconferencia.
- g) Soporte de rutas estáticas, IPSec Routing, RIP, OSPFv2 y OSPFv3(IPv6), IGMP, PIM SM, PIM DM PIM SSM, BGP, EBGP Multihop y IPv6 BGP-4.
- h) Soporte de PBR (policy based routing) que permite ante la presencia de dos o más enlaces, se pueda decidir por que enlace ingresa y egresa un tráfico determinado.
- i) Debe soportar redundancia de hasta 03 enlaces de distintos proveedores ISP (Internet Service Provider) redundantes, sin la necesidad de una licencia adicional o software/hardware de terceros.
- j) La redundancia de ISP puede ser a nivel de "compartición de carga" (load sharing) y detección de falla enlace (primary/backup).
- k) Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster.
- l) La solución debe soportar registro de tablas ARP estáticas y dinámicas, definiendo cantidad de entradas ARP y el tiempo de duración.

7.1.1.3. Gestión de Políticas

- a) El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como: Redes y Grupos de Redes, Host, Zonas, Objetos Dinámicos, Dominios FQDN, Usuarios, Grupos de Usuarios, Clientes Remotos VPN, Servicios y Aplicaciones Web y Comunidad de VPN.
- b) Sobre la base de las políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Drop, Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final.
- c) Las reglas deben permitir manejo de ancho de banda de distintos protocolos y aplicaciones web, permitiendo la limitación del uso ancho de banda, tanto para carga (upload) y descarga (download) por cada regla.
- d) Debe poder analizar la utilización de las reglas, con niveles de indicador: muy alto, alto, medio, bajo y cero, este último indicador permitirá identificar que dicha regla no ha tenido conexiones (sin uso). El uso también debe poder identificarse numéricamente en miles, millones, gigas y teras de hits por regla. El contador de uso de la regla podrá configurarse en ventanas de tiempo de: día, semana, mes y total.
- e) Las reglas de firewall deben poder establecer vigencia en base a objetos de tiempo, basado en periodos: diario, semanal, mensual y tener un horario de recurrencia en la cual la regla está vigente.
- f) Capacidad de crear reglas de firewall en base fuentes dinámicas externas, los cuales serán basados en fuentes de URL externas (HTTP/HTTPS) que contengan archivos planos (CSV) y JSON. En el caso de archivos planos se debe poder el tipo de dato y los delimitadores. En caso de JSON debe emplear la sintaxis JQ.
- g) Las fuentes externas deben ser consultadas automáticamente por el firewall, con la finalidad de automatizar las reglas de acceso, no siendo necesario instalar reglas en el firewall.
- h) Las reglas de firewall en base fuentes dinámicas externas deben soportar como mínimo Dirección IP, Rango de Red, IP y mascara de red y dominio FQDN. Estas fuentes deberán ser efectivas en reglas de acceso tanto en origen como destino.

- i) En el caso de navegación en internet, debe tener capacidad de crear políticas con acciones de interacción al usuario final, tales como:
 - Preguntar al usuario si desea continuar o no, y deben indicar una razón para continuar.
 - Informar al usuario, ellos pueden continuar a la aplicación o cancelar el requerimiento.
 - Bloquear indicando al usuario final un mensaje de bloque a la aplicación.
- j) Los mensajes de bloqueo e interacción con el usuario final deben ser editables en idioma y contenido.
- k) Soportar la creación de políticas basada en Geolocalización, configurando que el tráfico de determinado País y/o Países sean bloqueados o permitidos.
- l) Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
- m) Debe posibilitar la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.
- n) Las actualizaciones de las direcciones o rangos de IP publica por cada país, debe realizarse periódicamente y de manera automática.
- o) Debe tener capacidad de controlar el tipo de contenido para el tráfico entrante y saliente.
- p) El control se debe realizar por tipo de dato en tránsito, por lo menos de dos maneras: mediante el tipo de contenido, clasificado analizando el contenido del archivo, y mediante el tipo de archivo, analizando el ID o metadato del archivo.
Los formatos de tipo de archivo a restringir deben ser como mínimo: PDF, Ejecutables (EXE, COM, DLL, DRV, SCR, VBX, SYS), Microsoft (Power Point, Excel, Word), archivos comprimidos (ZIP, 7Z, RAR, TAR, GZIP) y Bases de Datos (Microsoft Access, DB y DBF).

7.1.1.4. Prevención de Intrusos – IPS

- a) La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad.
- b) El IPS debe contar con mecanismo de detección de amenazas de múltiples métodos: detección por firmas, validación de protocolo, detección anómala y análisis de comportamiento.
- c) El IPS debe contar con motor de identificación de patrones, que le permita diferenciar entre paquetes inofensivos y paquetes maliciosos, detectando expresiones regulares en los flujos de como un segundo nivel de análisis, para reducir la tasa de falsos positivos.
- d) El IPS debe poder detectar evasiones en la retransmisión de paquetes o el envío de paquetes maliciosos en la retransmisión, proveyendo capacidad de reensamblaje de flujo para conexiones TCP y reordenamiento de paquetes.
- e) Debe tener protección contra ataques de DoS (Denial of Service).
- f) Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en objetos de red o mediante las reglas de seguridad configuradas.
- g) Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP, SMTP, DNS, POP e IMAP,
- h) Las políticas de protección de IPS deben poder establecerse en base a parámetros tales como: número del CVE, nivel de severidad y nivel de efectividad (confianza).
- i) Debe permitir adicionar excepciones a las protecciones de IPS desde el log o de manera manual.
- j) Debe poder capturar paquetes de eventos de IPS, para proveer un análisis posterior.

7.1.1.5. Anti-Bot y/o Antispyware

- a) La solución debe proveer una herramienta que haga descubrimiento de “bots” dentro de la red. Dicha herramienta debe bloquear la comunicación que intenten establecer los equipos infectados “bots” hacia las redes de los atacantes en Internet (botnet).
- b) La solución debe incluir al menos los siguientes métodos de identificación:
 - Identificación de direcciones web de Comando y Control utilizadas por los criminales para controlar los bots.
 - Identificación de patrones (fingerprints) de comunicación utilizada por cada familia de bots.
 - Identificación de comportamiento de bots.

- c) La solución debe contar con un repositorio en la nube del propio fabricante para la identificación de direcciones y patrones de comunicación de “botnet”. El Anti-Bot se debe actualizar continuamente de manera automática.
- d) La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de direcciones IP, URL y recursos DNS no identificados y/o no clasificados.
- e) La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA) y DNS Tunneling, empleando protección basada en Machine Learning. Estas funcionalidades deben emplear las fuentes de inteligencia de amenazas en nube del propio fabricante.
- f) La solución debe tener una capa de protección DNS para ataques del tipo Non-Existent Domain (NXNS) Attack y también protección de protocolo DNS sobre HTTPS (DoH).
- g) La solución debe contar con análisis la reputación de direcciones URL, direcciones IP y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C)

7.1.1.6. Control de Aplicaciones y URL Filtering

- a) La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web.
- b) Se requiere que capacidad de detección de 4,000 aplicaciones en la base de datos de control de aplicaciones para la aplicación de políticas.
- c) La base de datos de control de aplicaciones debe actualizarse por un servicio basado en la nube, la actualización debe ser periódica y automática.
- d) Debe permitir la creación de firmas personalizadas para el Control de Aplicaciones y URL Filtering, mediante herramientas del propio del fabricante.
- e) Debe alertar al usuario cuando una aplicación o página web fuera bloqueada.
- f) Solución debe soportar como mínimo 70 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, Botnets y/o Command and Control, Anonymizer, Hacking y Spyware/ Malicious Sites.
- g) Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.
- h) Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales (usuarios) y grupos de usuarios.
- i) La solución debe categorizar las aplicaciones y URLs por factor de riesgo.
- j) Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario.
- k) Solución debe inspeccionar el tráfico web cifrado (SSL/TLS) de los usuarios, y permitir excepciones granulares de inspección para proteger la privacidad de los usuarios y/o cumplir con regulaciones.
- l) Debe permitir la categorización de los sitios HTTPS basado en el contenido del campo SNI (Server Name Indication), sin la necesidad de descifrar el tráfico web.
- m) Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y HTTP/2.
- n) Debe soportar la inspección de tráfico HTTPS sobre puertos no estándar (distinto a los puertos HTTP/HTTPS).

7.1.1.7. Prevención de Amenazas

- a) Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en el repositorio la clasificación y/o reputación de direcciones IP, Dominios, URL, redes de Comando y Control y ataques DoS.
- b) Debe tener capacidad de clasificación y análisis de archivos y posterior validación en el repositorio de inteligencia de amenazas en nube del propio fabricante, sin generar un impacto en el rendimiento de la red.
- c) Los equipos deben tener integrada la detección y prevención de virus y amenazas (antimalware).
- d) La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.

- e) Debe tener capacidad de protección de pre-infección del malware que fue identificado en los archivos.
- f) Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), Mail (SMTP o POP3), SMB y FTP.
- g) Debe tener una base de datos local de firmas de malware y cache de reputación de URL, para una respuesta rápida. Si una URL no está ubicada en la cache, debe ser consultada automáticamente en el repositorio de Inteligencia de amenazas en nube para su clasificación y prevención.
- h) Debe soportar Inspección de tráfico cifrado/encryptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).
- i) Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware.
- j) Debe tener capacidades de inspección y prevención de amenaza en el canal cifrado SSH, con las siguientes capacidades:
 - Bloquear ataques en canal SSH.
 - Bloquea la transmisión de virus a través de los protocolos SCP y SFTP.
 - Prevenir el descifrado de contraseñas en fuerza bruta de servidores SSH/SFTP.
- k) Debe soportar para la alimentación de IoC (Indicadores de Compromiso) desde fuentes externas, en formato CSV y STIX XML (Structured Threat Information Expression) para la prevención de amenazas.
- l) Los IoC deben ser actualizados automáticamente de acuerdo con un intervalo definido en la consola.
- m) Los IoC definidos en las fuentes externas deberán poder ser como mínimo: URL, Dominio, IP, Rango de IP, Hash (MD5, SHA1, SHA256) y campos de correo (Mail From, To, CC, Subject).

7.1.1.8. Prevención de Amenazas Desconocidas o de Día Cero

- a) La solución debe ser capaz de identificar y prevenir ataques y malware no conocido, presentes en documentos y/o archivos ejecutables.
- b) La solución debe ser capaz de emular los archivos identificados en el firewall de forma automática, a través del envío y posterior análisis en la nube del propio fabricante de la solución de firewall para la Emulación de Malware (SandBox). La nube de emulación de amenazas del fabricante debe tener certificación SOC2 Tipo II.
- c) La solución debe proteger a los usuarios internos, de manera que prevenga el acceso o descarga a los archivos en tanto estos son analizados en el equipo de emulación, si el archivo en benigno se entrega el archivo original al usuario y si el archivo el maligno se deniega su acceso o descarga.
- d) La solución debe proporcionar la capacidad de protección contra ataques de malware desconocido y de día cero antes de que se hayan creado protecciones de firmas estáticas.
- e) La solución debe proveer prevención en tiempo real de malware desconocido en las descargas web y canal de correo electrónico.
- f) La solución deberá poder emular archivos para la identificación de malware que viajan en los protocolos: HTTP, HTTPS, SMTP, IMAP, CIFS, SMBv3, SMBv3 multi-channel y FTP.
- g) La solución deberá poder emular al menos los siguientes tipos de archivos: Adobe PDF, Microsoft Office (documentos y plantillas), DLL, Java, Flash, Scripts, archivos comprimidos (ZIP, 7Z, RAR, GZ, TGZ, TAR, TAR.GZ y JAR), ejecutables (EXE, COM, LNK, DLL, DRV, SYS, SCR, VBX) y archivos de MacOS (APP, DMG, PKG).
- h) El motor de emulación debe detectar llamadas API, cambios en el sistema de archivos, cambios en el registro, conexiones de red, procesos de sistema.
- i) El motor de emulación debe analizar y emular los URL contenidos en documentos Microsoft Office y PDF, para detectar y prevenir descargas maliciosas de malware.
- j) El motor de emulación debe emplear mecanismos de Machine Learning para detectar y prevenir ataques ocultos sobre archivos LNK (accesos directos) tales como: Icon Spoofing, File Attribute Manipulation, Shortened URLs.

- k) El motor de emulación debe contar con tecnologías de ML basadas en Redes Neuronales (Neural Networks) para la detección de amenazas en los archivos Microsoft Office y PDF.
- l) Las soluciones deben admitir motores de detección automatizados basados en machine learning.
- m) La solución debe ser capaz de soportar escaneo de enlaces (links) dentro de correos para detección de malware.
- n) La solución debe ser resistente a los casos en los que el código de shell o el malware no se ejecutarían si detectaran la existencia de un entorno virtual.

7.1.1.9. VPN IPSec

- a) Debe soportar por lo menos 2,000 túneles VPN Client-to-Site IPSec y SSL.
- b) Debe soportar túneles VPN punto a punto Site-to-Site de manera ilimitada o hasta la máxima capacidad soportada por el equipamiento.
- c) Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- d) Deben soportar encriptación AES-128 y AES-256 para las fases I y II de IKE.
- e) Deben soportar integridad en MD5, SHA1, SHA-256, SHA-512, AES-XCBC para las fases I y II de IKE.
- f) Debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit), Grupo 19 (256-bit ECP) y Grupo 20 (384-bit ECP) para las fases I y II de IKE.
- g) Debe poder integrarse con Directorio Activo Microsoft para crear reglas de control de acceso a través de VPN, empleando: usuarios, grupos de usuarios, maquinas, dirección IP y redes.
- h) Debe poder integrarse con Azure AD (Microsoft) mediante SAML para autenticación en el acceso remoto de clientes VPN.
- i) El cliente VPN, debe instalarse sobre sistemas operativos Windows, Linux y MacO

7.1.1.10. Identificación de Usuarios

- a) La solución debe proveer diferentes métodos para obtener las identidades de los usuarios, tales como:
 - Sin agente, haciendo búsquedas al Directorio Activo Microsoft.
 - Con agente implementado en los servidores de Directorio Activo Microsoft.
 - Empleando un Portal Cautivo.
 - Empleando un Proveedor de Identidad (IdP) basado en SAML
- b) La solución debe soportar el uso del protocolo WMI (Windows management instrumentation).
- c) La solución debe soportar el uso del protocolo Kerberos (Transparent Kerberos Authentication).
- d) Debe proveer un "Portal Cautivo", para autenticar a los usuarios que no están dentro del Directorio Activo, los usuarios que no tienen plataforma Windows y/o los usuarios invitados.
- e) Cuando se detecte que los usuarios no se han autenticado, la solución tiene que redireccionarlos a un Portal Cautivo, a través del protocolo HTTP.
- f) Debe soportar al menos los siguientes métodos de autenticación: nombre de usuario y contraseña, que podrá ser configurado en la base de datos Interna del equipo, servidor de LDAP.
- g) La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall.

7.1.1.11. Instalación y configuración:

- a) La migración deberá realizarse en horario fuera de oficina, sin que estas acciones afecten el normal funcionamiento de los sistemas y accesos a los recursos informáticos, teniendo una ventana de tiempo de 12 horas por cada día de trabajo de migración, en coordinación con la oficina de tecnologías de información de las OEFA.
- b) Asegurar la compatibilidad y funcionamiento de los servicios migrados en la nueva solución.

- c) El contratista deberá configurar el equipo de seguridad perimetral para que realice backups automáticos, los cuales serán almacenados en un servidor que será brindado por la OTI.
- d) El especialista de la solución por parte del postor ganador debe garantizar que la solución ofertada cuenta con el sistema operativo actualizado con la última versión estable y recomendada por la marca al momento de la instalación y configuración.
- e) El contratista será responsable del correcto funcionamiento de todas las políticas implementadas para que los servicios publicados no se vean afectados
- f) La implementación de la nueva solución de seguridad perimetral debe ser transparente, de tal manera que conserve los permisos a nivel de usuario y no afecte a las aplicaciones.
- g) La implementación y puesta en producción de la solución requerida deberá contemplar las buenas prácticas en diseño de redes y esquemas lógicos de configuración, según la marca ofertada.
- h) El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo, Activando las capacidades de seguridad incluidas en cada equipo, de manera que se utilice satisfactoriamente el licenciamiento adquirido.
- i) Realizar el desmontaje de los equipos actuales de seguridad Checkpoint
- j) Rackeo, implementación y configuración de la solución ofertada en el centro de procesamiento de datos de OEFA.
- k) Realizar actividades de configuración, las cuales consisten en:
 - a. Configuración por zonas. (permitirá crear una sólida política de control de acceso que controla el tráfico entre partes de la red)
 - b. Habilitar la alta disponibilidad (en los equipos que lo permitan).
 - c. Remoción de objetos redundantes o que estén duplicados.
 - d. Remoción de reglas redundantes o que estén duplicadas.
 - e. Optimización de tablas de enrutamiento.
 - f. Revisar la configuración de NAT y reducir la cantidad de reglas (de ser necesario).
 - g. Activar la configuración de logs de la solución.
 - h. Realizar pruebas de funcionalidad sobre la instalación y configuración de la solución ofertada.
 - i. Realizar pruebas de alta disponibilidad de la solución ofertada.
 - j. Migrar la configuración actual del equipamiento existente que será reemplazado, según el siguiente detalle.

OBJETO	TIPO DE OBJETO	CANTIDAD
	Limitacion de Navegacion	16
Objeto Network	Address Ranges	7
	Domains	78
	Dynamic Objects	6
	Gateways and Servers	5
	Groups	81
	Host	1116
	Interoperable Devices	18
	Networks	120
	Security Zones	3
Server	Radius	1
	Trusted CA	1
Services		
	CITRIX TCP	1
	Compound TCP	4
	GTP	4
	Other Services	26
	Grupo de Servicio	56
	TCP	261
	UDP	105

OBJETO	TIPO DE OBJETO	CANTIDAD
User-Identities	Access Roles	172
	LDAP Account Units	10
	LDAP Groups	10
	User Groups	13
	Users	147
	User Templates	10
VPN	VPN Communities	18

7.1.2. SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALL TIPO II

- Cantidad: 02 appliance
- Tamaño: Altura máxima de 01 RU, para ser instalado en bandeja para gabinete de 19"
- Rendimiento (throughput) en prevención de amenazas de 16 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, URL Filtering (opcional), IPS, Antivirus y/o Antimalware, DNS Security y Emulación Malware día-cero con log habilitado.
- Rendimiento (throughput) en NGFW de 50 Gbps (medido con Capacidades habilitadas de: Firewall y Control de Aplicaciones.
- Conexiones Concurrentes: 28'000,000 sesiones o conexiones concurrentes, o 5'000,000 de sesiones o conexiones concurrentes en caso se analice a través de transacciones HTTP.
- Conexiones por segundo: 530,000 conexiones o sesiones por segundo, o 270,000 de conexiones o sesiones por segundo en caso se analice a través de transacciones HTTP.
- 02 Fuentes redundantes.
- Interfaces:
 - 08 puertos de red 1GB (RJ45)
 - 04 puerto de red 10G SFP+ (inc. Transeivers 10G Base-SR).
 - 01 puerto de Sincronización
 - 01 puerto de Gestión RJ45
 - 01 puerto de consola tipo: USB Type-C o Micro USB
 - 01 puerto USB

7.1.2.1. Consideraciones Generales

- El sistema operativo deberá ser del fabricante de la solución de firewall ofertado, el mismo deberá venir de fábrica con el "hardening" necesario para no tener componentes y/o configuraciones que puedan causar vulnerabilidades.
- En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan publicado y/o anunciado el "End-of-life" y/o "End-of-Support", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos. Este requerimiento deberá ser respaldado con una carta del fabricante adjuntando la documentación publica de Internet que la respalde.
- Las versiones de sistema operativo y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) altas o críticas (acumuladas entre sus diferentes versiones) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas. Este requerimiento deberá ser sustentando con documentación publica en Internet del fabricante.
- La solución de seguridad debe soportar la configuración de clúster en modo de operación en alta disponibilidad (HA).
- Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster.
- Administración accesible a través de SSH y de interfaz Web segura (HTTPS).
- La herramienta debe ser capaz de realizar backup/restore de la configuración, permitiendo al administrador programar la realización de los backups en periodos diario, semanal y mensual.

- h) Los backups pueden ser generados transferidos vía SFTP, SCP, FTP y localmente. El backup debe tener capacidad de ser cifrado.
- i) La comunicación entre la consola de gestión y los equipos de seguridad (firewall), debe ser cifrada y autenticada.

7.1.2.2. Funcionalidades de Red

- a) La solución debe ser capaz de operar en modalidad Layer 3 (routing), modalidad in-line (bridge) y L2 (port mirroring y/o monitor mode).
- b) Deben soportar inspección del tráfico cifrado (SSL/HTTPS).
- c) Debe soportar enrutamiento con IPv4 e IPv6.
- d) Debe soportar DHCP en modos: Servidor DHCP y DHCP Relay (reenvío) en IPv4 e IPv6.
- e) Debe contar con un módulo de control QoS basado en prioridades y pesos para el control de: porcentaje del ancho de banda disponible, basado en prioridad de regla, ancho de banda mínimo garantizado y ancho de banda máximo, basado en límites.
- f) Debe contar con un módulo de control QoS garantizar el ancho de banda y controlar la latencia para aplicaciones de transmisión, como son Voz sobre IP (VoIP) y videoconferencia.
- g) Soporte de rutas estáticas, IPSec Routing, RIP, OSPFv2 y OSPFv3(IPv6), IGMP, PIM SM, PIM DM PIM SSM, BGP, EBGP Multihop y IPv6 BGP-4.
- h) Soporte de PBR (policy based routing) que permite ante la presencia de dos o más enlaces, se pueda decidir por que enlace ingresa y egresa un tráfico determinado.
- i) Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster.
- j) La solución debe soportar registro de tablas ARP estáticas y dinámicas, definiendo cantidad de entradas ARP y el tiempo de duración

7.1.2.3. Gestión de Políticas

- a) El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como: Redes y Grupos de Redes, Host, Zonas, Objetos Dinámicos, Dominios FQDN, Usuarios, Grupos de Usuarios, Clientes Remotos VPN, Servicios y Aplicaciones Web y Comunidad de VPN.
- b) Sobre la base de las políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Drop, Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final.
- c) Las reglas deben permitir manejo de ancho de banda de distintos protocolos y aplicaciones web, permitiendo la limitación del uso ancho de banda, tanto para carga (upload) y descarga (download) por cada regla.
- d) Debe poder analizar la utilización de las reglas, con niveles de indicador: muy alto, alto, medio, bajo y cero, este último indicador permitirá identificar que dicha regla no ha tenido conexiones (sin uso). El uso también debe poder identificarse numéricamente en miles, millones, gigas y teras de hits por regla. El contador de uso de la regla podrá configurarse en ventanas de tiempo de: día, semana, mes y total.
- e) Las reglas de firewall deben poder establecer vigencia en base a objetos de tiempo, basado en periodos: diario, semanal, mensual y tener un horario de recurrencia en la cual la regla está vigente.
- f) Capacidad de crear reglas de firewall en base fuentes dinámicas externas, los cuales serán basados en fuentes de URL externas (HTTP/HTTPS) que contengan archivos planos (CSV) y JSON. En el caso de archivos planos se debe poder el tipo de dato y los delimitadores. En caso de JSON debe emplear la sintaxis JQ.
- g) Las fuentes externas deben ser consultadas automáticamente por el firewall, con la finalidad de automatizar las reglas de acceso, no siendo necesario instalar reglas en el firewall.
- h) Las reglas de firewall en base fuentes dinámicas externas deben soportar como mínimo Dirección IP, Rango de Red, IP y mascara de red y dominio FQDN. Estas fuentes deberán ser efectivas en reglas de acceso tanto en origen como destino.
- i) En el caso de navegación en internet, debe tener capacidad de crear políticas con acciones de interacción al usuario final, tales como:

- Preguntar al usuario si desea continuar o no, y deben indicar una razón para continuar.
 - Informar al usuario, ellos pueden continuar a la aplicación o cancelar el requerimiento.
 - Bloquear indicando al usuario final un mensaje de bloque a la aplicación.
- j) Los mensajes de bloqueo e interacción con el usuario final deben ser editables en idioma y contenido.
- k) Soportar la creación de políticas basada en Geolocalización, configurando que el tráfico de determinado País y/o Países sean bloqueados o permitidos.
- l) Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
- m) Debe posibilitar la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.
- n) Las actualizaciones de las direcciones o rangos de IP publica por cada país, debe realizarse periódicamente y de manera automática.
- o) Debe tener capacidad de controlar el tipo de contenido para el tráfico entrante y saliente.
- p) El control se debe realizar por tipo de dato en tránsito, por lo menos de dos maneras: mediante el tipo de contenido, clasificado analizando el contenido del archivo, y mediante el tipo de archivo, analizando el ID o metadato del archivo.
- q) Los formatos de tipo de archivo a restringir deben ser como mínimo: PDF, Ejecutables (EXE, COM, DLL, DRV, SCR, VBX, SYS), Microsoft (Power Point, Excel, Word), archivos comprimidos (ZIP, 7Z, RAR, TAR, GZIP) y Bases de Datos (Microsoft Access, DB y DBF).

7.1.2.4. Prevención de Intrusos – IPS

- a) La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad.
- b) El IPS debe contar con mecanismo de detección de amenazas de múltiples métodos: detección por firmas, validación de protocolo, detección anómala y análisis de comportamiento.
- c) El IPS debe contar con motor de identificación de patrones, que le permita diferenciar entre paquetes inofensivos y paquetes maliciosos, detectando expresiones regulares en los flujos de como un segundo nivel de análisis, para reducir la tasa de falsos positivos.
- d) El IPS debe poder detectar evasiones en la retransmisión de paquetes o el envío de paquetes maliciosos en la retransmisión, proveyendo capacidad de reensamblaje de flujo para conexiones TCP y reordenamiento de paquetes.
- e) Debe tener protección contra ataques de DoS (Denial of Service).
- f) Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en objetos de red o mediante las reglas de seguridad configuradas.
- g) Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP, SMTP, DNS, POP e IMAP,
- h) Las políticas de protección de IPS deben poder establecerse en base a parámetros tales como: número del CVE, nivel de severidad y nivel de efectividad (confianza).
- i) Debe permitir adicionar excepciones a las protecciones de IPS desde el log o de manera manual.
- j) Debe poder capturar paquetes de eventos de IPS, para proveer un análisis posterior.

7.1.2.5. Control de Aplicaciones

- a) La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web.
- b) Se requiere que capacidad de detección de 4,000 aplicaciones en la base de datos de control de aplicaciones para la aplicación de políticas.
- c) La base de datos de control de aplicaciones debe actualizarse por un servicio basado en la nube, la actualización debe ser periódica y automática.
- d) Debe permitir la creación de firmas personalizadas para el Control de Aplicaciones y/o URL Filtering, mediante herramientas del propio del fabricante.
- e) Debe alertar al usuario cuando una aplicación o página web fuera bloqueada.
- f) Debe ser posible definir nuevas aplicaciones, así como categorías y grupos que no estén definidos dentro de la base de datos.

- g) Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales (usuarios) y grupos de usuarios.
- h) La solución debe categorizar las aplicaciones y/o URLs por factor de riesgo.
- i) Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario.
- j) Solución debe inspeccionar el tráfico web cifrado (SSL/TLS) de los usuarios, y permitir excepciones granulares de inspección para proteger la privacidad de los usuarios y/o cumplir con regulaciones.
- k) Debe permitir la categorización de los sitios HTTPS basado en el contenido del campo SNI (Server Name Indication), sin la necesidad de descifrar el tráfico web.
- l) Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y HTTP/2.
- m) Debe soportar la inspección de tráfico HTTPS sobre puertos no estándar (distinto a los puertos HTTP/HTTPS).

7.1.2.6. Identificación de Usuarios

- a) La solución debe proveer diferentes métodos para obtener las identidades de los usuarios, tales como:
- b) Sin agente, haciendo búsquedas al Directorio Activo Microsoft.
- c) Con agente implementado en los servidores de Directorio Activo Microsoft.
- d) Empleando un Portal Cautivo.
- e) Empleando un Proveedor de Identidad (IdP) basado en SAML
- f) La solución debe soportar el uso del protocolo WMI (Windows management instrumentation).
- g) La solución debe soportar el uso del protocolo Kerberos (Transparent Kerberos Authentication).
- h) Debe proveer un "Portal Cautivo", para autenticar a los usuarios que no están dentro del Directorio Activo, los usuarios que no tienen plataforma Windows y/o los usuarios invitados.
- i) Cuando se detecte que los usuarios no se han autenticado, la solución tiene que redireccionarlos a un Portal Cautivo, a través del protocolo HTTP.
- j) Debe soportar al menos los siguientes métodos de autenticación: nombre de usuario y contraseña, que podrá ser configurado en la base de datos Interna del equipo, servidor de LDAP.
- k) La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall

7.1.2.7. Prevención de Fuga de Información - DLP

- a) La solución debe ser implementado en modalidad in-line (bridge) para las funcionalidades de DLP de red.
- b) Debe contar más mas de 700 tipos de datos (data types) predefinidos.
- c) Debe contar con data types editables o capacidad de crear nuevos data types según la necesidad.
- d) Debe contar con notificaciones configurables en múltiples idiomas.
- e) Deben soportar inspección del tráfico cifrado (SSL/HTTPS) para las políticas de DLP.
- f) Deben soportar inspección del tráfico SMTP, FTP, HTTPS para las políticas de DLP.
- g) Deben soportar inspección basada en patrones (Pattern), keyword matching y diccionarios. La coincidencia de patrones y la clasificación de archivos deben permitir la identificación de tipos de contenido independientemente de la extensión aplicada al archivo o la compresión aplicada al archivo.
- h) Deben soportar inspección basada en los atributos del archivo (File attribute-based matching)
- i) Deben soportar inspección basada en la estructura del contenido (structured content)
- j) Deben soportar el uso de lenguaje de programación abierto para crear tipos de datos específicos, tales como expresiones regulares RegEx.

- k) Debe soportar capacidad avanzada de tipos de datos (data types) con características de sensibilidad entre mayúsculas y minúsculas, proximidad de palabras, múltiples ocurrencias de una palabra y capturar parte o la totalidad de una palabra.
- l) Deben soportar el escaneo (análisis) de repositorio locales compartidos (CIFS y NFS) para realizar protección basada en finger-print.
- m) Deben soportar lista blanca (Whitelist) basado en archivo y repositorios.
- n) Deben soportar incluir marca de agua (watermarks) sea visible o invisible a los documentos de Microsoft Office.
- o) Debe cuarentenar archivos y enviar una notificación sobre las posibles brechas de seguridad al propietario de la información.
- p) Las reglas de firewall deben poder tener limitantes y/o vigencia en base a tiempo o determinado período (día, mes, año, día de la semana y hora) para las políticas de DLP.
- q) Las opciones de acción para las políticas de DLP deben ser por lo menos las siguientes cuando se coincida con una regla de seguridad:
 - a. Informar al usuario (deja pasar información, pero notifica)
 - b. Pregunta al usuario (información se retienen, a notificación es enviada al usuario final para que decida liberar o no la información retenida)
 - c. Previene, la transmisión de información es bloqueada.
 - d. Marca de agua (watermarks) a los archivos de Microsoft Office (Word, Excel, Power Point), sea esta visible en el documento, o invisible (encriptada)
- r) Las opciones de seguimiento o notificación para las políticas de DLP deben ser por lo menos las siguientes cuando se coincida con una regla de seguridad:
 - a. Enviar un email
 - b. Registrar (log)
 - c. Enviar un SNMP Trap
 - d. Guardar el Incidente con la data incluida
- s) Cuando se coincida con una regla DLP y se guarde el incidente, en el caso de tráfico Web, el texto que coincido con la regla DLP debe ser almacenado, así como el archivo que intento subir (upload) a la página web, debe ser almacenado.

7.1.2.8. Instalación y configuración:

- a) La migración deberá realizarse en horario fuera de oficina, sin que estas acciones afecten el normal funcionamiento de los sistemas y accesos a los recursos informáticos, teniendo una ventana de tiempo de 12 horas por cada día de trabajo de migración, en coordinación con la oficina de tecnologías de información de las OEFA.
- b) Asegurar la compatibilidad y funcionamiento de los servicios migrados en la nueva solución
- c) El contratista deberá configurar el equipo de seguridad perimetral para que realice backups automáticos, los cuales serán almacenados en un servidor que será brindado por la OTI.
- d) El especialista de la solución por parte del postor ganador debe garantizar que la solución ofertada cuenta con el sistema operativo actualizado con la última versión estable y recomendada por la marca al momento de la instalación y configuración.
- e) El contratista será responsable del correcto funcionamiento de todas las políticas implementadas para que los servicios publicados no se vean afectados
- f) La implementación de la nueva solución de seguridad perimetral debe ser transparente, de tal manera que conserve los permisos a nivel de usuario y no afecte a las aplicaciones.
- g) La implementación y puesta en producción de la solución requerida deberá contemplar las buenas prácticas en diseño de redes y esquemas lógicos de configuración, según la marca ofertada.
- h) El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo, Activando las capacidades de seguridad incluidas en cada equipo, de manera que se utilice satisfactoriamente el licenciamiento adquirido.
- i) Realizar el desmontaje de los equipos actuales de seguridad Checkpoint
- j) Rackeo, implementación y configuración de la solución ofertada en el centro de procesamiento de datos de OEFA.
- k) La configuración de la solución debe realizarse de acuerdo con las mejores prácticas de

- la marca.
- l) Realizar la protección sobre los dominios web públicos de OEFA.
 - m) Activar las capacidades de seguridad adquiridas, de manera que se utilice satisfactoriamente el licenciamiento adquirido.
 - n) Integrar la solución requerida al menos con las siguientes capacidades:
 - a. Configurar reglas customizadas.
 - b. Configurar excepciones.
 - c. Activar los modos de operación prevención y/o aprendizaje/detección.
 - d. Habilitar emulación de amenazas no conocidas.
 - e. Subir certificados para poder proteger sitios https de la institución.
 - f. Habilitar el motor de aprendizaje.
 - g. Activación de logs de auditoría.
 - h. Configuración de los reportes automatizados.
 - i. Configuración de las alarmas o notificaciones a los administradores.
 - o) Realizar pruebas de funcionalidad sobre la implementación de la solución ofertada.

7.1.3. SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALL TIPO III:

- a) Cantidad: 02 appliance.
Se debe contar con 01 appliance en modo productivo, y 01 en modo de contingencia o respaldo en sitio ante averías, este último no requiere estar licenciado.
- b) Tamaño: Altura máxima de 01 RU, para ser instalado en bandeja para gabinete de 19"
- c) Rendimiento (throughput) en prevención de amenazas de 09 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, URL Filtering (opcional), IPS, Antivirus, Anti-Bot o Antispyware, DNS Security y Emulación Malware día-cero con log habilitado.
- d) Rendimiento (throughput) en NGFW de 26 Gbps (medido con Capacidades habilitadas de: Firewall y Control de Aplicaciones.
- e) Conexiones Concurrentes: 16'000,000 sesiones o conexiones concurrentes, o 2'500,000 de sesiones o conexiones concurrentes en caso se analice a través de transacciones HTTP.
- f) Conexiones por segundo: 300,000 conexiones o sesiones por segundo, o 230,000 de conexiones o sesiones por segundo en caso se analice a través de transacciones HTTP.
- g) 02 Fuentes redundantes.
- h) Interfaces:
 - a. 08 puertos de red 1GB (RJ45)
 - b. 04 puerto de red 10G SFP+ (inc. Transeivers 10G Base-SR).
 - c. 01 puerto de Sincronización
 - d. 01 puerto de Gestión RJ45
 - e. 01 puerto de consola tipo: USB Type-C o Micro USB
 - f. 01 puerto USB

7.1.3.1. Consideraciones Generales

- a) El sistema operativo deberá ser del fabricante de la solución de firewall ofertado, el mismo deberá venir de fábrica con el "hardening" necesario para no tener componentes y/o configuraciones que puedan causar vulnerabilidades.
- b) En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan publicado y/o anunciado el "End-of-life" y/o "End-of-Support", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos. Esto requerimiento deberá ser respaldado con una carta del fabricante donde se precise la documentación publica de Internet que la respalde.
- c) Las versiones de sistema operativo y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) altas o críticas (acumuladas entre sus diferentes versiones) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas. Esto requerimiento deberá ser sustentando con documentación publica en Internet del fabricante.

- d) La solución de seguridad debe soportar la configuración de clúster en modo de operación en alta disponibilidad (HA).
- e) Debe soportar redundancia de enlaces WAN o de ISP (Internet Service Provider) redundantes, sin la necesidad de una licencia adicional o software/hardware de terceros.
- f) La redundancia de ISP emplea la detección de falla enlace para conmutación automática.
- g) Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster.
- h) Administración accesible a través de SSH y de interfaz Web segura (HTTPS).
- i) La herramienta debe ser capaz de realizar backup/restore de la configuración, permitiendo al administrador programar la realización de los backups en periodos diario, semanal y mensual.
- j) Los backups pueden ser generados transferidos vía SFTP, SCP, FTP y localmente. El backup debe tener capacidad de ser cifrado.
- k) La comunicación entre la consola de gestión y los equipos de seguridad (firewall), debe ser cifrada y autenticada.

7.1.3.2. Funcionalidades de Red

- a) La solución debe ser capaz de operar en modalidad Layer 3 (routing), modalidad in-line (bridge) y L2 (port mirroring y/o monitor mode).
- b) Deben soportar inspección del tráfico cifrado (SSL/HTTPS).
- c) Debe soportar enrutamiento con IPv4 e IPv6.
- d) Debe soportar DHCP en modos: Servidor DHCP y DHCP Relay (reenvío) en IPv4 e IPv6.
- e) Debe contar con un módulo de control QoS basado en prioridades y pesos para el control de: porcentaje del ancho de banda disponible, basado en prioridad de regla, ancho de banda mínimo garantizado y ancho de banda máximo, basado en límites.
- f) Debe contar con un módulo de control QoS garantizar el ancho de banda y controlar la latencia para aplicaciones de transmisión, como son Voz sobre IP (VoIP) y videoconferencia.
- g) Soporte de rutas estáticas, IPSec Routing, RIP, OSPFv2 y OSPFv3(IPv6), IGMP, PIM SM, PIM DM PIM SSM, BGP, EBGp Multihop y IPv6 BGP-4.
- h) Soporte de PBR (policy based routing) que permite ante la presencia de dos o más enlaces, se pueda decidir por que enlace ingresa y egresa un tráfico determinado.
- i) Debe soportar redundancia de hasta 03 enlaces de distintos proveedores ISP (Internet Service Provider) redundantes, sin la necesidad de una licencia adicional o software/hardware de terceros.
- j) La redundancia de ISP puede ser a nivel de “compartición de carga” (load sharing) y detección de falla enlace (primary/backup).
- k) Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster.
- l) La solución debe soportar registro de tablas ARP estáticas y dinámicas, definiendo cantidad de entradas ARP y el tiempo de duración.

7.1.3.3. Gestión de Políticas

- a) El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como: Redes y Grupos de Redes, Host, Zonas, Objetos Dinámicos, Dominios FQDN, Usuarios, Grupos de Usuarios, Clientes Remotos VPN, Servicios y Aplicaciones Web y Comunidad de VPN.
- b) Sobre la base de las políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Drop, Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final.
- c) Las reglas deben permitir manejo de ancho de banda de distintos protocolos y aplicaciones web, permitiendo la limitación del uso ancho de banda, tanto para carga (upload) y descarga (download) por cada regla.
- d) Debe poder analizar la utilización de las reglas, con niveles de indicador: muy alto, alto, medio, bajo y cero, este último indicador permitirá identificar que dicha regla no ha tenido conexiones (sin uso). El uso también debe poder identificarse numéricamente en miles, millones, gigas y teras de hits por regla. El contador de uso de la regla podrá configurarse en ventanas de tiempo de: día, semana, mes y total.

- e) Las reglas de firewall deben poder establecer vigencia en base a objetos de tiempo, basado en periodos: diario, semanal, mensual y tener un horario de recurrencia en la cual la regla está vigente.
- f) Capacidad de crear reglas de firewall en base fuentes dinámicos externas, los cuales serán basados en fuentes de URL externas (HTTP/HTTPS) que contengan archivos planos (CSV) y JSON. En el caso de archivos planos se debe poder el tipo de dato y los delimitadores. En caso de JSON debe emplear la sintaxis JQ.
- g) Las fuentes externas deben ser consultadas automáticamente por el firewall, con la finalidad de automatizar las reglas de acceso, no siendo necesario instalar reglas en el firewall.
- h) Las reglas de firewall en base fuentes dinámicos externas deben soportar como mínimo Dirección IP, Rango de Red, IP y mascara de red y dominio FQDN. Estas fuentes deberán ser efectivas en reglas de acceso tanto en origen como destino.
- i) En el caso de navegación en internet, debe tener capacidad de crear políticas con acciones de interacción al usuario final, tales como:
 - a. Preguntar al usuario si desea continuar o no, y deben indicar una razón para continuar.
 - b. Informar al usuario, ellos pueden continuar a la aplicación o cancelar el requerimiento.
 - c. Bloquear indicando al usuario final un mensaje de bloque a la aplicación.
- j) Los mensajes de bloqueo e interacción con el usuario final deben ser editables en idioma y contenido.
- k) Soportar la creación de políticas basada en Geolocalización, configurando que el tráfico de determinado País y/o Países sean bloqueados o permitidos.
- l) Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
- m) Debe posibilitar la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.
- n) Las actualizaciones de las direcciones o rangos de IP publica por cada país, debe realizarse periódicamente y de manera automática.
- o) Debe tener capacidad de controlar el tipo de contenido para el tráfico entrante y saliente.
- p) El control se debe realizar por tipo de dato en tránsito, por lo menos de dos maneras: mediante el tipo de contenido, clasificado analizando el contenido del archivo, y mediante el tipo de archivo, analizando el ID o metadato del archivo.
- q) Los formatos de tipo de archivo a restringir deben ser como mínimo: PDF, Ejecutables (EXE, COM, DLL, DRV, SCR, VBX, SYS), Microsoft (Power Point, Excel, Word), archivos comprimidos (ZIP, 7Z, RAR, TAR, GZIP) y Bases de Datos (Microsoft Access, DB y DBF)

7.1.3.4. Prevención de Intrusos – IPS

- a) La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad.
- b) El IPS debe contar con mecanismo de detección de amenazas de múltiples métodos: detección por firmas, validación de protocolo, detección anómala y análisis de comportamiento.
- c) El IPS debe contar con motor de identificación de patrones, que le permita diferenciar entre paquetes inofensivos y paquetes maliciosos, detectando expresiones regulares en los flujos de como un segundo nivel de análisis, para reducir la tasa de falsos positivos.
- d) El IPS debe poder detectar evasiones en la retransmisión de paquetes o el envío de paquetes maliciosos en la retransmisión, proveyendo capacidad de reensamblaje de flujo para conexiones TCP y reordenamiento de paquetes.
- e) Debe tener protección contra ataques de DoS (Denial of Service).
- f) Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en objetos de red o mediante las reglas de seguridad configuradas.
- g) Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP, SMTP, DNS, POP e IMAP,
- h) Las políticas de protección de IPS deben poder establecerse en base a parámetros tales como: número del CVE, nivel de severidad y nivel de efectividad (confianza).
- i) Debe permitir adicionar excepciones a las protecciones de IPS desde el log o de manera manual.

- j) Debe poder capturar paquetes de eventos de IPS, para proveer un análisis posterior.

7.1.3.5. Anti-Bot y/o Antispyware

- a) La solución debe proveer una herramienta que haga descubrimiento de “bots” dentro de la red. Dicha herramienta debe bloquear la comunicación que intenten establecer los equipos infectados “bots” hacia las redes de los atacantes en Internet (botnet).
- b) La solución debe incluir al menos los siguientes métodos de identificación:
 - a. Identificación de direcciones web de Comando y Control utilizadas por los criminales para controlar los bots.
 - b. Identificación de patrones (fingerprints) de comunicación utilizada por cada familia de bots.
 - c. Identificación de comportamiento de bots.
- c) La solución debe contar con un repositorio en la nube del propio fabricante para la identificación de direcciones y patrones de comunicación de “botnet”. El Anti-Bot se debe actualizar continuamente de manera automática.
- d) La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de direcciones IP, URL y recursos DNS no identificados y/o no clasificados.
- e) La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA) y DNS Tunneling, empleando protección basada en Machine Learning. Estas funcionalidades deben emplear las fuentes de inteligencia de amenazas en nube del propio fabricante.
- f) La solución debe tener una capa de protección DNS para ataques del tipo Non-Existent Domain (NXNS) Attack y también protección de protocolo DNS sobre HTTPS (DoH).
- g) La solución debe contar con análisis la reputación de direcciones URL, direcciones IP y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).

7.1.3.6. Control de Aplicaciones y URL Filtering

- a) La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web.
- b) Se requiere que capacidad de detección de 4,000 aplicaciones en la base de datos de control de aplicaciones para la aplicación de políticas.
- c) La base de datos de control de aplicaciones debe actualizarse por un servicio basado en la nube, la actualización debe ser periódica y automática.
- d) Debe permitir la creación de firmas personalizadas para el Control de Aplicaciones y URL Filtering, mediante herramientas del propio del fabricante.
- e) Debe alertar al usuario cuando una aplicación o página web fuera bloqueada.
- f) Solución debe soportar como mínimo 70 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, SPAM, Botnets, Anonymizer, Hacking, Inactive Sites y Spyware/ Malicious Sites.
- g) Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.
- h) Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales (usuarios) y grupos de usuarios.
- i) La solución debe categorizar las aplicaciones y URLs por factor de riesgo.
- j) Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario.
- k) Solución debe inspeccionar el tráfico web cifrado (SSL/TLS) de los usuarios, y permitir excepciones granulares de inspección para proteger la privacidad de los usuarios y/o cumplir con regulaciones.
- l) Debe permitir la categorización de los sitios HTTPS basado en el contenido del campo SNI (Server Name Indication), sin la necesidad de descifrar el tráfico web.
- m) Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y HTTP/2.
- n) Debe soportar la inspección de tráfico HTTPS sobre puertos no estándar (distinto a los puertos HTTP/HTTPS).

7.1.3.7. Prevención de Amenazas

- a) Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en el repositorio la clasificación y/o reputación de direcciones IP, Dominios, URL, redes de Comando y Control y ataques DoS.
- b) Debe tener capacidad de clasificación y análisis de archivos y posterior validación en el repositorio de inteligencia de amenazas en nube del propio fabricante, sin generar un impacto en el rendimiento de la red.
- c) Los equipos deben tener integrada la detección y prevención de virus y amenazas (antimalware).
- d) La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.
- e) Debe tener capacidad de protección de pre-infección del malware que fue identificado en los archivos.
- f) Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), Mail (SMTP o POP3), SMB y FTP.
- g) Debe tener una base de datos local de firmas de malware y cache de reputación de URL, para una respuesta rápida. Si una URL no está ubicada en la cache, debe ser consultada automáticamente en el repositorio de Inteligencia de amenazas en nube para su clasificación y prevención.
- h) Debe soportar Inspección de tráfico cifrado/encryptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).
- i) Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware.
- j) Debe tener capacidades de inspección y prevención de amenaza en el canal cifrado SSH, con las siguientes capacidades:
 - a. Bloquear ataques en canal SSH.
 - b. Bloquea la transmisión de virus a través de los protocolos SCP y SFTP.
 - c. Prevenir el descifrado de contraseñas en fuerza bruta de servidores SSH/SFTP.
- k) Debe soportar para la alimentación de IoC (Indicadores de Compromiso) desde fuentes externas, en formato CSV y STIX XML (Structured Threat Information Expression) para la prevención de amenazas.
- l) Los IoC deben ser actualizados automáticamente de acuerdo con un intervalo definido en la consola.
- m) Los IoC definidos en las fuentes externas deberán poder ser como mínimo: URL, Dominio, IP, Rango de IP, Hash (MD5, SHA1, SHA256) y campos de correo (Mail From, To, CC, Subject).

7.1.3.8. VPN IPSec

- a) Debe soportar túneles VPN punto a punto Site-to-Site de manera ilimitada o hasta la máxima capacidad soportada por el equipamiento.
- b) Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- c) Deben soportar encriptación AES-128 y AES-256 para las fases I y II de IKE.
- d) Deben soportar integridad en MD5, SHA1, SHA-256, SHA-512, AES-XCBX para las fases I y II de IKE.
- e) Debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit), Grupo 19 (256-bit ECP) y Grupo 20 (384-bit ECP) para las fases I y II de IKE.
- f) Debe poder integrarse con Directorio Activo Microsoft para crear reglas de control de acceso a través de VPN, empleando: usuarios, grupos de usuarios, maquinas, dirección IP y redes.
- g) Debe poder integrarse con Azure AD (Microsoft) mediante SAML para autenticación en el acceso remoto de clientes VPN.
- h) El cliente VPN, debe instalarse sobre sistemas operativos Windows, Linux y MacOS.

7.1.3.9. Identificación de Usuarios

- a) La solución debe proveer diferentes métodos para obtener las identidades de los usuarios, tales como:
 - a. Sin agente, haciendo búsquedas al Directorio Activo Microsoft.
 - b. Con agente implementado en los servidores de Directorio Activo Microsoft.
 - c. Empleando un Portal Cautivo.
 - d. Empleando un Proveedor de Identidad (IdP) basado en SAML
- b) La solución debe soportar el uso del protocolo WMI (Windows management instrumentation).
- c) La solución debe soportar el uso del protocolo Kerberos (Transparent Kerberos Authentication).
- d) Debe proveer un "Portal Cautivo", para autenticar a los usuarios que no están dentro del Directorio Activo, los usuarios que no tienen plataforma Windows y/o los usuarios invitados.
- e) Cuando se detecte que los usuarios no se han autenticado, la solución tiene que redireccionarlos a un Portal Cautivo, a través del protocolo HTTP.
- f) Debe soportar al menos los siguientes métodos de autenticación: nombre de usuario y contraseña, que podrá ser configurado en la base de datos Interna del equipo, servidor de LDAP.
- g) La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall.

7.1.3.10. Instalación y configuración:

- a) La migración deberá realizarse en horario fuera de oficina, sin que estas acciones afecten el normal funcionamiento de los sistemas y accesos a los recursos informáticos, teniendo una ventana de tiempo de 12 horas por cada día de trabajo de migración, en coordinación con la oficina de tecnologías de información de las OEFA.
- b) Asegurar la compatibilidad y funcionamiento de los servicios migrados en la nueva solución
- c) El contratista deberá configurar el equipo de seguridad perimetral para que realice backups automáticos, los cuales serán almacenados en un servidor que será brindado por la OTI.
- d) El contratista será responsable del correcto funcionamiento de todas las políticas implementadas para que los servicios publicados no se vean afectados
- e) La implementación de la nueva solución de seguridad perimetral debe ser transparente, de tal manera que conserve los permisos a nivel de usuario y no afecte a las aplicaciones.
- f) El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo, Activando las capacidades de seguridad incluidas en cada equipo, de manera que se utilice satisfactoriamente el licenciamiento adquirido.
- g) Realizar el desmontaje de los equipos actuales de seguridad Checkpoint
- h) Rackeo, implementación y configuración de la solución ofertada en el centro de procesamiento de datos de OEFA.
- i) Realizar actividades de configuración, las cuales consisten en:
 - a. Realizar el procedimiento para la puesta en producción del equipo que estará en pasivo.
 - b. El especialista de la solución por parte del postor ganador debe garantizar que la solución ofertada cuenta con el sistema operativo actualizado con la última versión estable y recomendada por la marca al momento de la implementación.
 - c. Activar la configuración de logs de la solución.
 - d. Configurar la generación de Backups de la solución.
 - e. Activar las capacidades de seguridad incluidas en cada equipo, de manera que se utilice satisfactoriamente el licenciamiento adquirido.
- j) La configuración de la solución debe realizarse de acuerdo con las mejores prácticas de la marca

7.1.4. SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALL TIPO IV:

- a) Cantidad 31 appliance.
- b) Rendimiento (throughput) en prevención de amenazas de 500 Mbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, URL Filtering (opcional), IPS, Antivirus, Anti-Bot y/o DNS Security y Emulación Malware día-cero con log habilitado.
- c) Rendimiento (throughput) en NGFW de 950 Mbps (medido con Capacidades habilitadas de: Firewall y Control de Aplicaciones.
- d) Conexiones Concurrentes: 1'000,000 sesiones o conexiones concurrentes, o 300,000 de sesiones o conexiones concurrentes en caso se analice a través de transacciones HTTP.
- e) Conexiones por segundo: 15,000 conexiones o sesiones por segundo, o 10,000 de conexiones o sesiones por segundo en caso se analice a través de transacciones HTTP.
- f) Interfaces:
 - a. 08 puertos de red 1GB (RJ45)
 - b. 01 puerto de red 1GB SFP (1000 Base F).
 - c. 01 puerto de consola tipo: USB Type-C o Micro USB
 - d. 01 puerto USB
- g) El OEFA proporcionará al postor ganador los backups de los 31 equipos de la Marca Checkpoint Modelo SMB 1530.
- h) El OEFA proporcionará al postor ganador un cuadro en Excel que contendrá la siguiente información (Nombre de la OD, IP del Checkpoint y el nombre del backup), para proceder a restaurar en los equipos propuestos.

7.1.4.1. Consideraciones Generales

- a) El sistema operativo deberá ser del fabricante de la solución de firewall ofertado, el mismo deberá venir de fábrica con el "hardening" necesario para no tener componentes y/o configuraciones que puedan causar vulnerabilidades.
- b) En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan publicado y/o anunciado el "End-of-life" y/o "End-of-Support", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos. Este requerimiento deberá ser respaldado con una carta del fabricante adjuntando la documentación publica de Internet que la respalde.
- c) Las versiones de sistema operativo y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) altas o críticas (acumuladas entre sus diferentes versiones) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas.
- d) La solución de seguridad debe soportar la configuración de clúster en modo de operación en alta disponibilidad (HA).
- e) Debe soportar redundancia de enlaces WAN o de ISP (Internet Service Provider) redundantes, sin la necesidad de una licencia adicional o software/hardware de terceros.
- f) La redundancia de ISP emplea la detección de falla enlace para conmutación automática.
- g) Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster.
- h) Administración accesible a través de SSH y de interfaz Web segura (HTTPS).
- i) La herramienta debe ser capaz de realizar backup/restore de la configuración, permitiendo al administrador programar la realización de los backups en periodos diario, semanal y mensual.
- j) Los backups pueden ser generados transferidos vía SFTP, SCP, FTP y localmente. El backup debe tener capacidad de ser cifrado.
- k) La comunicación entre la consola de gestión y los equipos de seguridad (firewall), debe ser cifrada y autenticada

7.1.4.2. Funcionalidades de Red

- a) La solución debe ser capaz de operar en modalidad Layer 3 (routing), modalidad in-line (bridge) y L2 (port mirroring y/o monitor mode).
- b) Deben soportar inspección del tráfico cifrado (SSL/HTTPS).

- c) Debe soportar enrutamiento con IPv4 e IPv6.
- d) Debe soportar DHCP en modos: Servidor DHCP y DHCP Relay (reenvío) en IPv4 e IPv6.
- e) Debe contar con un módulo de control QoS basado en prioridades y pesos para el control de: porcentaje del ancho de banda disponible, basado en prioridad de regla, ancho de banda mínimo garantizado y ancho de banda máximo, basado en límites.
- f) Debe contar con un módulo de control QoS garantizar el ancho de banda y controlar la latencia para aplicaciones de transmisión, como son Voz sobre IP (VoIP) y videoconferencia.
- g) Soporte de rutas estáticas, IPSec Routing, RIP, OSPFv2 y OSPFv3(IPv6), IGMP, PIM SM, PIM DM PIM SSM, BGP, EBGp Multihop y IPv6 BGP-4.
- h) Soporte de PBR (policy based routing) que permite ante la presencia de dos o más enlaces, se pueda decidir por que enlace ingresa y egresa un tráfico determinado.
- i) Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster.
- j) La solución debe soportar registro de tablas ARP estáticas y dinámicas, definiendo cantidad de entradas ARP y el tiempo de duración

7.1.4.3. Gestión de Políticas

- a) El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como: Redes y Grupos de Redes, Host, Zonas, Objetos Dinámicos, Dominios FQDN, Usuarios, Grupos de Usuarios, Clientes Remotos VPN, Servicios y Aplicaciones Web y Comunidad de VPN.
- b) Sobre la base de las políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Drop, Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final.
- c) Las reglas deben permitir manejo de ancho de banda de distintos protocolos y aplicaciones web, permitiendo la limitación del uso ancho de banda, tanto para carga (upload) y descarga (download) por cada regla.
- d) Debe poder analizar la utilización de las reglas, con niveles de indicador: muy alto, alto, medio, bajo y cero, este último indicador permitirá identificar que dicha regla no ha tenido conexiones (sin uso). El uso también debe poder identificarse numéricamente en miles, millones, gigas y teras de hits por regla. El contador de uso de la regla podrá configurarse en ventanas de tiempo de: día, semana, mes y total.
- e) Las reglas de firewall deben poder establecer vigencia en base a objetos de tiempo, basado en periodos: diario, semanal, mensual y tener un horario de recurrencia en la cual la regla está vigente.
- f) Capacidad de crear reglas de firewall en base fuentes dinámicos externas, los cuales serán basados en fuentes de URL externas (HTTP/HTTPs) que contengan archivos planos (CSV) y JSON. En el caso de archivos planos se debe poder el tipo de dato y los delimitadores. En caso de JSON debe emplear la sintaxis JQ.
- g) Las fuentes externas deben ser consultadas automáticamente por el firewall, con la finalidad de automatizar las reglas de acceso, no siendo necesario instalar reglas en el firewall.
- h) Las reglas de firewall en base fuentes dinámicos externas deben soportar como mínimo Dirección IP, Rango de Red, IP y mascara de red y dominio FQDN. Estas fuentes deberán ser efectivas en reglas de acceso tanto en origen como destino.
- i) En el caso de navegación en internet, debe tener capacidad de crear políticas con acciones de interacción al usuario final, tales como:
 - a. Preguntar al usuario si desea continuar o no, y deben indicar una razón para continuar.
 - b. Informar al usuario, ellos pueden continuar a la aplicación o cancelar el requerimiento.
 - c. Bloquear indicando al usuario final un mensaje de bloque a la aplicación.
- j) Los mensajes de bloqueo e interacción con el usuario final deben ser editables en idioma y contenido.
- k) Soportar la creación de políticas basada en Geolocalización, configurando que el tráfico de determinado País y/o Países sean bloqueados o permitidos.
- l) Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.

- m) Debe posibilitar la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.
- n) Las actualizaciones de las direcciones o rangos de IP publica por cada país, debe realizarse periódicamente y de manera automática.
- o) Debe tener capacidad de controlar el tipo de contenido para el tráfico entrante y saliente.
- p) El control se debe realizar por tipo de dato en tránsito, por lo menos de dos maneras: mediante el tipo de contenido, clasificado analizando el contenido del archivo, y mediante el tipo de archivo, analizando el ID o metadato del archivo.

7.1.4.4. Prevención de Intrusos – IPS

- a) La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad.
- b) El IPS debe contar con mecanismo de detección de amenazas de múltiples métodos: detección por firmas, validación de protocolo, detección anómala y análisis de comportamiento.
- c) El IPS debe contar con motor de identificación de patrones, que le permita diferenciar entre paquetes inofensivos y paquetes maliciosos, detectando expresiones regulares en los flujos de como un segundo nivel de análisis, para reducir la tasa de falsos positivos.
- d) El IPS debe poder detectar evasiones en la retransmisión de paquetes o el envío de paquetes maliciosos en la retransmisión, proveyendo capacidad de reensamblaje de flujo para conexiones TCP y reordenamiento de paquetes.
- e) Debe tener protección contra ataques de DoS (Denial of Service).
- f) Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en objetos de red o mediante las reglas de seguridad configuradas.
- g) Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP, SMTP, DNS, POP e IMAP,
- h) Las políticas de protección de IPS deben poder establecerse en base a parámetros tales como: número del CVE, nivel de severidad y nivel de efectividad (confianza).
- i) Debe permitir adicionar excepciones a las protecciones de IPS desde el log o de manera manual.
- j) Debe poder capturar paquetes de eventos de IPS, para proveer un análisis posterior.

7.1.4.5. Anti-Bot y/o Antispyware

- a) La solución debe proveer una herramienta que haga descubrimiento de “bots” dentro de la red. Dicha herramienta debe bloquear la comunicación que intenten establecer los equipos infectados “bots” hacia las redes de los atacantes en Internet (botnet).
- b) La solución debe incluir al menos los siguientes métodos de identificación:
 - Identificación de direcciones web de Comando y Control utilizadas por los criminales para controlar los bots.
 - Identificación de patrones (fingerprints) de comunicación utilizada por cada familia de bots.
 - Identificación de comportamiento de bots.
- c) La solución debe contar con un repositorio en la nube del propio fabricante para la identificación de direcciones y patrones de comunicación de “botnet”. El Anti-Bot se debe actualizar continuamente de manera automática.
- d) La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de direcciones IP, URL y recursos DNS no identificados y/o no clasificados.
- e) La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA) y DNS Tunneling, empleando protección basada en Machine Learning. Estas funcionalidades deben emplear las fuentes de inteligencia de amenazas en nube del propio fabricante.
- f) La solución debe contar con análisis la reputación de direcciones URL, direcciones IP y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).

7.1.4.6. Control de Aplicaciones y URL Filtering

- a) La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web.

- b) Se requiere que capacidad de detección de 4,000 aplicaciones en la base de datos de control de aplicaciones para la aplicación de políticas.
- c) La base de datos de control de aplicaciones debe actualizarse por un servicio basado en la nube, la actualización debe ser periódica y automática.
- d) Debe permitir la creación de firmas personalizadas para el Control de Aplicaciones y URL Filtering, mediante herramientas del propio del fabricante.
- e) Debe alertar al usuario cuando una aplicación o página web fuera bloqueada.
- f) Solución debe soportar como mínimo 70 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, SPAM, Botnets, Anonymizer, Hacking, Inactive Sites y Spyware/ Malicious Sites.
- g) Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.
- h) Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales (usuarios) y grupos de usuarios.
- i) La solución debe categorizar las aplicaciones y URLs por factor de riesgo.
- j) Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario.
- k) Solución debe inspeccionar el tráfico web cifrado (SSL/TLS) de los usuarios, y permitir excepciones granulares de inspección para proteger la privacidad de los usuarios y/o cumplir con regulaciones.
- l) Debe permitir la categorización de los sitios HTTPS basado en el contenido del campo SNI (Server Name Indication), sin la necesidad de descifrar el tráfico web.
- m) Debe soportar la inspección de tráfico HTTPS sobre puertos no estándar (distinto a los puertos HTTP/HTTPS).

7.1.4.7. Prevención de Amenazas

- a) Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en el repositorio la clasificación y/o reputación de direcciones IP, Dominios, URL, redes de Comando y Control y ataques DoS.
- b) Debe tener capacidad de clasificación y análisis de archivos y posterior validación en el repositorio de inteligencia de amenazas en nube del propio fabricante, sin generar un impacto en el rendimiento de la red.
- c) Los equipos deben tener integrada la detección y prevención de virus y amenazas (antimalware).
- d) La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.
- e) Debe tener capacidad de protección de pre-infección del malware que fue identificado en los archivos.
- f) Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), SMB y FTP.
- g) Debe tener una base de datos local de firmas de malware y cache de reputación de URL, para una respuesta rápida. Si una URL no está ubicada en la cache, debe ser consultada automáticamente en el repositorio de Inteligencia de amenazas en nube para su clasificación y prevención.
- h) Debe soportar Inspección de tráfico cifrado/encryptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).
- i) Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware.
- j) Debe tener capacidades de inspección y prevención de amenaza en el canal cifrado SSH, con las siguientes capacidades:
 - Bloquear ataques en canal SSH.
 - Bloquea la transmisión de virus a través de los protocolos SCP y SFTP.
 - Prevenir el descifrado de contraseñas en fuerza bruta de servidores SSH/SFTP.
- k) Debe soportar para la alimentación de IoC (Indicadores de Compromiso) desde fuentes externas, en formato CSV y STIX XML (Structured Threat Information Expression) para la prevención de amenazas.

- l) Los IoC deben ser actualizados automáticamente de acuerdo con un intervalo definido en la consola.
- m) Los IoC definidos en las fuentes externas deberán poder ser como mínimo: URL, Dominio, IP, Rango de IP, Hash (MD5, SHA1, SHA256) y campos de correo (Mail From, To, CC, Subject).

7.1.4.8. Prevención de Amenazas Desconocidas o de Día Cero

- a) La solución debe ser capaz de identificar y prevenir ataques y malware no conocido, presentes en documentos y/o archivos ejecutables.
- b) La solución debe ser capaz de emular los archivos identificados en el firewall de forma automática, a través del envío y posterior análisis en la nube del propio fabricante de la solución de firewall para la Emulación de Malware (SandBox). La nube de emulación de amenazas del fabricante debe tener certificación SOC2 Tipo II.
- c) La solución debe proteger a los usuarios internos, de manera que prevenga el acceso o descarga a los archivos en tanto estos son analizados en el equipo de emulación, si el archivo es benigno se entrega el archivo original al usuario y si el archivo es maligno se deniega su acceso o descarga.
- d) La solución debe proporcionar la capacidad de protección contra ataques de malware desconocido y de día cero antes de que se hayan creado protecciones de firmas estáticas.
- e) La solución debe proveer prevención en tiempo real de malware desconocido en las descargas web y canal de correo electrónico.
- f) La solución deberá poder emular archivos para la identificación de malware que viajan en los protocolos: HTTP, HTTPS, SMTP, IMAP, CIFS, SMBv3, SMBv3 multi-channel y FTP.
- g) La solución deberá poder emular al menos los siguientes tipos de archivos: Adobe PDF, Microsoft Office (documentos y plantillas), DLL, Java, Flash, Scripts, archivos comprimidos (ZIP, 7Z, RAR, GZ, TGZ, TAR, TAR.GZ y JAR), ejecutables (EXE, COM, LNK, DLL, DRV, SYS, SCR, VBX) y archivos de MacOS (APP, DMG, PKG).
- h) El motor de emulación debe detectar llamadas API, cambios en el sistema de archivos, cambios en el registro, conexiones de red, procesos de sistema.
- i) El motor de emulación debe analizar y emular los URL contenidos en documentos Microsoft Office y PDF, para detectar y prevenir descargas maliciosas de malware.
- j) El motor de emulación debe emplear mecanismos de Machine Learning para detectar y prevenir ataques ocultos sobre archivos LNK (accesos directos) tales como: Icon Spoofing, File Attribute Manipulation, Shortened URLs.
- k) El motor de emulación debe contar con tecnologías de ML basadas en Redes Neuronales (Neural Networks) para la detección de amenazas en los archivos Microsoft Office y PDF.
- l) Las soluciones deben admitir motores de detección automatizados basados en machine learning.
- m) La solución debe ser capaz de soportar escaneo de enlaces (links) dentro de correos para detección de malware.
- n) La solución debe ser resistente a los casos en los que el código de shell o el malware no se ejecutarían si detectaran la existencia de un entorno virtual

7.1.4.9. VPN IPSec

- a) Debe soportar por lo menos 200 VPN Client-to-Site IPSec.
- b) Debe soportar túneles VPN punto a punto Site-to-Site de manera ilimitada o hasta la máxima capacidad soportada por el equipamiento.
- c) Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- d) Deben soportar encriptación AES-128 y AES-256 para las fases I y II de IKE.
- e) Deben soportar integridad en MD5, SHA1, SHA-256, SHA-512, AES-XCBC para las fases I y II de IKE.
- f) Debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit), Grupo 19 (256-bit ECP) y Grupo 20 (384-bit ECP) para las fases I y II de IKE.

- g) Debe poder integrarse con Directorio Activo Microsoft para crear reglas de control de acceso a través de VPN, empleando: usuarios, grupos de usuarios, maquinas, dirección IP y redes.
- h) Debe poder integrarse con Azure AD (Microsoft) mediante SAML para autenticación en el acceso remoto de clientes VPN.
- i) El cliente VPN, debe instalarse sobre sistemas operativos Windows, Linux y MacOS

7.1.4.10. Identificación de Usuarios

- a) La solución debe proveer diferentes métodos para obtener las identidades de los usuarios, tales como:
 - a. Sin agente, haciendo búsquedas al Directorio Activo Microsoft.
 - b. Con agente implementado en los servidores de Directorio Activo Microsoft.
 - c. Empleando un Portal Cautivo.
 - d. Empleando un Proveedor de Identidad (IdP) basado en SAML
- b) La solución debe soportar el uso del protocolo WMI (Windows management instrumentation).
- c) La solución debe soportar el uso del protocolo Kerberos (Transparent Kerberos Authentication).
- d) Debe proveer un "Portal Cautivo", para autenticar a los usuarios que no están dentro del Directorio Activo, los usuarios que no tienen plataforma Windows y/o los usuarios invitados.
- e) Cuando se detecte que los usuarios no se han autenticado, la solución tiene que redireccionarlos a un Portal Cautivo, a través del protocolo HTTP.
- f) Debe soportar al menos los siguientes métodos de autenticación: nombre de usuario y contraseña, que podrá ser configurado en la base de datos Interna del equipo, servidor de LDAP.
- g) La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall.

7.1.4.11. Instalación y configuración:

- a. El postor ganador asegurará la compatibilidad y funcionamiento de los servicios migrados en la nueva solución
- b. El contratista deberá configurar el equipo de seguridad perimetral para que realice backups automáticos, los cuales serán almacenados en un servidor que será brindado por la OTI.
- c. El especialista de la solución por parte del postor ganador debe garantizar que la solución ofertada cuenta con el sistema operativo actualizado con la última versión estable y recomendada por la marca al momento de la instalación y configuración.
- d. El contratista será responsable del correcto funcionamiento de todas las políticas implementadas para que los servicios publicados no se vean afectados
- e. La implementación de la nueva solución de seguridad perimetral debe ser transparente, de tal manera que conserve los permisos a nivel de usuario y no afecte a las aplicaciones.
- f. La implementación y puesta en producción de la solución requerida deberá contemplar las buenas prácticas en diseño de redes y esquemas lógicos de configuración, según la marca ofertada.
- g. El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo, Activando las capacidades de seguridad incluidas en cada equipo, de manera que se utilice satisfactoriamente el licenciamiento adquirido.
- h. El OEFA proporcionará al postor ganador los **backups de los 30 equipos de la Marca Checkpoint Modelo SMB 1570.**
- i. El OEFA proporcionará al postor ganador un cuadro en Excel que contendrá los campos nombre de la OD, IP local del Checkpoint y el nombre del backup, para proceder a restaurar en los equipos propuestos.
- j. El postor ganador realizará las actividades de revisión del backup restaurado, las cuales consisten mínimo en:
 - a. Verificar la configuración restaurada del equipamiento de cada uno de los equipos de las OD's, según el siguiente detalle.

OBJETO	TIPO DE OBJETO	CANTIDAD
	Limitacion de Navegacion	16
Objeto Network	Address Ranges	4
	Domains	2
	Dynamic Objects	2
	Gateways and Servers	5
	Groups	5
	Host	30
	Interoperable Devices	5
	Networks	5
	Security Zones	3
Server	Radius	1
	Trusted CA	1
Services		
	CITRIX TCP	1
	Compound TCP	4
	GTP	4
	Other Services	16
	Grupo de Servicio	16
	TCP	15
	UDP	10
User-Identities	Access Roles	17
	LDAP Account Units	3
	LDAP Groups	2
	User Groups	3
	Users	30
	User Templates	10
VPN	VPN Communities	2

7.1.5. CONSOLA DE ADMINISTRACIÓN DE FIREWALLS

- La consola de administración debe ser ofertada en **modalidad SaaS** del mismo fabricante de los firewalls ofertados, y debe gestionara los siguientes firewalls ofertados:
 - Solucion de Next Generation Firewall – Tipo I
 - Solucion de Next Generation Firewall – Tipo II
 - Solucion de Next Generation Firewall – Tipo III
 - Solucion de Next Generation Firewall – Tipo IV
- La consola de administración debe ser ofrecido en modalidad SaaS, en la nube del propio fabricante de los firewalls ofertados.
- Los servicios de nube SaaS provistos por el fabricante deben cumplir con la certificación SOC 2 Type II.
- La consola de administración deberá estar alojada en nube provista por el fabricante de la solución ofertada y el acceso a consola de administración en nube debe soportar doble factor de autenticación (MFA) a través de Google Authenticator y Microsoft Authenticator.
- El acceso a consola de administración en nube debe soportar integración con proveedores de identidad (IdP) tales como: Microsoft Azure AD (Entra ID), Google Workspace, Okta, DUO y otros adicionales basados en SAML.
- Capacidad de almacenamiento y/o indexación de 70 Gb por día, con una retención mínima de 03 meses en línea.
- La consola centralizada debe permitir el despliegue de actualizaciones y parches de seguridad en los firewalls gestionados.
- Debe permitir el acceso concurrente de administradores y la instalación de políticas en modo simultaneo.
- Debe tener capacidad de revisión histórica de políticas, identificando las revisiones y cambios que fueron instalados y quien realizo los cambios. Debe tener capacidad de revertir a una versión especifica de política.

- d) En el proceso de instalación, debe realizar una validación de las reglas en la política, para verificar que son consistentes y no presentan reglas redundantes. Si se verifican errores, la política no deberá ser instalada.
- e) Debe contar con un módulo de cumplimiento basado en estándares internacionales, para la evaluación de la configuración y política de seguridad de los firewalls implementados. Esta evaluación debe comparar en base los siguientes estándares regulatorios como mínimo: ISO27001:2022, ISO27002:2022, NIST 800-41, NIST 800-53 y Cobit 5.0.
- f) El módulo de cumplimiento debe contar con reportes para ser exportados en formato Excel.
- g) En caso el fabricante no cuente con esta funcionalidad, el portor podrá ofertar una herramienta externa, licenciada para todos los firewalls, que cumpla con dichas características.
- h) La herramienta debe integrar en una única consola gráfica segmentando el estado general de todos los dispositivos administrados, la configuración de la política de seguridad, los logs registrados y el monitoreo de toda la plataforma.
- i) Debe incluir una herramienta que administre centralizadamente la licencia de todos los equipos, controlados desde la estación de administración.
- j) La herramienta debe permitir gestionar de forma centralizada los túneles VPN y las VPN de acceso remoto de los usuarios.
- k) La herramienta debe permitir sesiones concurrentes de diferentes usuarios o dispositivos para los cambios de políticas.
- l) La herramienta debe permitir la creación de perfiles de administradores, basados en roles, que accedan a secciones parciales de administración o a la totalidad, indicando también si los perfiles son de solo lectura o lectura/escritura.
- m) Capacidad de gestión y operaciones mediante API (Rest API), para lectura de información y enviar comandos.
- n) Debe contar con capacidad de envío (forward) de eventos hacia un SIEM o syslog server externos, empleando protocolos TLS sobre TCP, TCP y UDP.
- o) La seguridad con los SIEM o syslog, se podrá realizar mediante el uso de certificados cuando se emplea TLS sobre TCP.

7.1.6. CORRELACIÓN DE EVENTOS, LOGS Y REPORTE DE FIREWALLS

- a) Se deberá incluir una consola de correlación de eventos, Logs y reportes y en modalidad SaaS del mismo fabricante, para todos los firewalls ofertados en los Ítems:
 - Next Generation Firewall – Tipo I
 - Next Generation Firewall – Tipo II
 - Next Generation Firewall – Tipo III
 - Next Generation Firewall – Tipo IV
- b) La consola de correlación de eventos, Logs y reportes debe ser ofrecido en modalidad SaaS, en la nube del propio fabricante de los firewalls ofertados.
- c) **Los servicios de nube SaaS** provistos por el fabricante deben cumplir con la certificación SOC 2 Type II.
- d) Los logs de emulación de malware del firewall deben estar tener información detallada de los ataques, exponiendo las técnicas y tácticas de MITRE ATT&CK que fueron empleadas y revisar los incidentes de seguridad de la red de una manera que se expongan las principales técnicas y tácticas utilizadas por los atacantes. Debe tener la capacidad de realizar búsqueda en base a técnicas o tácticas específicas.
- e) Debe tener una vista de los ataques detectados, con la siguiente información:
 - a. Numero de host en la red infectados con malware.
 - b. Top de conexiones maliciosas de Command and Control, IP del sitio de C&C y número de conexiones, dirección IP origen.
 - c. Número de ataques prevenidos.
 - d. Numero de archivos maliciosos bloqueados.
- f) Debe tener una vista en formato “línea de tiempo” de los ataques detectados, con la siguiente información:
 - Línea de tiempo con los hosts en la red infectados con malware.
 - Línea de tiempo de los Ciber Ataques detectados por los módulos de IPS, Anti-Virus, Anti-Bot, y Emulación.

- Debe tener la capacidad de poder crear y editar los gráficos de información (widgets) en diferentes tipos tales como: tablas, cuadros (columnas, barras, pie), línea de tiempo, mapa e infografía.
- g) Debe tener una vista de la emulación de amenazas, indicando el número de archivos maliciosos prevenidos, top de fuentes origine y numero de archivo maliciosos descargados.
- h) El correlacionado de eventos, debe tener capacidad de respuesta automática, en base a eventos de seguridad según políticas definidas. Las acciones de respuesta automáticas deben ser: enviar un correo electrónico, generar un SNMP Trap, bloquear una IP origen de donde proviene el evento, bloquear un ataque distribuido que provienen de múltiples orígenes.
- i) Debe tener capacidad de vistas de los tuneles VPN donde se muestre el estado de los peers y la Fase 1 y Fase 2. Debe proveer una vista de los usuarios remotos por VPN, donde muestre las estadísticas de los usuarios remotos en tiempo real.

NOTA: Todo el cumplimiento referido a las capacidades de hardware y/o de rendimiento solicitadas, se deberá verificar a través de la documentación técnica (datasheet) y/o manuales y/o bochures emitidos públicamente por el propio fabricante de la solución de firewall, adjuntando el documento y enlace (URL) público de Internet del propio fabricante que lo sustente. No se aceptarán cartas de fabricante y/o representantes locales, como un fundamento para el cumplimiento de estos requerimientos solicitados

7.2. SOLUCIÓN DE FIREWALL DE APLICACIONES WEB – WAF

A continuación, se detallan las características técnicas que deben cumplir cada uno de los componentes de la solución Firewall de Aplicaciones Web.

7.2.1 Características Generales

- a) Se requiere una solución para la protección automatizada de aplicaciones web y API, la misma debe incorporar las siguientes tecnologías de protección.
 - a. Web Application Protection
 - b. API Security
 - c. Bot Prevention
 - d. Intrusion Prevention (IPS) (opcional).
 - e. File Security y/o Antimalware
 - f. Prevencion DDoS
- b) La solución debe emplear tecnología de Machine Learning para la detección y prevención de los ataques en las aplicaciones web y API.
- c) La tecnología de Machine Learning empleada, debe permitir tener un número muy bajo de falsos positivos y proteger contra ataques conocidos y no conocidos (día-cero) en tiempo real.
- d) La protección de día cero deberá ser realizada a través del aprendizaje del aplicativo y su comportamiento evitando ataques por headers o formularios web.
- e) La solución deberá de permitir una cantidad ilimitada de aplicaciones y de ancho de banda, ya que la solución brindara protección a diferentes ambientes WEB y API y la cantidad de estas aplicaciones es muy dinámica al igual que la cantidad del ancho de banda y su ubicación (nube/on-premise)
- f) La solución deberá brindar en conjunto una protección de al menos 180 Millones de solicitudes HTTP/S Web Request por año, y no debe tener un límite en la cantidad de aplicaciones y/o subdominios a ser protegidas.
- g) En caso la solución proteja a nivel de tráfico, se deberá considerar una capacidad mínima de protección de 1.5 Gbps de tráfico limpio hacia la entidad.
- h) La solución debe poder prevenir ciberataques conocidos y desconocidos.
- i) La implementación debe ser flexible y poderse realizar en diferentes ambientes en nube y en premisas.
- j) La solución deberá de ser administrada desde un portal en la nube.
- k) La solución debe poder proteger las aplicaciones en diferentes entornos construidos en cualquier arquitectura (on-premise, nube, contenedores) administrado desde un único portal centralizado.

- l) La solución debe poder analizar cada solicitud entrante y se debe analizar en contexto esta solicitud.
- m) El motor de inteligencia artificial de la solución debe poder llevar a cabo un análisis de riesgos mediante el examen de parámetros como:
 - a. El perfil del usuario
 - b. Los patrones observados en la sesión del usuario
 - c. La forma en que otros usuarios interactúan típicamente con la aplicación.
- n) A cada solicitud se le debe asignar una puntuación que determine la probabilidad de que sea maliciosa.
- o) El motor se debe poder adaptar automáticamente a los cambios de la aplicación al perfilar continuamente el usuario, la aplicación y el contenido.
- p) El motor deberá contar con un aprendizaje asistido donde el operador con una simple decisión pueda asegurar el tráfico.
- q) La solución debe poder detener los ataques contra aplicaciones que incluyen:
 - a. Cross Site Request Forgery
 - b. XML External Entity
 - c. Remote Code Execution
 - d. Evasion Techniques
 - e. LDAP Injection
 - f. Path Traversal
 - g. Vulnerability Scanning
 - h. SQL Injection
 - i. Métodos HTTP ilegales Entrada no válida para formularios
 - j. APIs Bot Scraping Brute Force Attacks
- r) La solución deberá proporcionar protecciones basadas en firmas para al menos 2,800 vulnerabilidades (CVE) y exposiciones comunes para aplicaciones Web.
- s) La solución debe poder ser instalada en diferentes ambientes, algunos actualmente implementados en la institución y otros que se implementaran en el futuro, al menos debe poder ser instalada en:
 - a. En nube publica: Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure
 - b. En contenedores: Docker, Kubernetes, Kubernetes Ingress.
 - c. En agente sobre NGINX Web Server o proxy reverso de NGINX
 - d. En plataforma Virtual: VMware
- t) En **Servicio WAF SaaS** (empleando registro DNS).

7.2.2 Funcionalidades para la seguridad WEB

- a) La solución deberá permitir aplicar políticas para definir los límites en los mensajes del protocolo HTTP. Incluir al menos los siguientes parámetros:
 - a. Tamaño del cuerpo (Body Size): tamaño máximo del cuerpo del mensaje HTTP
 - b. Tamaño de URL (URL Size): tamaño máximo de la URL, esto incluye todos los campos de consulta.
 - c. Tamaño del encabezado (Header Size): tamaño máximo del encabezado HTTP
 - d. Profundidad máxima del objeto (Object Depth): tamaño de profundidad máxima del objeto JSON / XML, esto incluye XML incrustado en JSON y lo contrario.
 - e. Métodos validos HTTP (RFP): Aceptar o bloquear métodos https no standard
- b) La solución deberá soportar métodos para poder distinguir a los usuarios entre sí. Deberá soportar al menos los siguientes mecanismos:
 - a. X-Forwarded-For
 - b. IP Origen
 - c. Cookie
 - d. Header Only
- c) La solución deberá poder limitar los siguientes parámetros
 - a. Los Bytes en el tamaño de URL
 - b. La profundidad de los objetos de HTTP

- c. El tamaño del body de una petición
- d. El tamaño del encabezado en una petición
- e. Deberá contar con una protección de CSRF
- d) La solución deberá ser capaz de configurar reglas custom para poder aceptar (Accept), rechazar (drop) y exceptuar análisis (skip) en el tráfico web, empleando operadores lógicos (and, or) y condiciones tales como igual (equals), no igual (not equals) y existe (exists) entre las diversas reglas creadas, de acuerdo con lo siguientes parámetros:
 - a. URI
 - b. IP Origen (source IP)
 - c. Identificador de Origen (XFF, Header Key, JWT Key, Cookie, Source IP)
 - d. Nombre de parámetro (expresión regular en el HTTP Reques o JSON File)
 - e. Valor de parámetro (expresión regular en el HTTP Reques o JSON File)
 - f. Código de País (Ej. PE para el caso de Perú)
 - g. Nombre de País (geolocalización)
 - h. Nombre y Hash SHA de un archivo
 - i. Método HTTP (GET, POST, PUT, DELETE, PATC)
 - j. Valor de Header (expresión regular)
 - k. Nombre de Header (expresión regular)
- e) La solución deberá ser capaz de configurar excepciones y modificar la acción que toma la herramienta de forma predeterminada, la solución deberá permitir aceptar o bloquear el tráfico cuando el mismo haga match a algunas de las condiciones mencionadas en el punto anterior.
- f) La solución deberá permitir subir certificados para poder proteger sitios https de la institución.
- g) La solución deberá incluir un motor de aprendizaje que ayude a disminuir la cantidad de eventos críticos y altos a lo largo del tiempo a medida que aprende el tráfico del sitio y comprende el comportamiento del usuario.
- h) El aprendizaje de la solución debe de funcionar de manera continua y no solo tener un “modo aprendizaje”
- i) La solución deberá clasificar cada solicitud y decidir sus posibilidades de ataque a través de un motor de inteligencia artificial.
- j) Las políticas de la solución deberán de poder operar en al menos los siguientes modos:
 - a. Prevención
 - b. Aprendizaje/detección
- k) La solución deberá incluir políticas predefinidas que sean Best Practice (o la práctica recomendada del fabricante). Estas políticas deberán de poder ser editadas en caso de ser necesario.

7.2.3 Funcionalidades para la seguridad de archivos (File Security o Antimalware)

- a) La solución debe contar con un motor de análisis de archivos maliciosos, que eviten que se carguen archivos maliciosos en los servidores de la organización. El motor de seguridad de archivos escanea el tráfico HTTP que ingresa a la organización.
- b) La solución debe contar con capacidad de emulación de amenazas no conocidas en una zona de pruebas ubicada en la nube de amenazas del propio fabricante, para evitar ataques en la etapa más temprana. La capacidad de emulación debe analizar varios tipos de archivos conocidos: Word, Excel, PowerPoint, PDF y archivos ejecutables.
- c) La solución debe proteger contra archivos maliciosos en formatos comprimidos en el tráfico HTTP entrante, analizando su contenido extraído, como mínimo en: ZIP, RAR, TAR y 7Z.

7.2.4 Funcionalidades para la seguridad de API

- a) La solución debe ofrecer protección preventiva para posibles vulnerabilidades de API a través de un procedimiento de validación de esquema (schema)

- b) La solución deberá integrarse a través de un API con el SDLC e integrar una validación de esquema de json, para conocer el comportamiento esperado del aplicativo.
- c) La solución debe revisar las solicitudes de API entrantes con estos esquemas (schema) para bloquear todas las solicitudes de API no válidas.
- d) A solución deberá también utilizar las funciones de WAF para detectar y bloquear automáticamente los payloads maliciosos en la API.
- e) La solución debe poder proteger las API utilizando técnicas como la validación automatizada mediante archivos de esquema Open API.

7.2.5 Funcionalidades para la protección Anti-bot

- a) La solución deberá poder inyectar scripts en páginas de aplicaciones web, como páginas de inicio de sesión o utilizar algún otro mecanismo para recopilar datos sobre patrones de entrada y canalice secuencias de pulsaciones de teclas, movimientos del ratón y toques con los dedos. Esto con el fin de poder diferenciar a un humano de un bot
- b) La solución deberá poder identificar estos patrones en caso de que un bot los utilice.
- c) La solución deberá poder tomar una decisión si la entrada es ingresada por un humano o por un script automático (como un bot), y bloquear esta actividad.
- d) La solución debe poder detener el relleno de credenciales (credential stuffing), los ataques de fuerza bruta y el site scraping con la protección avanzada de bots.
- e) Debe tener capacidad de establecer límites (rate limit) a recursos URI en aplicaciones web o API.
- f) Los límites se pueden establecer a direcciones IP o redes CIDR, estableciendo límites de request en un periodo de tiempo establecido.

7.2.6 Gestión Certificados SSL/TLS

- a) La solución debe permitir la carga de certificados SSL/TLS de la entidad para la publicación e inspección de las aplicaciones web a través de tráfico cifrado HTTPS.
- b) Se podrán emplear certificados del tipo wildcard.
- c) Los certificados digitales pueden ser almacenados en los gateways virtuales (VMware), en las plantillas de despliegue de los appliances virtuales Azure y AWS. Así mismo, también puede ser configurados en plataforma de micro-servicios Docker y Kubernetes.

7.2.7 Configuración e implementación.

- a) Se requiere un proveedor que realice las tareas de implementación, configuración y soporte técnico de la solución por todo el periodo contratado.
- b) El proveedor debe realizar como mínimo las siguientes capacidades:
 - a. Implementar las políticas de seguridad para el tráfico web, como la inspección de contenido, protección contra ataques, y la filtración de URLs maliciosas.
 - b. Activa las funciones básicas de protección como filtrado de IP, protección contra ataques conocidos (OWASP Top 10), y bloqueo de amenazas comunes.
 - c. Establece la recolección de registros y el monitoreo de eventos para detectar incidentes de seguridad.
 - d. Configura reglas y filtros personalizados según las necesidades de tus aplicaciones web. Esto incluye configurar excepciones o reglas específicas para ciertos tipos de tráfico.
 - e. Si es necesario, conecta el WAF con otros dispositivos de seguridad, como firewalls de red o sistemas de prevención de intrusiones (IPS).
- a) Despliegue progresivo: Si es posible, realiza un despliegue gradual para asegurar que el WAF no interrumpa las operaciones. Comienza en un entorno de prueba antes de ir a producción.
- b) Monitoreo continuo: Monitorea el rendimiento y los logs para identificar posibles falsos positivos y ajustar las reglas según sea necesario.

- c) El postor debe realizar la migración de los servidores de publicación de las aplicaciones de los servidores. Apps.oefa.gob.pe, publico.oefa.gob.pe, sistemas.oefa.gob.pe

7.3. SOLUCIÓN DE SEGURIDAD DE NUBE GOOGLE WORKSPACE

La entidad cuenta con una suscripción de Google Workspace productiva para todos sus colaboradores, a continuación, se detallan las características técnicas que deben cumplir la solución de seguridad para la nube Google Workspace.

7.3.1 Requerimientos generales de la solución requerida

- a. Debe estar licenciada para 1,800 buzones por un periodo de tres (03) años.
- b. La solución de seguridad debe ser en modalidad (SaaS) para la protección integral del correo electrónico en Google Workspace en modalidad SaaS, con capacidad avanzadas de anti-phishing para correos entrantes, salientes e internos, protección contra ransomware y malware de día cero (Sandboxing), protección de URL maliciosas (URL Sandboxing), capacidad de reescritura de URLs, identificación de anomalías y compromiso de cuentas de usuario, protección contra ataques de código QR y prevención de fuga de información (DLP).
- c. El servicio debe operar desde la propia nube del fabricante de seguridad e integrarse de manera nativa y con capacidad de prevención en línea (in-line) mediante tecnologías API, con la nube del proveedor de servicios de correo electrónico (Google Workspace). No se aceptarán soluciones basadas en "Security Email Gateway" o similares, y no debe ser necesario ningún cambio disruptivo en el servicio de correo, tales como cambios de registro DNS (MX) para envío del correo a plataformas externas, relay SMTP o cualquier otra modificación a nivel de tráfico SMTP antes de que ingrese a la nube del Google Workspace.

7.3.2 Funcionalidades generales requeridas de la solución de seguridad para Google Workspace

- a. La solución de seguridad deberá poder proteger de amenazas cibernéticas en modalidad SaaS (Software as a Service) al servicio de Google Workspace, para el componente de correo electrónico (GMail).
- b. La detección y prevención de amenazas para el correo electrónico debe ser tanto para el flujo entrante, saliente e interno (correos enviados entre usuarios dentro del mismo dominio o Tenant).
- c. La solución deberá proporcionar protección contra los siguientes ataques cibernéticos:
 - a. Amenazas de Phishing y Spam.
 - b. Detección de Malware no conocido de "día cero" en correo electrónico de Google Workspace mediante emulación de amenazas (Sandboxing) y extracción de amenazas (CDR).
 - c. Reputación y Emulación de URLs maliciosas
 - d. Reescritura URLs para protección de phishing de día-cero.
 - e. Protección contra ataques de Phishing basado en códigos QR.
 - f. Identificación y alerta del uso de aplicaciones SaaS públicas no autorizadas.
 - g. Detección de anomalías de usuarios y prevención de robo de cuentas.
 - h. Protección contra archivos protegidos o cifrados con contraseña.
 - i. Compromiso de Proveedores (Compromised Partner)
 - j. Prevención de Fuga de Información - DLP
- d. La solución deberá poner en cuarentena los correos electrónicos y su contenido malicioso y ofrecerá al usuario opciones para eliminar los recursos en cuarentena o restaurarlos.
- e. La solución debe proteger el correo mediante "prevención en línea", es decir detectando y previniendo las amenazas, antes de que estas lleguen a los buzones de correo de Google Workspace del usuario final.

- f. La solución debe ser compatible con la conexión a la nube de "inteligencia de amenazas" del fabricante para compartir IoC (indicadores de compromiso) y actualizaciones de amenazas.
- g. La solución debe tener capacidad de análisis de DMARC (Domain-based Message Authentication, Reporting and Conformance) para rechazar o llevar a cuarentena de correos entrantes que fallan en DMARC.
- h. La solución debe tener capacidad para proteger NickName Impersonation, que es el ataque donde el ciber-delincuente se hace pasar por los nombres y correos electrónicos de los ejecutivos de la empresa para intentar engañar a un empleado interno para que revele información confidencial o ejecute algún pago. Se debe poder configurar la protección para cuentas estratégicas de la organización.
- i. La solución debe tener una pista de auditoria (audit trail) sobre todos los cambios realizados en la plataforma, indicando: fecha y hora del cambio, usuario que realizo, tipo de cambio y descripción asociada.
- j. La solución debe tener capacidades reportes detallados diarios hacia los usuarios finales, sobre su cuarentena retenida en las últimas 24 horas, así como habilitar un portal de autoservicio para la gestión de la propia cuarentena por el usuario final. El acceso al portal de la cuarentena podrá ser autenticado empleando las propias credenciales y MFA (de ser el caso) de la nube Google.
- k. Los correos que fueron cuarentenados pueden ser liberados por el propio usuario final o solicitar su liberación al administrador (configurable basado en la política y flujo del evento de seguridad).
- l. La solución debe tener capacidades de analizar los correos que fueron considerados como spam por la propia nube de Google y que sean "falsos positivos", de manera que esto sean tratados como correos limpios y sean liberados al buzón entrante (inbox).

7.3.3 Capacidades requeridas de prevención de malware y phishing en Google Workspace

- a. La solución de seguridad deberá poder proteger de amenazas cibernéticas en modalidad SaaS (Software as a Service) al servicio de Google Workspace, para el componente de correo electrónico (GMail).
- b. La detección y prevención de amenazas para el correo electrónico debe ser tanto para el flujo entrante, saliente e interno (correos enviados entre usuarios dentro del mismo dominio o Tenant).
- c. La solución deberá proporcionar protección contra los siguientes ataques cibernéticos:
 - a. Amenazas de Phishing y Spam.
 - b. Detección de Malware no conocido de "día cero" en correo electrónico de Google Workspace mediante emulación de amenazas (Sandboxing).
 - c. Extracción de amenazas (CDR) (opcional).
 - d. Reputación y Emulación de URLs maliciosas
 - e. Reescritura URLs para protección de phishing de día-cero.
 - f. Protección contra ataques de Phishing basado en códigos QR.
 - g. Identificación y alerta del uso de aplicaciones SaaS públicas no autorizadas.
 - h. Detección de anomalías de usuarios y prevención de robo de cuentas.
 - i. Protección contra archivos protegidos o cifrados con contraseña.
 - j. Compromiso de Proveedores (Compromised Partner) (opcional).
 - k. Prevención de Fuga de Información – DLP.
- d. La solución deberá poner en cuarentena los correos electrónicos y su contenido malicioso y ofrecerá al usuario opciones para eliminar los recursos en cuarentena o restaurarlos.
- e. La solución debe proteger el correo mediante "prevención en línea", es decir detectando y previniendo las amenazas, antes de que estas lleguen a los buzones de correo de Google Workspace del usuario final.

- f. La solución debe ser compatible con la conexión a la nube de "inteligencia de amenazas" del fabricante para compartir IoC (indicadores de compromiso) y actualizaciones de amenazas.
- g. La solución debe tener capacidad de análisis de DMARC (Domain-based Message Authentication, Reporting and Conformance) para rechazar o llevar a cuarentena de correos entrantes que fallan en DMARC.
- h. La solución debe tener capacidad para proteger NickName Impersonation, que es el ataque donde el ciber-delincuente se hace pasar por los nombres y correos electrónicos de los ejecutivos de la empresa para intentar engañar a un empleado interno para que revele información confidencial o ejecute algún pago. Se debe poder configurar la protección para cuentas estratégicas de la organización.
- i. La solución debe tener una pista de auditoría (audit trail) sobre todos los cambios realizados en la plataforma, indicando: fecha y hora del cambio, usuario que realizó, tipo de cambio y descripción asociada.
- j. La solución debe tener capacidades reportes detallados diarios hacia los usuarios finales, sobre su cuarentena retenida en las últimas 24 horas, así como habilitar un portal de autoservicio para la gestión de la propia cuarentena por el usuario final. El acceso al portal de la cuarentena podrá ser autenticado empleando las propias credenciales y MFA (de ser el caso) de la nube Google.
- k. Los correos que fueron cuarentenados pueden ser liberados por el propio usuario final o solicitar su liberación al administrador (configurable basado en la política y flujo del evento de seguridad).
- l. La solución debe tener capacidades de analizar los correos que fueron considerados como spam por la propia nube de Google y que sean "falsos positivos", de manera que esto sean tratados como correos limpios y sean liberados al buzón entrante (inbox)

7.3.4 Capacidades requeridas de detección de comportamiento anómalo para identificar robo o compromiso de cuentas en Google Workspace

- a. El motor de detección de anomalías debe detectar comportamientos y acciones que parecen anormales observando en el contexto y la actividad de todos los usuarios de Google Workspace.
- b. Debe analizar el comportamiento, utilizando un algoritmo de aprendizaje automático, para crear un perfil basado en eventos históricos que incluyen ubicaciones y horas de inicio de sesión, comportamiento de transferencia de datos y patrones de mensajes de correo electrónico.
- c. La solución deberá detectar anomalías del comportamiento todos los usuarios de Google Workspace, tales como:
 - a. Detección de comportamiento anómalo basado en motor de Inteligencia Artificial (AI) que inspecciona varios parámetros de la actividad anómala: incluyendo dirección IP, tipo de navegador, versión de navegador, dispositivo y producto VPN empleado.
 - b. Geolocalización, detecta si el usuario ha iniciado sesión de sitios distantes geográficamente en un corto tiempo, inclusive desde localizaciones dentro de un mismo país.
 - c. Detecta si el usuario ha iniciado sesión en un país, en el cual nunca se había iniciado sesión antes.
 - d. Detecta si el usuario ha iniciado sesión desde una dirección IP pública que sea categorizada como maliciosa o como fuente de envío de correos phishing.
 - e. Correo electrónico inusual, detecta si el usuario tiene reglas de correos electrónicos que podrían indicar una intención maliciosa.
 - f. Auto reenvío a correo externos, cuando se crean reglas de reenvío hacia dominios externos.

- g. Fallas de autenticación de multi-factor MFA, analizando el número de eventos fallidos y satisfactorios de un usuario, para reducir la tasa de falsos-positivos.
- h. Envíos masivos, detecta a través de un desvío de línea-base (baseline) a partir de un periodo de aprendizaje sobre la actividad de los usuarios internos, cuando detecta un alto volumen y genera una alerta.
- i. Anomalía de restablecimiento de contraseña, detecta cuando un usuario ha recibido tres o más correos de restablecimiento de contraseña diferentes en un periodo corto de tiempo.
- j. Anomalía de eliminación de correos nuevos, detecta cuando se configura una regla de eliminación de todos los correos nuevos entrantes, para identificar robo de cuenta.
- k. Detecta cuando un usuario envía correos maliciosos de phishing al interno de la organización (destinatarios internos).
- d. Si se logró validar a través de los motores de anomalías, que la cuenta de un usuario está comprometida, la solución debe permitir tomar remediación desde la propia consola donde se registran los eventos anómalos, mediante las acciones de:
 - a. Bloquear la cuenta del usuario comprometido (flujo de remediación automático).
 - b. Poner en lista negra todos los correos salientes de la cuenta comprometida (flujo de remediación automático).
 - c. Restablecimiento de la contraseña de una cuenta de usuario (flujo de remediación manual).
 - d. Desbloquear una cuenta de usuario bloqueada (flujo de remediación manual).
 - e. Restablecer contraseña y desbloquear una cuenta de usuario bloqueada.
- e. La solución debe tener capacidades de análisis retrospectivo de cuentas comprometidas. Inmediatamente después de detectar una cuenta comprometida, los correos electrónicos enviados desde esta cuenta hasta 03 horas antes de la detección se deben volver a escanear con parámetros de sensibilidad más altos y, si se descubre que los correos electrónicos son maliciosos, también se deben poner en cuarentena automáticamente.

7.3.5 Alianzas Estratégicas y Uso de Aplicaciones de Terceros

- a. La solución debe tener capacidad de identificar el riesgos y compromiso en los proveedores con los que interactúa la organización, basados en el volumen de correos intercambiados y las solicitudes de pagos de dominios externos con la organización.
- b. La detección de compromiso de los proveedores debe por lo menos detectar los siguientes indicadores de riesgo asociados:
 - a. Se detecta correos electrónicos de phishing enviados a la organización desde el dominio del proveedor y el remitente estaba autenticado (SPF aprobado).
 - b. Se detecta correos electrónicos de phishing enviados a otros clientes desde el dominio del proveedor y el remitente estaba autenticado (SPF aprobado).
 - c. Se detecta correos electrónicos de phishing enviados a la organización desde el dominio del proveedor, pero el remitente no estaba autenticado (SPF fallido).
- c. La solución debe contar con un módulo que detecte el uso de aplicaciones dentro de la organización, basado en el análisis de los correos.
- d. La detección de aplicaciones debe identificar las aplicaciones basado con los siguientes parámetros:
 - a. Aplicaciones por nivel de riesgo
 - b. Aplicaciones por categoría

c. Aplicaciones usadas a través de una línea de tiempo.

7.3.6 Prevención de Fuga de Información - DLP

- a. La solución debe ser capaz habilitar controles de DLP en el correo electrónico entrantes y salientes.
- b. La solución debe ser capaz de escanear correos electrónicos y archivos en busca de información confidencial para prevención de fuga de información (DLP).
- c. La solución de DLP deberá identificar y prevenir la fuga de archivos con las siguientes características:
 - a. Prevenir la fuga de información que contienen información confidencial, financiera y de identificación personal, incluidos: números de tarjetas de crédito, números de seguro social, números de cuentas bancaria o datos sensibles.
 - b. También deberá realizar prevención de fuga en base palabras claves o diccionarios, y en base a Expresiones Regulares (RegEx) en el correo, esta característica también se empleará para las expresiones regulares en el asunto del correo.
 - c. Generar alertas al remitente, los administradores o personas específicas, cuando se cumpla una regla de DLP.
- d. La solución de DLP debe tener los siguientes flujos de trabajo en capacidad de prevención en línea:
 - a. El correo electrónico queda bloqueado. El usuario recibe una alerta y se le permite solicitar una restauración (el administrador debe aprobar).
 - b. El correo electrónico queda bloqueado. El usuario recibe una alerta y se le permite restaurar el correo electrónico
 - c. El correo electrónico queda bloqueado y el usuario puede solicitar que se vuelva a enviar como cifrado (el administrador debe aprobarlo).
 - d. El correo electrónico queda bloqueado y el usuario puede volver a enviarlo cifrado.
 - e. Se permite el envío del correo electrónico y se envía cifrado.
 - f. Se permite el envío del correo electrónico y se adiciona un encabezado al correo electrónico.
- e. La solución debe proporcionar el panel de la interfaz de usuario y las políticas.
- f. La funcionalidad de DLP puede establecer distintos tipos de niveles de sensibilidad para cada política, donde se valida la cantidad de coincidencias (hit count).
- g. Debe permitir crear tipos de datos (data types) personalizados basados en expresiones regulares y diccionarios. Los diccionarios pueden ser importados desde archivos CSV.
- h. Debe permitir crear tipos de datos compuestos, donde se establece un tipo de dato mandatorio (padre) y tipo de dato opcional (hijo).
- i. Se puede establecer excepciones de políticas DLP para crear "lista blanca" (allow-list) donde la solución deje de analizar correos, mensajes y archivos basados en: Sender), Recipient, File MD5, y palabras que coincidan para la lista blanca

7.3.7 Consola de Administración

- a. La consola de administración deberá estar alojada en nube provista por el fabricante de la solución ofertada y el acceso a consola de administración en nube debe soportar doble factor de autenticación (MFA) a través de Google Authenticator y Microsoft Authenticator.
- b. El acceso a consola de administración en nube debe soportar integración con proveedores de identidad (IdP) tales como Microsoft ADFS, Microsoft Azure AD, Okta y otros basados en SAML.
- c. La consola debe contar con dashboard o vista principal que muestre los eventos de seguridad agrupados por: Phishing, Bussines Email Compromise (BEC), Malware, DLP, Mapa de eventos de Login.

- d. El mapa de eventos de login, debe mostrar los eventos anómalos por geolocalización, para los login satisfactorios y fallidos
- e. Debe contar con un dashboard de analítica, para poder realizar consultas por los tipos de ataques detectados, y las acciones realizadas por la solución de seguridad. La analítica debe mostrar los principales usuarios atacados, así como las áreas o departamentos más atacadas.
- f. La consola debe proveer reporte de seguridad automatizados, seleccionando periodos de los últimos 7, 14 y 30 días, y seleccionando en periodo de entrega para un día específico de la semana, una semana y día específico del mes.
- g. La solución debe poder enviar los eventos de seguridad a plataformas externas de SIEM, en diversos formatos tales como: JSON (Splunk, McAfee SIEM, LogRhythm).
- h. La solución debe tener una capacidad mínima de retención de los correos y sus metadatos, de acuerdo con lo siguiente:
 - a. Correo con amenazas sin cuarentena (metadatos y atributos) de 180 días
 - b. Correo en cuarentena (correo original y adjuntos) de 180 días
 - c. Correo en cuarentena (metadatos y atributos) de 180 días

7.3.8 Implementación

- a. Se requiere un proveedor que realice las tareas de implementación, configuración y soporte técnico de la solución por todo el periodo contratado
- b. El proveedor debe integrar la solución requerida al menos con las siguientes capacidades:
 - a. Integración con el tenant de Google de la entidad con la solución ofrecida vía API.
 - b. Habilitación de la consola con acceso a través del Proveedor de Identidad (IdP) del tenant de Google de entidad, para los usuarios administradores.
 - c. Configuración de las políticas de seguridad para malware, phishing, spam para el correo de acuerdo con las necesarias de las áreas usuarias.
 - d. Configuración de las reglas entrantes y salientes de DLP.
 - e. Configuración de las notificaciones de cuarentena a los usuarios finales.
 - f. Configuración de las reglas de remediación para eventos anómalos o compromiso de cuentas.
 - g. Configuración de los reportes automatizados.
 - h. Configuración de las alarmas o notificaciones a los administradores.
 - i. El postor deberá demostrar ser un partner (socio de negocios) autorizado por el fabricante, para lo cual deberá presentar una carta del fabricante.

7.4. SOLUCIÓN DE INTELIGENCIA DE AMENAZAS Y AUTOMATIZACIÓN

7.4.1. Requerimientos generales de la solución requerida

- a. La solución de Inteligencia de Amenazas debe ser ofertada en **modalidad SaaS**. Esta solución debe almacenar y correlacionar todos los registros (logs) de seguridad de las herramientas ofertadas: Firewall NGFW Tipo I, II, III y IV, y de la solución de protección de Correo para Google Workspace.
- b. La solución de Inteligencia de Amenazas debe tener capacidad de respuesta, integrada a través de API y/o a través de IoC (indicadores de compromiso), con las soluciones ofertadas.
- c. Debe brindar una comprensión integral de la postura de seguridad de la organización, lo que le permite tomar medidas más confiables y efectivas para mitigar y prevenir ataques.
- d. Debe contar detecciones basadas en Advanced User Entity Behavioral Analytics (UEBA).
- e. Debe crear incidentes de seguridad, donde un incidente, es una colección de eventos de uno o más productos que juntos representan una historia de ataque. Para ellos, debe utilizar la inteligencia artificial (IA) y aplicar modelos de aprendizaje automático (ML) para correlacionar los eventos de los productos integrados (eventos benignos y de seguridad) en incidentes unificados.
- f. El nivel de prioridad del incidente se debe calcular en función de los IoC del incidente, incluidos los niveles de confianza y gravedad de la detección.

- g. Los incidentes de seguridad deben tener los estados de: nuevo, asignado, en proceso y cerrado.
- h. Debe mostrar una vista general de línea de tiempo de todos los incidentes de seguridad agrupados e identificados por severidad (crítico, alto, medio, bajo) mediante colores.
- i. La plataforma debe crear los incidentes de manera automática, y estos deben ser asignados a un analista de seguridad
- j. Cada incidente de seguridad asociado a un analista debe tener la siguiente información:
 - i. Nivel de prioridad
 - ii. Fuente Origen
 - iii. Tácticas de MITRE ATT&CK involucradas.
 - iv. Activos involucrados.
 - v. Indicadores de compromiso identificados.
 - vi. Acciones de prevención realizadas y acciones de prevención recomendadas.
 - vii. Cronología (línea de tiempo) del incidente
- k. Las capacidades de análisis de cada incidente deben permitir tener una vista detallada de:
 - i. Información y análisis forense para ver procesos, archivos, URL, dominios y registros involucrados en la información y relacionados con el incidente.
 - ii. Indicadores (IoC) y artefactos para ver los indicadores y artefactos relacionados con el incidente.
 - iii. Árbol de ataque para ver una representación gráfica del informe forense generado por la solución de Endpoint para cada detección realiza.
 - iv. MITRE para conocer las tácticas MITRE ATT&CK utilizadas en el incidente.
 - v. Por cada IoC relacionado con el incidente se debe poder buscar este dato en el Mapa de Captura de Amenazas, la consola de Inteligencia de Amenazas y en la búsqueda de Incidentes.
- l. Debe permitir crear indicadores de compromiso de manera automatizada sobre la base de cada uno de los incidentes.
- m. Capacidad de automatización en base a una severidad específica. La respuesta automática debe tener la capacidad de creación de IoC.
- n. Debe contar con un módulo de Inteligencia de Amenazas, que nos permita tener contexto a través de fuentes del propio fabricante, así como de fuentes terceras, con los siguientes datos:
 - i. Información del indicador (IoC) en una descripción general de alto nivel del indicador analizado:
 - o Para dominios y URL, muestra una captura de pantalla en vivo del sitio web.
 - o Para los archivos, muestra el detalle del hash del archivo: MD5, SHA1 y SHA256
 - o Etiquetas obtenidas por la fuente de Virtus Total.
 - o Visto por primera vez: fecha en que se vio el archivo por primera vez.
 - o Visto por última vez: fecha en que se vio el archivo por última vez.
 - ii. Información de Research o Búsqueda que muestre para Dominios y URLs:
 - o Datos del Whois, muestra usuarios registrados de un recurso de Internet, como un nombre de dominio o un bloque de direcciones IP.
 - o Datos de reputación resumidos en este dominio.
 - o Subdominios asociados para este dominio.
 - o URL relacionadas a este dominio.
 - o Comunicando archivos que se vieron comunicándose con el dominio buscado.
 - o Archivos descargados de este dominio.
 - o Agente de usuario (user-agent) utilizado para ponerse en contacto con este dominio durante un evento malicioso.
 - iii. Información de Research o Búsqueda que muestre para Archivos:
 - o Los nombres de archivo observados por el fabricante para este tipo archivo.
 - o El tráfico de red que creó el archivo durante la emulación de amenazas.
 - o Solicitudes DNS del archivo creados durante la emulación de amenazas.

- Proceso principal (parent process) que creó el archivo.
- El hash del archivo de archivo disponible.
- URL de origen desde las que se descargó el archivo.
- Asuntos de correo electrónico que contienen este archivo, como archivo adjunto.
- iv. Información de análisis de tráfico global:
 - Geolocalización, para el uso del IoC en diferentes ubicaciones geográficas.
 - Muestra los 3 principales países que tienen el mayor número de visitas para este IoC.
 - Muestra las 3 principales industrias donde se vio este IoC.
 - Tipos de plataformas que accedieron al indicador (Ejemplo, Web, Correo electrónico)
 - Numero de eventos en estado salvaje a lo largo del tiempo para el IoC.
- v. Otras Fuentes de Inteligencia (Open Source) tales como:
 - Fuente propia del fabricante de la solución
 - Redes sociales, donde se menciona el IoC
 - Google, resultados de búsqueda para el IoC.
 - Referencias de fuentes terceras de páginas donde se muestre el IoC.
- o. Debe permitir crear respuesta automática en base al nivel de confianza y severidad de los indicadores de compromiso (IoC) sobre la base de cada uno de los incidentes, para que estos puedan ser habilitados en el gestor de IoC y su posterior aplicación automática en los Firewalls NGFW, Solucion WAF y de Prevencion de Correo para Google Workspace ofertados.
- p. Se debe poder crear notificaciones automáticas ante la prioridad de un incidente (critica, alta, media) empleando correo electrónico y canales de Microsoft Teams (URL).
- q. Debe contar con un módulo de emulación de amenazas, que nos permita cargar un archivo o una ruta de archivo en URL, en la plataforma Sandbox del propio fabricante para su análisis.
- r. Luego de analizado, se debe enviar un veredicto del análisis. Si se determinó que el archivo es malicioso, la informe emulación de amenazas está disponible para descarga.
- s. Debe proveer una herramienta de investigación que permite realizar consultas avanzadas sobre todos los eventos forenses maliciosos y benignos recopilados de los eventos de seguridad.
- t. La información recopilada debe permitir:
 - i. Investigue el alcance completo de un ataque.
 - ii. Descubrir un ataque sigiloso mediante la observación de una actividad sospechosa.
 - iii. Reparar el ataque antes de que cause más daño.
 - iv. Busque de forma proactiva ataques avanzados mediante la búsqueda de anomalías y el uso de pistas de búsqueda.
- u. La caza de amenazas debe permitir:
 - i. Recopilación y enriquecimiento de datos: todos los eventos se recopilan a través de múltiples sensores en agente, se envían a un repositorio unificado y se complementan con información de inteligencia de amenazas y mapa de MITRE.
 - ii. Consultas predefinidas y un panel de MITRE que mapean toda la actividad y permite el inicio rápido a la búsqueda proactiva de amenazas.
 - iii. Acciones de remediación por cada resultado o de manera masiva, para tomar acciones como la cuarentena de archivos, terminar procesos, iniciar análisis forense y aislar equipos.
 - iv. Los datos del mapa de captura de amenazas se deben almacenar con un periodo mínimo de retención de 30 días.
- v. Debe poder crear y editar indicadores de compromiso (IoC) que se aplican a todos los productos integrados con la solución de seguridad.
- w. Por cada uno de los IoC se debe tener las siguientes capacidades:
 - i. Debe poder habilitar y deshabilitar cada uno de los IoC
 - ii. Definir tipo: Dominio, IP, URL, Hash (MD5, SHA1, SHA256)
 - iii. Nivel de confianza y nivel de severidad

- iv. Fecha de expiración del IoC.
- v. Debe permitir la carga masiva de IoC de terceros, mediante archivos CSV.
- x. Debe permitir la creación de IoC Feeds propios de la solución, que serán accesibles mediante enlaces URL. El enlace contiene un archivo CSV dinámico que contiene una lista de los IoC que se deben aplicar.
- y. Debe contar con las siguientes capacidades de automatización integrada en los firewalls ofertados:
 - i. Bloquear la IP de los scanner de red conocidos identificados por el motor de IPS.
 - ii. Bloquear la IP de los atacantes identificados por el motor de IPS.
 - iii. Bloquear la IP con reputación maliciosa de atacantes identificada por el motor de IPS.
 - iv. Notificar ante un número elevado (configurable) de conexiones bloqueadas por un mismo origen
 - v. Bloquear el acceso saliente (cuarentena) de IP internas.
- z. Las automatizaciones deben ser parametrizables, pudiendo configurar parámetros tales como:
 - i. Aprobación o no del administrador para aplicar el bloqueo.
 - ii. Duración del bloqueo de la dirección IP o las conexiones.
- aa. Las automatizaciones que requieran un flujo de aprobación deben notificar a los administradores a través de los canales configurados para la aprobación o rechazo de las acciones. Debe contar también con capacidad de revertir una acción automatizada.
- bb. Debe contar con un dashboard que muestre las acciones pendientes de aprobación por el administrador, las cuales también pueden ser rechazadas o revertidas.
- cc. El dashboard debe mostrar un resumen de las acciones automatizadas tales como:
 - i. Línea de tiempo de las automatizaciones ejecutadas.
 - ii. Línea de tiempo de la cantidad de direcciones IP que fueron bloqueadas
 - iii. Línea de tiempo de la cantidad de conexiones que fueron bloqueadas.
 - iv. Número de acciones ejecutadas por tipo de automatización.
- dd. Las notificaciones para cada automatización pueden ser configurables de acuerdo con el nivel deseado de atención para un evento, pudiendo ser inmediato o programado. Las notificaciones pueden ser configuradas para ser enviadas por correo electrónico, SMS y canal de Microsoft Teams.

7.4.2. Implementación

- a) Configuración de la herramienta de inteligencia de amenazas.
- b) Integración de los feeds de inteligencia de diversas fuentes, las mismas que podrán ser libres o pagadas.
- c) Configuración de la automatización para que las amenazas detectadas sean manejadas sin intervención manual (bloqueo de IPs, aislamiento de dispositivos comprometidos, generación de alertas, etc.).
- d) Integración con la solución SIEM que cuenta el OEFA.
- e) Establecer umbrales para generar alertas o acciones automatizadas basadas en la gravedad de las amenazas.
- f) Crear scripts y playbooks para automatizar acciones como el bloqueo de direcciones IP maliciosas, la cuarentena de dispositivos comprometidos, o el bloqueo de comunicaciones sospechosas.

➤ **PRESTACIÓN ACCESORIA**

7.5. SERVICIO DE CYBERSOC

7.5.1. Servicio de Monitoreo y correlación de Eventos de seguridad

- a) Este servicio deberá supervisar el estado y logs de eventos de los equipos gestionados y generará las alertas correspondientes que puedan afectar a la seguridad de la información. Este servicio deberá contar con las siguientes características mínimas:

- b) Deberá monitorear el estado de salud de los equipos de seguridad gestionados declarados en la **Tabla 02: Resumen** en diversos niveles, abarcando:
 - **Nivel 1:** El monitoreo nivel 1 deberá estar orientado al estado de salud de la plataforma física de los equipos del anexo 1 (CPU, memoria, interfaces, enlaces principales, discos duros, entre otros)
 - **Nivel 2:** El monitoreo nivel 2 deberá estar orientado al estado de salud de los servicios principales como flujo y/o aplicaciones de los equipos del anexo 1 (conectividad, estabilidad y flujo entre otras)
 - **Nivel 3:** El monitoreo nivel 3 deberá estar orientado al estado a verificar los eventos de seguridad del cliente. En este tipo de monitoreo se requieren herramientas especializadas como plataformas de colección de eventos y/o plataformas de correlación para la ejecución de estas tareas.
- c) Deberá mantener siempre la disponibilidad de los equipos de seguridad gestionados. En caso de indisponibilidad se debe realizar el análisis correspondiente y documentarlo para ser detallado en el entregable mensual.
- d) Deberá discernir entre falsos positivos o negativos analizando los diferentes eventos detectados.
- e) Deberá clasificar y priorizar (severidad Crítica, alto, medio o bajo) los diferentes eventos generados por el proceso de monitorización. Dependiendo de las funciones de los equipos de seguridad.
- f) Deberá procesar y correlacionar los eventos en tiempo real para detectar sucesos relevantes en los equipos gestionados que puedan ser indicativos de un ataque y emitir las alertas oportunas.

7.5.2. Servicio de Detección y Prevención de Ciberataques

- a) Este servicio deberá alertar sobre las amenazas detectadas por los componentes adquiridos de acuerdo con el nivel de severidad y el impacto que pueda generar en la organización.
- b) Deberá realizar detección y recolección de evidencias que ocurran en los equipos de seguridad gestionados y que puedan poner en peligro la seguridad de la información.
- c) Deberá analizar, detectar y bloquear ciberataques.
- d) Deberá contemplar alertas automáticas para la identificación temprana de amenazas.
- e) Deberá establecer mecanismos de protección, detección y prevención frente a ataques de día Zero, ataques dirigidos o APTs (Amenazas avanzadas persistentes). Estos mecanismos deben ser complementarios a lo que el fabricante del equipamiento de seguridad otorgue.

7.5.3. Servicio de Soporte a Incidentes

- a) Este servicio deberá reaccionar ante cualquier incidente de seguridad identificado y realizará todas las acciones necesarias para la mitigación, contención o neutralización.
- b) Deberá proponer un plan de acción para mitigar, contener o remediar cualquier incidente de seguridad identificado.
- c) Deberá proponer los canales de comunicación adecuados a fin de realizar el escalamiento del incidente detectado.
- d) Deberá notificar el incidente de seguridad detectado a los canales de comunicación establecidos por OEFA.
- e) El servicio podrá complementarse con herramientas automatizadas que permitan tomar acciones de contención basados en playbook, respuesta rápida a incidentes y que tomen como fuente a los componentes adquiridos.
- f) Deberá mantener un historial de incidentes de seguridad actualizados y realizará el análisis estadístico de cantidad de incidentes, como mínimo por: IP origen, IP destino, puerto destino vulnerado, sistema operativo, nombre de la amenaza. Como valor agregado el proveedor deberá detallar los niveles de monitoreo que ofrecerá.
- g) Todos los incidentes (críticos y altos) o solicitudes deberán ser recibidos y procesados hasta su completa resolución.

- h) Reuniones de reportes trimestrales con las recomendaciones a las incidencias detectadas.
- i) El servicio debe incluir incluye el mantenimiento correctivo y preventivo de las Tecnologías que se encuentren bajo la cobertura de soporte.

7.6. SERVICIO GESTIONADO PROACTIVO

Este servicio deberá asumir la administración de toda la infraestructura según detalle en el cuadro de la **Tabla 02: Resumen**

- a) Deberá realizar la gestión proactiva del equipamiento ofertado.
- b) Se deberán emitir las alertas sobre el término del licenciamiento por lo menos 45 días antes de la expiración.
- c) Deberá analizar, recomendar y aplicar las actualizaciones de versión de firmware más estable de los equipos gestionados (Previa coordinación, autorización y supervisión de OEFA).
- d) Deberá analizar y recomendar las mejores prácticas sobre la configuración de los equipos de seguridad del equipamiento Gestionado (Previa coordinación con OEFA).
- e) Deberá informar sobre cualquier anuncio de fin de ciclo de vida del equipamiento gestionado o versión de firmware.
- f) Deberá recomendar optimizaciones sobre las configuraciones para la mejora del rendimiento (CPU y/o RAM) de los equipos gestionados. (Previa coordinación con OEFA).
- g) Deberá ejecutar los respaldos de las configuraciones de los equipos de manera segura, periódica y automática.
- h) El contratista será responsable del servicio gestionado proactivo, esta actividad será bajo supervisión del **SUPERVISOR DE OPERACIONES** solicitado en el **literal c) del numeral 9.1. Perfil del personal**
- i) Toda la solución integral de seguridad deberá estar monitoreada **8X5**, por el **ESPECIALISTA RESIDENTE** solicitado en el **literal d) del numeral 9.1. Perfil del personal** para realizar el monitoreo y mitigación de los incidentes críticos.
- j) Para la atención de incidentes y/o requerimientos en fuera de horario de oficina (incluidos feriados, días festivos); el contratista deberá monitorear y atender a través del **Centro de Operaciones de Seguridad (SOC)** propio, el mismo que debe contar con la membresía activa en FIRST durante toda la ejecución del servicio, **ese documento debe ser presentado para acreditar la admisión de ofertas señalado en el numeral 19 del TDR.**

7.7. NIVELES DE SERVICIO

El contratista deberá contar con un **Centro de Operaciones de Seguridad (SOC)** propia para brindar el soporte 24x7x365 incluidos domingos y feriados. El SOC debe contar con certificación ISO9001 e ISO27001, la cual debe ser adjuntada para la admisión de la oferta.

El contratista deberá proporcionar un número telefónico y correo electrónico para contactar a su Centro de Operaciones de Seguridad (SOC), y debe estar disponible de lunes a domingo (24 horas, 7 días a la semana) durante el tiempo de prestación del servicio.

En caso que el Proveedor requiera realizar trabajos de mantenimiento o mejoras tecnológicas a la plataforma, deberá comunicar por correo electrónico a infraestructuraoti@oefa.gob.pe a la OTI con dos (02) días calendario de anticipación. Estos trabajos no representarán costo alguno al OEFA debido a que se generan en base a mantener la disponibilidad y seguridad del servicio brindado por el Proveedor.

Tiempo de atención: tiempo transcurrido desde que se reporta el incidente por parte de la OTI (el reporte del incidente será vía telefónica y/o por correo electrónico), hasta que el proveedor responda consignando el Ticket de incidente para dar inicio a la solución, el cual deberá ser comunicado al correo electrónico de la persona que reportó el incidente.

Tiempo de solución: Tiempo que transcurre desde que se consigna el ticket de incidente por parte del proveedor a la persona que reportó la avería (OTI), hasta la solución del mismo (presencial y/o remoto, determinado por el proveedor en coordinación con OTI). En caso supere el tiempo de solución establecido en la siguiente tabla se aplicará la penalidad indicada en el **numeral 11. OTRAS PENALIDADES.**

El servicio de soporte técnico se realizará de acuerdo a los niveles de servicios establecidos en el siguiente numeral:

Tabla 03 – Niveles de servicios establecidos

ITEM	SLA	
Clasificación de los incidentes.	<ul style="list-style-type: none"> Nivel 1: Prioridad Critica 	<ul style="list-style-type: none"> Falla total del servicio que impacta al 100% de usuarios o servicios.
	<ul style="list-style-type: none"> Nivel 2: Prioridad Alta. 	<ul style="list-style-type: none"> Degradación del servicio que impacta a más del 60 % de usuarios o servicios.
	<ul style="list-style-type: none"> Nivel 3: Prioridad Media. 	<ul style="list-style-type: none"> Degradación parcial del servicio que impacta a un grupo de usuarios comunes o usuarios VIP.
	<ul style="list-style-type: none"> Nivel 4: Prioridad Baja. 	<ul style="list-style-type: none"> Degradación parcial del servicio que impacta a un usuario o usuarios en particular.
	<ul style="list-style-type: none"> Nivel 5: Requerimientos s/ Solicitudes. 	<ul style="list-style-type: none"> Requerimientos de documentación, o mejoras en la solución. Consultas de cambios en la funcionalidad del producto.

Tabla 04 – Tiempos de niveles de servicios establecidos

Severidad	Tiempo de atención	Tiempo de solución	Modo Atención
Nivel 1	Máximo 30 minutos	Máximo 04 horas	Presencial o remoto, correo o vía telefónica.
Nivel 2	Máximo 01 hora	Máximo 06 horas	Presencial o remoto, correo o vía telefónica.
Nivel 3	Máximo 02 horas	Máximo 08 horas	Presencial o remoto, correo o vía telefónica.
Nivel 4	Máximo 04 horas	Máximo 24 horas	Presencial o remoto, correo o vía telefónica.
Nivel 5	Máximo 08 horas	Máximo 48 horas	Presencial o remoto, correo o vía telefónica.

7.8. VISITA TECNICA

Los proveedores podrán efectuar una visita de carácter técnico al Centro de datos (Avenida Faustino Sánchez Carrión 603- 607- 615 - Jesús María), a fin de evaluar el alcance del servicio de manera precisa, verificar los equipos señalados en la **Tabla 02: Resumen, numeral 7.1 SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALLS de los términos de referencia**, previa coordinación con la Oficina de Tecnologías de la Información desde la indagación de mercado o durante cualquier etapa del procedimiento de selección hasta 3 días calendarios antes de la presentación de su oferta.

Para efectos de coordinación de la visita técnica, los proveedores deberán enviar un correo a infraestructuraoti@oefa.gob.pe, indicando la fecha y hora en la que desean efectuar dicha visita, el horario de atención es de Lunes a Viernes de 10:00am a 04:00pm

7.9. SERVICIO DE ENTRENAMIENTO

- El proveedor debe realizar el entrenamiento de las soluciones ofertadas.
 - NEXT GENERATION FIREWALLS,
 - FIREWALL DE APLICACIONES WEB – WAF,
 - SEGURIDAD DE NUBE GOOGLE WORKSPACE y
 - SOLUCIÓN DE INTELIGENCIA DE AMENAZAS Y AUTOMATIZACIÓN.
- Duración: 32 horas en total
- Participantes: 04
- Modalidad: Presencial
- Dictado: ESPECIALISTAS EN SEGURIDAD, señalado en el literal B. del numeral 9.1.

8. ENTREGABLES

Los entregables, serán dirigidos a la Jefatura de la Oficina de Tecnologías de la Información, en cualquiera de las siguientes modalidades:

Presencial: medio físico y se realizará a través de Mesa de Partes de la Sede Central del OEFA, sito en la Avenida Faustino Sánchez Carrión N° 603 Jesús María, en el horario de 8:30 horas hasta las 16:30 horas de lunes a viernes; o,

Virtual: En la ventanilla electrónica, remitir la documentación a través de la mesa de partes virtual del OEFA <https://sistemas.oefa.gob.pe/mpv> el cual se encuentra disponible de lunes a domingo, las 24 horas del día. Los documentos ingresados entre las 00:00 horas hasta las 23:59, se consideran presentados dentro del mismo día hábil. Los documentos presentados los días sábados, domingos y feriados se consideran presentados al día hábil siguiente.

Tabla 05

Nº	Entregable	Plazo
8.1 PRESTACIÓN PRINCIPAL		
A	Plan de trabajo	Dentro de los diez (10) días calendario , contabilizado desde el día siguiente de suscrito el contrato.
B	Informe de implementación	Dentro de los cinco (05) días calendario , contabilizado a partir de suscrito el Acta de inicio de solución integral de seguridad perimetral .
C	Carta de soporte ³ , del Primer año	Dentro de los diez (10) días calendario , contabilizado a partir del día calendario siguiente de iniciado el servicio de soporte.
D	Carta de soporte, del Segundo año	Dentro de los diez (10) días calendario , contabilizados a partir del día calendario siguiente del término del primer año del servicio de Soporte.
E	Carta de soporte, del Tercer año	Dentro de los diez (10) días calendario , contabilizados a partir del día calendario siguiente del término del segundo año del servicio de Soporte.
8.2 PRESTACIÓN ACCESORIA		
A	Informe mensual	Dentro de los cinco (05) días calendario , contabilizado a partir del día siguiente de culminado el periodo mensual del servicio.

8.1. PRESTACIÓN PRINCIPAL

A. PLAN DE TRABAJO

El contratista en coordinación con la Oficina de Tecnologías de la Información, definirá la fecha y hora de la reunión **Kick Off**, la cual se llevará a cabo dentro de los **cinco (05) días calendarios** siguientes de suscrito el contrato.

El Plan de trabajo debe incluir lo siguiente:

- Acta de reunión de “Kick Off”** del lanzamiento del proyecto, la cual debe ser suscrita por **personal del contratista⁴ y por el personal designado por la OTF⁵**.
- Debe incluir el cronograma de actividades y la estructura de desglose de trabajo (EDT), el diccionario de la EDT, en donde se pueda establecer la fecha de inicio, la ejecución, monitoreo y control, y conclusión del servicio.
- Debe especificar el **Plan de Implementación y configuración de los equipos de seguridad** (cronograma y actividades a desarrollar) del **numeral 7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO**.
- Acuerdo de Confidencialidad firmado.
- Debe especificar el directorio del equipo del contratista.

³ Incluye el derecho de soporte, actualizaciones de reléase y parches de toda la solución implementada en el presente servicio.

⁴ Jefe de proyecto – Personal Clave

⁵ Gestor de Infraestructura y Comunicaciones, Administrador de Operaciones y Administrador de Red.

EL **PLAN DE TRABAJO** deberá ser entregado como máximo a los **diez (10) días calendario**, contabilizado desde el día siguiente de suscrito el contrato.

OEFA tiene un plazo máximo de **tres (03) días calendario** para brindar respuesta al Plan de Trabajo remitida por el contratista. Este entregable estará sujeto a la aprobación del OEFA, y el atraso en su presentación por Mesa de Partes dará origen a las penalidades descritas en la sección **numeral 11. OTRAS PENALIDADES**.

El contratista tendrá un plazo máximo de **tres (03) días calendario** para levantar las observaciones, desde que recibe la notificación por parte del OEFA.

B. INFORME DE IMPLEMENTACIÓN

El contratista deberá presentar el informe de implementación.

- i. Informe de implementación de las soluciones implementadas.
- ii. Diagrama lógico para cada solución implementada.
- iii. Usuario y clave para el acceso mediante un portal web de acceso seguro mediante HTTPS
- iv. **Acta de inicio de solución integral de seguridad perimetral**, el cual consignará que la ejecución del servicio contratado será de mil noventa y cinco (1,095) días calendario, el cual iniciará al culminar el Contrato N° 018-2022-OEFA el cual se encuentra vigente hasta el 03 de octubre de 2025.
- v. El contratista debe presentar el procedimiento para la atención de incidentes y requerimientos.
- vi. El contratista debe presentar una matriz de escalamiento con el detalle de los números telefónicos y direcciones electrónicas del personal del contratista.

C. CARTA DE SOPORTE, DEL PRIMER AÑO

- a) Carta de Soporte, emitido por el fabricante, en el cual indique **las soluciones SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALLS, SOLUCIÓN DE FIREWALL DE APLICACIONES WEB - WAF, SOLUCIÓN DE SEGURIDAD DE NUBE GOOGLE WORKSPACE, SOLUCIÓN DE INTELIGENCIA DE AMENAZAS Y AUTOMATIZACIÓN**, y precise el periodo **PRIMER AÑO** e indicar fecha inicio y fin, por el periodo de trescientos sesenta y cinco (365) días calendarios, contabilizados a partir del día calendario siguiente de suscrito el **Acta de inicio de solución integral de seguridad perimetral**.

D. CARTA DE SOPORTE, DEL SEGUNDO AÑO

- a) Carta de Soporte, emitido por el fabricante, en el cual indique **las soluciones SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALLS, SOLUCIÓN DE FIREWALL DE APLICACIONES WEB - WAF, SOLUCIÓN DE SEGURIDAD DE NUBE GOOGLE WORKSPACE, SOLUCIÓN DE INTELIGENCIA DE AMENAZAS Y AUTOMATIZACIÓN**, y precise el periodo **SEGUNDO AÑO** e indicar fecha inicio y fin, por el periodo de trescientos sesenta y cinco (365) días calendarios, contabilizados a partir del día calendario siguiente de terminado el soporte del primer año.

E. CARTA DE SOPORTE, DEL TERCER AÑO

- a) Carta de Soporte, emitido por el fabricante, en el cual indique **las soluciones SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALLS, SOLUCIÓN DE FIREWALL DE APLICACIONES WEB - WAF, SOLUCIÓN DE SEGURIDAD DE NUBE GOOGLE WORKSPACE, SOLUCIÓN DE INTELIGENCIA DE AMENAZAS Y AUTOMATIZACIÓN**, y precise el periodo **TERCER AÑO** e indicar fecha inicio y fin, por el periodo de trescientos sesenta y cinco (365) días calendarios, contabilizados a partir del día calendario siguiente de terminado el soporte del primer año.

8.2. PRESTACIÓN ACCESORIA

A. INFORME MENSUAL

El contratista iniciará la presentación de este informe a los **treinta (30) días calendario** de suscrito el “**Acta de inicio de solución integral de seguridad perimetral.**”

El contratista deberá entregar mensual, según el plazo establecido en la **Tabla 5**, el **Informe del servicio mensual**

El informe deberá detallar las actividades realizadas como parte del **i) servicio de Cybersoc, ii) servicio gestionado proactivo, iii) servicio de detección y prevención de ciberataques, y iv) servicio de soporte a incidentes** de las siguientes soluciones:

- Reporte mensual de estado de los equipos y eventos de seguridad por cada módulo activado en la solución de seguridad Next Generation Firewalls, WAF, Herramienta de seguridad de nube Google Workspace, Herramienta de inteligencia de amenazas y automatización, y deberá ser suscrita por el **SUPERVISOR DE OPERACIONES**.
- Bitácora de gestión de cambios por cada regla, política configurada en la solución de seguridad Next Generation Firewalls, WAF, Herramienta de seguridad de nube Google Workspace, Herramienta de inteligencia de amenazas y automatización, cada cambio debe registrarse en una ficha que deberá ser suscrita por el **SUPERVISOR DE OPERACIONES** y personal de la OTI.
- Reporte de incidentes y/o eventos de seguridad, alertas sobre el equipamiento y soluciones implementadas, detección, prevención y mitigación de ciberataques dirigidos a la entidad, y deberá ser suscrita por el **SUPERVISOR DE OPERACIONES**
- Informe de las acciones realizadas para la mitigación y/o remediación de incidentes asociados a seguridad, y deberá ser suscrita por el **SUPERVISOR DE OPERACIONES**
- Reporte con el detalla de los mantenimientos y/o mejoras tecnológicas que el contratista haya realizada a las soluciones implementadas, y deberá ser suscrita por el **SUPERVISOR DE OPERACIONES**
- Para el caso de los reportes de tickets (incidentes y/o requerimientos) debe considerar los niveles de servicio (**numeral 7.5.3 del TDR**)

Número del ticket, fecha y hora de atención, fecha y hora en la que se le dio solución al incidente o requerimiento, tiempo de indisponibilidad efectiva (en base a este parámetro se aplicará la penalidad) y el detalle de la solución aplicada, así como a quien se le atribuye la responsabilidad de la “no disponibilidad” del servicio.

9. REQUERIMIENTO DEL PERSONAL DEL PROVEEDOR

9.1. PERFIL DEL PERSONAL

A. UN (01) JEFE DEL PROYECTO - PERSONAL CLAVE

Presencial y/o remoto en las instalaciones del proveedor y bajo demanda para que se desplace a las instalaciones del OEFA, atenderá **hasta el término de la implementación y puesta en operación del servicio.**

i. Actividades:

- Responsable de la coordinación como único punto de contacto con OEFA durante la implementación del servicio.
- Elaborar el plan de trabajo y el informe de implementación, señalados en la **Tabla 05**.
- Responsable del servicio durante la implementación del servicio.
- Realizar la gestión, ejecución, control, seguimiento y cierre del proyecto, de acuerdo con el Plan de Trabajo.

ii. Certificación:

- Certificación oficial y vigente en “ITIL Foundation Certificate IT Service Management”, y/o “Project Management Professional (PMP)” y/o “Scrum Product Owner Professional Certificate”
- La certificación deberá ser acreditada mediante **copia simple del certificado para el perfeccionamiento del contrato.**

B. ESPECIALISTAS EN SEGURIDAD - PERSONAL CLAVE

Presencial y/o remoto en las instalaciones del proveedor y bajo demanda para que se desplace a las instalaciones del OEFA, atenderá **hasta el término de la implementación y puesta en operación del servicio.**

➤ SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALLS

i. Actividades:

- Configuración y Gestión: Definir reglas y políticas de filtrado de tráfico para permitir o bloquear conexiones según las necesidades de seguridad.
- Monitoreo y Análisis: Supervisar el tráfico de red en tiempo real, detectar amenazas y responder a incidentes de seguridad.
- Mantenimiento y Actualización: Aplicar parches, actualizaciones y mejoras de firmware para proteger contra vulnerabilidades emergentes.
- Gestión de Accesos: Controlar el acceso a la red mediante autenticación de usuarios y segmentación de tráfico.
- Registro y Auditoría: Mantener registros de actividad y generar informes para auditorías de seguridad y cumplimiento normativo de la OEFA

ii. Certificación:

- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante en soluciones de Next Generation Firewalls.
- La certificación deberá ser acreditada mediante **copia simple del certificado para el perfeccionamiento del contrato.**

➤ SOLUCIÓN DE FIREWALL DE APLICACIONES WEB – WAF

i. Actividades:

- Configuración y Gestión: Definir y ajustar reglas para proteger contra amenazas como inyección SQL, cross-site scripting (XSS), CSRF y otros ataques web.
- Monitoreo y Análisis: Supervisar el tráfico HTTP/HTTPS en tiempo real para detectar y mitigar amenazas dirigidas a aplicaciones web.
- Mantenimiento y Actualización: Aplicar parches, actualizaciones y ajustes de firmas para proteger contra nuevas vulnerabilidades (OWASP Top 10, por ejemplo).
- Gestión de Políticas de Seguridad: Implementar políticas de seguridad basadas en perfiles de aplicaciones y requisitos de cumplimiento.
- Análisis Forense y Reportes: Investigar incidentes de seguridad, generar reportes de eventos y mejorar continuamente la postura de seguridad.

ii. Certificación:

- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante en soluciones de Next Generation Firewalls.
- La certificación deberá ser acreditada mediante **copia simple del certificado para el perfeccionamiento del contrato.**

➤ **SOLUCIÓN DE INTELIGENCIA DE AMENAZAS Y AUTOMATIZACIÓN**

i. Actividades:

- Configuración de la herramienta de inteligencia de amenazas:
- Integración de los feeds de inteligencia de diversas fuentes,
- Configuración de la automatización para que las amenazas detectadas sean manejadas sin intervención manual (bloqueo de IPs, aislamiento de dispositivos comprometidos, generación de alertas, etc.).
- Integración con la solución SIEM que cuenta el OEFA.
- Establecer umbrales para generar alertas o acciones automatizadas basadas en la gravedad de las amenazas.
- Crear scripts y playbooks para automatizar acciones como el bloqueo de direcciones IP maliciosas, la cuarentena de dispositivos comprometidos, o el bloqueo de comunicaciones sospechosas.

ii. Certificación:

- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante, en soluciones de inteligencia de amenazas y automatización, emitida por el fabricante en protección de usuarios finales.
- Las certificaciones deberán ser acreditadas mediante **copia simple del certificado para el perfeccionamiento del contrato.**

➤ **SOLUCIÓN DE SEGURIDAD DE NUBE GOOGLE WORKSPACE**

i. Actividades:

- Monitoreo y Análisis: Supervisar los correos electrónicos entrantes y salientes para detectar posibles amenazas. Revisar logs y reportes de actividad para identificar tendencias en ataques dirigidos a la OEFA.
- Mantenimiento y Actualización: Mantener actualizado el motor antispam con nuevas firmas y patrones de ataques emergentes. Aplicar parches y mejoras a la plataforma de filtrado.
- Protección contra Phishing y Malware: Implementar autenticación de correo electrónico (SPF, DKIM y DMARC) para evitar la suplantación de identidad.
- Gestión de Cuarentena y Reportes: Administrar la cuarentena de correos sospechosos y permitir la recuperación de falsos positivos de correos dirigidos a la institución.
- Generar reportes sobre correos bloqueados, incidentes de seguridad y métricas de efectividad del antispam.

ii. Certificación:

- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante en Email y Collaboration y/o contar Certified in Cybersecurity ISC2.
- Las certificaciones deberán ser acreditadas mediante **copia simple del certificado para el perfeccionamiento del contrato.**

IMPORTANTE: Un especialista podrá realizar la implementación de uno (01) o más soluciones, por cada solución deberá contar con el certificado solicitado, como máximo se aceptarán a cuatro (04) especialistas.

C. UN (01) SUPERVISOR DE OPERACIONES - PERSONAL CLAVE

Presencial y/o remoto en las instalaciones del proveedor y bajo demanda para que se desplace a las instalaciones del OEFA, atenderá durante el plazo de ejecución de la

prestación, **mil noventa y cinco (1,095) días calendario**, contados a partir del día siguiente de la suscripción del “**Acta de inicio de solución integral de seguridad perimetral.**”

i. Actividades:

- Gestionar los servicios, disponiendo de los recursos necesarios para que se ejecuten de acuerdo con lo previsto. Asimismo, monitorear los indicadores de niveles de servicio y disponibilidad de los servicios establecidos en los TDR.
- Realizar el seguimiento gestión de los incidentes, solicitudes, problemas, activos y cambios para que estos sean atendidos oportunamente.
- Elaborar los informes mensuales, señalado en la **Tabla 05**, documentación de mantenimiento preventivo y el informe final.
- Tener reuniones bimensuales de forma presencial y/o remoto con el gestor de infraestructura para ver las mejoras de políticas y/o actualizaciones.
- Velar por el cumplimiento de las actividades relacionadas a la seguridad a cargo del **ESPECIALISTA RESIDENTE.**
- Velar por el cumplimiento de los compromisos contractuales en el marco del presente servicio.

ii. Certificación:

- Certificación oficial y vigente “ITIL Foundation Certificate”, y/o “Lead Cybersecurity Professional Certificate” y “Service Desk Leader Professional Certificate
- La certificación deberá ser acreditada mediante **copia simple del certificado para el perfeccionamiento del contrato.**

iii. Colegiatura y habilitación

- El personal clave deberá estar colegiado y habilitado para su inicio de la presente participación en el servicio, por lo que deberá presentar su colegiatura y habilidad para la firma del **Acta de inicio de solución integral de seguridad perimetral.**

D. ESPECIALISTA RESIDENTE - PERSONAL CLAVE

i. Presencial en las instalaciones del OEFA, atenderá durante el plazo de ejecución de la prestación, **mil noventa y cinco (1,095) días calendario**, contados a partir del día siguiente de la suscripción del “**Acta de inicio de solución integral de seguridad perimetral**”

ii. El horario de trabajo del **Especialista Residente** será dentro del horario laboral de lunes a viernes de 8:30am a 5:30pm, asimismo la Entidad brindará el espacio físico y mobiliario necesario, sin embargo, el equipamiento debe ser proporcionado por el contratista (mínimo laptop y celular), además coordinará con el Equipo de Respuesta ante Incidentes FIRST).

iii. Actividades:

a. Gestión de Firewalls Perimetrales

- a. Configuración y administración de los equipos de seguridad incluidos en el servicio a contratar (Asegurar que los firewalls perimetrales estén configurados correctamente para filtrar tráfico no autorizado, bloquear ataques y permitir solo el tráfico legítimo.
- b. Monitoreo de tráfico: Monitorear el tráfico que pasa por el firewall para detectar comportamientos anómalos, intrusos o amenazas potenciales.
- c. Revisión y actualización de reglas: Gestionar y actualizar las reglas de firewall periódicamente, basándose en cambios en la red, amenazas emergentes y las políticas de seguridad de la organización.
- d. Auditoría de firewalls: Realizar auditorías regulares para verificar la correcta implementación de las políticas de seguridad y detectar vulnerabilidades en las configuraciones de los dispositivos de seguridad.

- b. Gestión de VPNs (Redes Privadas Virtuales)
 - a. Configuración y administración de VPN: Administrar conexiones seguras para usuarios remotos y sucursales mediante VPNs, configurando accesos y políticas para asegurar la comunicación entre redes.
 - b. Monitoreo y gestión de túneles VPN: Supervisar el estado de los túneles VPN, garantizar que se mantengan seguros y sin interrupciones, y optimizar el rendimiento de las conexiones.
 - c. Autenticación y acceso: Gestionar métodos de autenticación para los usuarios de VPN, asegurando que las credenciales sean seguras y se cumplan las políticas de acceso.
- c. Protección contra Intrusiones (IPS/IDS)
 - a. Configuración de sistemas IPS/IDS: Implementar y gestionar sistemas de prevención y detección de intrusiones para detectar posibles ataques en tiempo real.
 - b. Análisis de alertas: Analizar las alertas generadas por los sistemas IPS/IDS para identificar incidentes de seguridad y determinar su gravedad.
 - c. Ajuste de reglas y firmas: Actualizar y ajustar las reglas de detección y prevención en los sistemas IPS/IDS para adaptarse a nuevas amenazas y mejorar su eficacia.
- d. Protección contra Malware y Amenazas Avanzadas
 - a. Implementación de soluciones antimalware: Desplegar y gestionar soluciones para la protección contra malware, incluidos antivirus, antispam y herramientas antiransomware, a nivel perimetral.
 - b. Monitoreo de tráfico malicioso: Supervisar y detectar tráfico sospechoso o malicioso (como malware, phishing, etc.) que pueda intentar infiltrarse en la red.
 - c. Análisis de amenazas: Colaborar en la investigación de amenazas avanzadas, como APTs (Amenazas Persistentes Avanzadas), y configurar controles para mitigar los riesgos.
- e. Gestión de Proxy y Filtrado de Contenidos
 - a. Administración de servidores proxy: Implementar y gestionar servidores proxy para controlar el acceso a internet y filtrar contenido no autorizado, malicioso o inapropiado.
 - b. Filtrado de URLs y contenido: Asegurar que las políticas de filtrado de contenido estén en vigor para bloquear sitios web peligrosos o inapropiados.
 - c. Análisis de tráfico web: Supervisar el tráfico web entrante y saliente en busca de patrones inusuales, para detectar posibles filtraciones o ataques.
- f. Análisis de Vulnerabilidades y Gestión de Parches
 - a. Escaneo de vulnerabilidades: Realizar escaneos periódicos de seguridad para identificar vulnerabilidades en los dispositivos perimetrales, incluyendo firewalls, routers, servidores, etc.
 - b. Aplicación de parches y actualizaciones: Asegurar que todos los dispositivos de seguridad, incluyendo firewalls y sistemas de prevención de intrusiones, reciban actualizaciones regulares de seguridad y parches de vulnerabilidades.
 - c. Gestión de configuración segura: Revisar la configuración de los sistemas perimetrales para garantizar que se sigan las mejores prácticas de seguridad y evitar configuraciones inseguras.
- g. Gestión de Redes Perimetrales
 - a. Monitoreo de la infraestructura de red perimetral: Supervisar la infraestructura de la red perimetral, incluyendo routers, switches y otros dispositivos de red, para detectar problemas de rendimiento o amenazas de seguridad.
 - b. Segmentación de red: Implementar políticas de segmentación de la red para limitar el acceso a las zonas más críticas y reducir la superficie de ataque.
 - c. Gestión de acceso: Gestionar los accesos y conexiones de usuarios y sistemas internos y externos a la red perimetral, garantizando que solo las conexiones autorizadas estén permitidas.

- h. Respuesta ante Incidentes de Seguridad
- Monitoreo de alertas de seguridad: Configurar sistemas de monitoreo y alerta para detectar incidentes de seguridad (como ataques DDoS, accesos no autorizados, etc.).
 - Investigación de incidentes: Analizar incidentes de seguridad, identificar su origen y tomar acciones correctivas, como bloquear direcciones IP maliciosas o ajustar las reglas del firewall.
 - Coordinación con otros equipos: Trabajar estrechamente con el equipo de respuesta a incidentes FIRST y otros departamentos de seguridad para mitigar los riesgos y aplicar las correcciones necesarias.
- i. Auditoría de Seguridad y Cumplimiento
- Revisión de políticas de seguridad: Asegurarse de que las políticas de seguridad estén alineadas con las regulaciones y los estándares de la industria, como PCI-DSS, GDPR, etc.
 - Informes y auditorías: Producir informes periódicos sobre el estado de la seguridad perimetral, incluyendo análisis de amenazas, incidentes y acciones correctivas implementadas.
 - Cumplimiento normativo: Asegurar que la infraestructura perimetral cumpla con los requisitos regulatorios y normativos, realizando auditorías de cumplimiento y gestionando las evidencias necesarias

iv. Certificación:

- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante en soluciones de Next Generation Firewalls y/o
- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante, en soluciones de inteligencia de amenazas y automatización, emitida por el fabricante en protección de usuarios finales y/o
- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante en Email y Collaboration y/o contar Certified in Cybersecurity ISC2.
- La certificación deberá ser acreditada mediante **copia simple del certificado para el perfeccionamiento del contrato.**

IMPORTANTE: El especialista residente debe contar con **DOS (02)** certificados oficiales como mínimo.

10. PENALIDAD POR MORA

De conformidad con el artículo 162° del Reglamento de la Ley de Contrataciones del Estado, en el caso de retraso injustificado del Contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso en la ejecución del servicio hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente.

11. OTRAS PENALIDADES

En concordancia con el artículo 163° del RLCE.

Se establecen otras penalidades distintas a la penalidad por mora, de acuerdo con el artículo 163° del Reglamento de la Ley de Contrataciones del Estado. En caso de incumplimiento, en la ejecución de las prestaciones materia del contrato, el OEFA aplicará al contratista otras penalidades y son las siguientes:

Niveles de atención y solución – Entrega de documentos			
PRESTACION PRINCIPAL			
1	Por el retraso en la implementación y puesta en funcionamiento del servicio de solución integral de seguridad perimetral para el OEFA del numeral 13.2	10% del monto de la prestación principal por cada día de atraso.	Informe del área usuaria
PRESTACION ACCESORIA			
2	Por retraso en la atención de los incidentes y requerimientos, señalados en la Tabla 04	5% de UIT vigente por cada hora o fracción	Informe por incidente adjunto con acuses de correo o registro de llamadas.
3	Por retraso en la solución de los incidentes y requerimientos, señalados en la Tabla 04	5% de UIT vigente por cada hora o fracción	Informe por incidente adjunto con acuses de correo o registro de llamadas.
4	Por retraso en la presentación del informe de implementación, señalado en el numeral 8.1.B del TDR . (Tabla 05 del numeral 8 del TDR)	5% de UIT vigente por cada día de retraso	Se verificará la fecha de entrega del Informe de implementación
5	Por retraso en la presentación del informe mensual, señalado en el numeral 8.2.A del TDR . (Tabla 05 del numeral 8 del TDR)	5% de UIT vigente por cada día de retraso	Se verificará la fecha de entrega del Informe mensual.
6	Incumplimiento de las normas de seguridad y salud en el trabajo del OEFA ⁶	S/100.00 (cien soles) por ocurrencia	Informe del área usuaria

Nota: UIT Aplicable vigente.

12. MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

- 12.1. Área que coordinará con el proveedor:** La Oficina de Tecnologías de la Información.
- 12.2. Área responsable de la medida de control:** La Oficina de Tecnologías de la Información
- 12.3. Áreas que brindan la conformidad del servicio:** La conformidad será otorgada por el Jefe de Oficina de Tecnologías de la Información, en un plazo que no excederá los siete (07) días calendarios, contabilizado a partir del día calendario siguiente de la recepción de los entregables detallados en el **numeral 8**.

13. LUGAR Y PLAZO DE IMPLEMENTACIÓN Y EJECUCIÓN DE LA PRESTACIÓN DEL SERVICIO

13.1. Lugar

- a) La entrega de los bienes señalado en el numeral 7.1 SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALLS de la Tabla N° 02 del TDR, se realizará en la Sede Central del OEFA, sito en la Avenida Faustino Sánchez Carrión N° 603, 608 y 615 Jesús María, se debe realizar en un plazo de **setenta y cinco (75) días calendario**, contabilizado a partir del día siguiente de suscrito el contrato.

13.2. Plazo de implementación y ejecución de la prestación

- b) La instalación, configuración y puesta en funcionamiento de los bienes señalados en los sub numerales (7.1.1, 7.1.2, 7.1.3), del numeral 7.1. SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALLS deberá realizar en un plazo de **setenta y cinco (75) días calendario**, contabilizado a partir del día siguiente de suscrito el contrato.
- c) La instalación y configuración de los bienes señalados en el sub numeral (7.1.4), del numeral 7.1. SOLUCIÓN DE SEGURIDAD NEXT GENERATION FIREWALLS deberá realizar en un plazo de **setenta y cinco (75) días calendario**, contabilizado a partir

⁶ Conforme al numeral 19.4 del Artículo 19° del Reglamento Interno de Seguridad y Salud en el Trabajo del OEFA, aprobado mediante Resolución de Secretaría General N°037-2018-OEFA/SEG, se prevé la penalidad por incumplimiento de las normas de seguridad y salud en el trabajo establecidas por el OEFA o en la normativa vigente.

del día siguiente de suscrito el contrato.

Cabe precisar que la OTI se encargará del traslado correspondiente a sus Oficinas Desconcentradas y de Enlace a Nivel Nacional.

- d) La instalación, configuración y puesta en funcionamiento de los bienes señalados en los numerales (7.2 SOLUCIÓN DE FIREWALL DE APLICACIONES WEB - WAF, 7.3 SOLUCIÓN DE SEGURIDAD DE NUBE GOOGLE WORKSPACE y 7.4 SOLUCIÓN DE INTELIGENCIA DE AMENAZAS Y AUTOMATIZACIÓN), deberá realizar en un plazo de **setenta y cinco (75) días calendario**, contabilizado a partir del día siguiente de suscrito el contrato.
- e) La ejecución del servicio contratado será de **mil noventa y cinco (1,095) días calendario**, el cual iniciará al culminar el Contrato N° 018-2022-OEFA el cual se encuentra vigente hasta el 03 de octubre de 2025.

14. FORMA DE PAGO

14.1. PRESTACIÓN PRINCIPAL

El pago se efectuará en **tres armadas**, previa conformidad de los entregables detallados en el **numeral 8.1** y en un plazo que no excederá los diez (10) días calendarios, y de acuerdo con lo establecido en el artículo 171° del Reglamento de la Ley de Contrataciones del Estado.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Informe del funcionario responsable de la Oficina de Tecnologías de la Información emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

Entregable	Forma de Pago
Primero	Primer pago anual (pago corresponde al 40% del monto total de la prestación principal), dentro de los diez (10) días calendario siguiente de emitida la conformidad del entregable. <ul style="list-style-type: none"> - PLAN DE TRABAJO - INFORME DE IMPLEMENTACIÓN - CARTA DE SOPORTE, DEL PRIMER AÑO
Segundo	Segundo pago anual (pago corresponde al 30% del monto total de la prestación principal), dentro de los diez (10) días calendario siguiente de emitida la conformidad del entregable. <ul style="list-style-type: none"> - CARTA DE SOPORTE, DEL SEGUNDO AÑO
Tercero	Tercer pago anual (pago corresponde al 30% del monto total de la prestación principal), dentro de los diez (10) días calendario siguiente de emitida la conformidad del entregable. <ul style="list-style-type: none"> - CARTA DE SOPORTE, DEL TERCER AÑO

14.2. PRESTACIÓN ACCESORIA

El pago se efectuará, previa conformidad de los entregables detallados en el **numeral 8.2** y de acuerdo con lo establecido en el artículo 171° del Reglamento de la Ley de Contrataciones del Estado; de acuerdo con el siguiente detalle:

Entregables	Forma de Pago
1	Primer pago trimestral , (cada pago trimestral corresponde al 10% del monto total de la prestación accesoria), dentro de los diez (10) días calendario siguiente de emitida la conformidad.
2	Segundo pago trimestral , (cada pago trimestral corresponde al 10% del monto total de la prestación accesoria), dentro de los diez (10) días calendario siguiente de emitida la conformidad.
3	Tercer pago trimestral , (cada pago trimestral corresponde al 8% del monto total de la prestación accesoria), dentro de los diez (10) días calendario siguiente de emitida la conformidad.
4	Cuarto pago trimestral , (cada pago trimestral corresponde al 8% del monto total de la prestación accesoria), dentro de los diez (10) días calendario siguiente de emitida la conformidad.

Entregables	Forma de Pago
5	Quinto pago trimestral , (cada pago trimestral corresponde al 8% del monto total de la prestación accesoria), dentro de los diez (10) días calendario siguiente de emitida la conformidad.
6	Sesto pago trimestral , (cada pago trimestral corresponde al 8% del monto total de la prestación accesoria), dentro de los diez (10) días calendario siguiente de emitida la conformidad.
7	Séptimo pago trimestral , (cada pago trimestral corresponde al 8% del monto total de la prestación accesoria), dentro de los diez (10) días calendario siguiente de emitida la conformidad.
8	Octavo pago trimestral , (cada pago trimestral corresponde al 8% del monto total de la prestación accesoria), dentro de los diez (10) días calendario siguiente de emitida la conformidad.
9	Noveno pago trimestral , (cada pago trimestral corresponde al 8% del monto total de la prestación accesoria), dentro de los diez (10) días calendario siguiente de emitida la conformidad.
10	Décimo pago trimestral , (cada pago trimestral corresponde al 8% del monto total de la prestación accesoria), dentro de los diez (10) días calendario siguiente de emitida la conformidad.
11	Décimo primero pago trimestral , (cada pago trimestral corresponde al 8% del monto total de la prestación accesoria), dentro de los diez (10) días calendario siguiente de emitida la conformidad.
12	Décimo segundo pago trimestral , (cada pago trimestral corresponde al 8% del monto total de la prestación accesoria), dentro de los diez (10) días calendario siguiente de emitida la conformidad.

15. GARANTÍA DE HARDWARE

- Garantizar en toda circunstancia la posibilidad de escalamiento del servicio con el fabricante para una oportuna solución de los eventos presentados. Con apoyo directo del proveedor.
- El fabricante deberá contar con un centro de soporte mundial para la creación de casos con tiempo de atención 24x7, la facilidad para la creación de casos y consultas deberá ser vía chat, teléfono o correo.
- Para todo el software que comprende la solución, la garantía de buen funcionamiento debe incluir la permanente actualización del software provisto, incluyendo el suministro de nuevas versiones (releases) y reparaciones (en general denominadas comercialmente como parches, temporales fixes, etc.)
- El proveedor deberá brindar soporte técnico local, a través de la línea telefónica, correo electrónico, sistemas en línea o en sitio cuando se requiera. Por el periodo de 36 meses en modalidad 24x7x365.
- El proveedor brinda el servicio de soporte técnico reactivo a todo costo. Por lo que deberá ser asumido íntegramente por el proveedor y debe comprender como mínimo lo siguiente: la mano de obra, materiales, repuesto, partes y piezas. El suministro de partes y piezas es por cuenta y cargo del proveedor.
- Se considera atención remota o en sitio para los equipos ubicado en Lima. Para los equipos ubicados en sedes remotas, se realizará de manera remota con apoyo de OEFA.

16. RESPONSABILIDAD POR VICIOS OCULTOS

Se establece que el plazo de responsabilidad del proveedor por vicios ocultos es por un (01) año, contabilizados a partir de la última conformidad del entregable indicado en los **numerales 8.1 y 8.2.**

17. OTRAS OBLIGACIONES

El proveedor debe cumplir con las disposiciones establecidas en las Normas de Seguridad y Salud en el Trabajo, aprobado por el OEFA a través de la Resolución de Secretaría

General N°037-2018-OEFA/SEG y modificatorias.

18. CONFIDENCIALIDAD DE LA INFORMACIÓN

Toda la información y/o documentación generada como parte de la prestación objeto de la contratación será de propiedad exclusiva de la Entidad, no pudiendo el contratista utilizarla fuera del presente contrato.

El Contratista para la prestación del servicio deberá guardar confidencialidad sobre toda información del OEFA a la que tenga acceso, así como hacerse responsable de que su personal cumpla con este punto, debiendo mantener las reservas del caso y no transmitir ninguna información, por ningún medio, a ninguna persona natural o jurídica, sin la autorización expresa y por escrito de la Oficina de Tecnología de la Información del OEFA.

Esta obligación de reserva o confidencialidad seguirá vigente aún después de culminada la prestación, de la rescisión o resolución del presente contrato, haciéndose responsable el proveedor de los daños y perjuicios que pudiera irrogar la difusión de datos o informes no publicados.

19. OTROS DOCUMENTOS PARA ACREDITAR EN LA ADMISIÓN DE OFERTAS:

- i. El postor debe presentar una carta del fabricante de los equipos de seguridad solicitado en el numeral 7.1 que señale que los equipos (marca y modelo ofertado) se encuentran vigentes tecnológicamente y con soporte del fabricante durante el periodo de prestación de servicios.
- ii. Contar con un **Centro de Operaciones de Seguridad (SOC)** propia para brindar el soporte 24x7x365 incluidos domingos y feriados. El SOC debe contar con certificación ISO9001 e ISO27001, la cual debe ser adjuntada para la admisión de la oferta.
- iii. El postor deberá presentar su certificado de **membresía activa en FIRST** en inglés y traducido el cual evidencia un reconocimiento hacia el compromiso con las mejores prácticas internacionales en materia de seguridad cibernética y gestión de incidentes.
- iv. El postor deberá acreditar para la admisión de la oferta que la solución de seguridad Firewall debe estar presente en los **últimos 08 reportes de Gartner (Magic Quadrant)**, en el cuadrante de Líderes para Network Enterprise Firewalls, adjuntando la carta del fabricante y/o subsidiaria del fabricante en el Perú señalando la marca y modelo de los equipos ofertados, además deberá adjuntar información pública sustentando el cumplimiento de lo solicitado.

20. OTROS DOCUMENTOS PARA EL PERFECCIONAMIENTO DEL CONTRATO

- i. El postor deberá acreditar para admisión de la oferta **ser representante o distribuidor autorizado de la marca ofertada, adjuntando una carta del fabricante haciendo referencia al proceso y dirigido a la entidad.**
- ii. La documentación que sustenta la certificación del **“JEFE DE PROYECTO”**
 - Certificación oficial y vigente en “ITIL Foundation Certificate IT Service Management”, y/o “Project Management Professional (PMP)” y/o “Scrum Product Owner Professional Certificate”
- iii. La documentación que sustenta la certificación del **“SUPERVISOR DE OPERACIONES”**
 - Certificación oficial y vigente “ITIL Foundation Certificate”, y/o “Lead Cybersecurity Professional Certificate” y “Service Desk Leader Professional Certificate”

iv. La documentación que sustenta la certificación del “**ESPECIALISTA RESIDENTE**”

- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante en soluciones de Next Generation Firewalls y/o
- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante, en soluciones de inteligencia de amenazas y automatización, emitida por el fabricante en protección de usuarios finales y/o
- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante en Email y Collaboration y/o contar Certified in Cybersecurity ISC2.

IMPORTANTE: El especialista residente debe contar con **DOS (02)** certificados oficiales como mínimo.

v. La documentación que sustenta la certificación del “**ESPECIALISTA EN SEGURIDAD**”

- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante en soluciones de Next Generation Firewalls.
- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante en Email y Collaboration y/o contar Certified in Cybersecurity ISC2.
- Certificación oficial y vigente de la solución ofertada a nivel especialista y/o administrador y/o experto y/o maestro, emitida por el fabricante, en soluciones de inteligencia de amenazas y automatización, emitida por el fabricante en protección de usuarios finales.

IMPORTANTE: Un especialista podrá realizar la implementación de uno (01) o más soluciones, por cada solución deberá contar con la certificación solicitado, como máximo se aceptarán a cuatro (04) especialistas.

21. ANTICORRUPCIÓN

- ✓ El CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación con el contrato.
- ✓ Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.
- ✓ Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.
- ✓ Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

22. SISTEMA DE GESTIÓN ANTISOBORNO Y DE SEGURIDAD DE LA INFORMACIÓN

El OEFA ha implementado el Sistema de Gestión Integrado (SGI)⁷, que abarca a los Sistemas de Gestión de Calidad, **Seguridad de Información** y Antisoborno del OEFA; asimismo, cuenta con la Política del SIG, que incluye, entre otros, el compromiso referido a prohibir y sancionar todo acto de soborno y corrupción; garantizando la confidencialidad y el acceso efectivo a los canales de denuncia⁸.

En atención a ello, las actividades desarrolladas para la prestación del presente servicio se sujetarán a lo dispuesto en la Política **Integrada** del SGI y a los controles establecidos como parte del Sistema de Gestión Antisoborno del OEFA y *las Políticas Específicas del Sistema de Gestión de Seguridad de la Información, esta última incluye compromisos que asume el contratista*⁹.

⁷ Política Integrada del SGI:

<https://cdn.www.gob.pe/uploads/document/file/3356268/RESOLUCION%20DE%20PRESIDENCIA%20DEL%20CONSEJO%20DIRECTIVO%2000048-2022-OEFA-PCD.pdf?v=1657130259>

⁸ La presentación de las denuncias se realiza de la siguiente manera:

- a. En forma presencial: a través de la Mesa de Partes.
- b. En forma virtual: (i) Mesa de Partes Virtual; (ii) al correo electrónico, a la dirección: denunciasanticorruccion@oefa.gob.pe; o, (iii) a través del Sistema de Denuncias por presuntos actos de corrupción

- PDUCD "Plataforma Digital Única de Denuncias del Ciudadano" (<https://denuncias.servicios.gob.pe/>)

⁹ Política Específica de Seguridad de la Información, aprobada con Resolución de Gerencia General N° 051-2020-OEFA/GEG.

Se encuentra en el siguiente enlace:

<https://cdn.www.gob.pe/uploads/document/file/4017211/Políticas%20Específicas%20de%20Seguridad%20de%20la%20Información%20del%20OEFA.pdf?v=1672787297>

Anexo 01 – Relación de equipos de Seguridad Perimetral actuales

Ítem	Tipo	Marca	Modelo	Cantidad de Puertos de Cobre Utilizados	Cantidad de Puertos de Fibra Utilizados	Garantía - Soporte Vigente
1	Firewall	Checkpoint	15600 – DLP 2	2	2	Si
2	Firewall	Checkpoint	15600 – DLP 1	2	2	Si
3	Firewall	Checkpoint	15600 – FW 2	3	2	Si
4	Firewall	Checkpoint	15600 – FW 1	3	2	Si
5	Firewall	Checkpoint	Smart-1 5050 – Management 1	2	-	Si
6	Firewall	Checkpoint	Smart-1 5050 – Management 2	2	-	Si
7	Firewall	Checkpoint	Smart-1 5050 - Smart Event	2	-	Si
8	Firewall	Checkpoint	Smart-1 5050 – Management	5	-	Si
9	Firewall	Checkpoint	Smart-1 5050 – Smart Event	1	-	Si
10	Firewall	Checkpoint	15600 – FW	3	-	Si

Anexo 02 Validación ficha técnica - CARACTERISTICAS QUE SE DEBEN ACREDITAR

7.1 Solución de Seguridad Next Generation Firewall

7.1.1: Solución de Seguridad Next Generation Firewall Tipo I

Marca y/o Fabricante:

Modelo:

DESCRIPCIÓN	CARACTERISTICAS QUE SE DEBEN ACREDITAR	CUMPLE / NO CUMPLE	N.º DE FOLIO /Pag. / Enlace URL
Rendimiento	Rendimiento (throughput) en prevención de amenazas de 16 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, URL Filtering (opcional), IPS, Antivirus y/o Antimalware, DNS Security y Emulación Malware día-cero con log habilitado).		
	Rendimiento (throughput) en NGFW de 50 Gbps (medido con Capacidades habilitadas de: Firewall y Control de Aplicaciones)		
	Conexiones Concurrentes: 28'000,000 sesiones o conexiones concurrentes, o 5'000,000 de sesiones o conexiones concurrentes en caso se analice a través de transacciones HTTP.		
	Conexiones por segundo: 530,000 conexiones o sesiones por segundo, o 270,000 de conexiones o sesiones por segundo en caso se analice a través de transacciones HTTP.		
Consideraciones Generales	En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan publicado y/o anunciado el "End-of-life" y/o "End-of-Support", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos. Esto requerimiento deberá ser respaldado con una carta del fabricante adjuntando la documentación publica de Internet que la respalde.		
	Las versiones de sistema operativo y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) altas o críticas (acumuladas entre sus diferentes versiones) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas		
Funcionalidades de Red	Debe soportar redundancia de hasta 03 enlaces de distintos proveedores ISP (Internet Service Provider) redundantes, sin la necesidad de una licencia adicional o software/hardware de terceros. La redundancia de ISP puede ser a nivel de "compartición de carga" (load sharing) y detección de falla enlace (primary/backup).		
Control de Aplicaciones y URL Filtering	Solución debe soportar como mínimo 70 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, Botnets y/o Command and Control, Anonymizer, Hacking y Spyware/ Malicious Sites.		
Anti-Bot y/o Antispyware / DNS Security	La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA) y DNS Tunneling, empleando protección basada en Machine Learning. Estas funcionalidades deben emplear las fuentes de inteligencia de amenazas en nube del propio fabricante.		
	La solución debe tener una capa de protección DNS para ataques del tipo Non-Existent Domain (NXNS) Attack y también protección de protocolo DNS sobre HTTPS (DoH).		
Prevención de Amenazas Desconocidas o de Día Cero	La solución debe ser capaz de emular los archivos identificados en el firewall de forma automática, a través del envío y posterior análisis en la nube del propio fabricante de la solución de firewall para la Emulación de Malware (SandBox). La nube de emulación de amenazas del fabricante debe tener certificación SOC2 Tipo II.		
	El motor de emulación debe analizar y emular los URL contenidos en documentos Microsoft Office y PDF, para detectar y prevenir descargas maliciosas de malware.		

7.1.2: Solución de Seguridad Next Generation Firewall Tipo II

Marca y/o Fabricante:

Modelo:

DESCRIPCIÓN	CARACTERÍSTICAS QUE SE DEBEN ACREDITAR	CUMPLE / NO CUMPLE	N.º DE FOLIO /Pag. / Enlace URL
Rendimiento	Rendimiento (throughput) en prevención de amenazas de 16 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, URL Filtering (opcional), IPS, Antivirus y/o Antimalware, DNS Security y Emulación Malware diácono con log habilitado.		
	Rendimiento (throughput) en NGFW de 50 Gbps (medido con Capacidades habilitadas de: Firewall y Control de Aplicaciones		
	Conexiones Concurrentes: 28'000,000 sesiones o conexiones concurrentes, o 5'000,000 de sesiones o conexiones concurrentes en caso se analice a través de transacciones HTTP.		
	Conexiones por segundo: 530,000 conexiones o sesiones por segundo, o 270,000 de conexiones o sesiones por segundo en caso se analice a través de transacciones HTTP.		
Consideraciones Generales	En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan publicado y/o anunciado el "End-of-life" y/o "End-of-Support", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos. Esto requerimiento deberá ser respaldado con una carta del fabricante adjuntando la documentación publica de Internet que la respalde.		
	Las versiones de sistema operativo y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) altas o críticas (acumuladas entre sus diferentes versiones) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas		
Prevencion de Intrusos – IPS	La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad. El IPS debe contar con mecanismo de detección de amenazas de múltiples métodos: detección por firmas, validación de protocolo, detección anómala y análisis de comportamiento		
Control de Aplicaciones y URL Filtering	Solución debe soportar como mínimo 70 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, Botnets y/o Command and Control, Anonymizer, Hacking y Spyware/ Malicious Sites.		
Prevencion de Fuga de Informacion - DLP	Deben soportar inspección del tráfico cifrado (SSL/HTTPS) para las políticas de DLP. Deben soportar inspección del tráfico SMTP, FTP, HTTPS para las políticas de DLP		
	Deben soportar inspección basada en patrones (Pattern), keyword matching y diccionarios. La coincidencia de patrones y la clasificación de archivos deben permitir la identificación de tipos de contenido independientemente de la extensión aplicada al archivo o la compresión aplicada al archivo.		
	Deben soportar inspección basada en los atributos del archivo (File attribute-based matching) y en la estructura del contenido (structured content)		
	Deben soportar el uso de lenguaje de programación abierto para crear tipos de datos específicos, tales como expresiones regulares RegEx.		
	Debe soportar capacidad avanzada de tipos de datos (data types) con características de sensibilidad entre mayúsculas y minúsculas, proximidad de palabras, múltiples ocurrencias de una palabra y capturar parte o la totalidad de una palabra		
	Las opciones de acción para las políticas de DLP deben ser por lo menos las siguientes cuando se coincida con una regla de seguridad: informar al usuario, preguntar al usuario, prevenir (bloqueo) y marca de agua en Archivos MS Office.		

7.1.3: Solucion de Seguridad Next Generation Firewall Tipo III

Marca y/o Fabricante:

Modelo:

DESCRIPCIÓN	CARACTERISTICAS QUE SE DEBEN ACREDITAR	CUMPLE / NO CUMPLE	N.º DE FOLIO /Pag. / Enlace URL
Rendimiento	Rendimiento (throughput) en prevención de amenazas de 09 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, URL Filtering (opcional), IPS, Antivirus y/o Antimalware, DNS Security y Emulación Malware diá-cero con log habilitado.		
	Rendimiento (throughput) en NGFW de 26 Gbps (medido con Capacidades habilitadas de: Firewall y Control de Aplicaciones		
	Conexiones Concurrentes: 16'000,000 sesiones o conexiones concurrentes, o 2'500,000 de sesiones o conexiones concurrentes en caso se analice a través de transacciones HTTP.		
	Conexiones por segundo: 300,000 conexiones o sesiones por segundo, o 230,000 de conexiones o sesiones por segundo en caso se analice a través de transacciones HTTP.		
Consideraciones Generales	En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan publicado y/o anunciado el "End-of-life" y/o "End-of-Support", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos. Esto requerimiento deberá ser respaldado con una carta del fabricante adjuntando la documentación publica de Internet que la respalde.		
	Las versiones de sistema operativo y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) altas o críticas (acumuladas entre sus diferentes versiones) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas. Esto requerimiento deberá ser sustentando con documentación publica en Internet del fabricante.		
Funcionalidades de Red	Debe soportar redundancia de hasta 03 enlaces de distintos proveedores ISP (Internet Service Provider) redundantes, sin la necesidad de una licencia adicional o software/hardware de terceros. La redundancia de ISP puede ser a nivel de "compartición de carga" (load sharing) y detección de falla enlace (primary/backup).		
Control de Aplicaciones y URL Filtering	Solución debe soportar como mínimo 70 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, Botnets y/o Command and Control, Anonymizer, Hacking y Spyware/ Malicious Sites.		
Anti-Bot y/o Antispyware / DNS Security	La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA) y DNS Tunneling, empleando protección basada en Machine Learning. Estas funcionalidades deben emplear las fuentes de inteligencia de amenazas en nube del propio fabricante.		
	La solución debe tener una capa de protección DNS para ataques del tipo Non-Existent Domain (NXNS) Attack y también protección de protocolo DNS sobre HTTPS (DoH).		
Prevención de Amenazas	Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en el repositorio la clasificación y/o reputación de direcciones IP, Dominios, URL, redes de Comando y Control y ataques DoS.		
	Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), Mail (SMTP o POP3), SMB y FTP		
VPN IPSec	Deben soportar encriptación AES-128 y AES-256 para las fases I y II de IKE. Deben soportar integridad en MD5, SHA1, SHA-256, SHA-512, AES-XCBX para las fases I y II de IKE		

7.1.4: Solución de Seguridad Next Generation Firewall Tipo IV

Marca y/o Fabricante:

Modelo:

DESCRIPCIÓN	CARACTERÍSTICAS QUE SE DEBEN ACREDITAR	CUMPLE / NO CUMPLE	N.º DE FOLIO /Pag. / Enlace URL
Rendimiento	Rendimiento (throughput) en prevención de amenazas de 500 Mbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, URL Filtering (opcional), IPS, Antivirus y/o Antimalware, Anti-Bot y/o DNS Security y Emulación Malware día-cero con log habilitado.		
	Rendimiento (throughput) en NGFW de 950 Mbps (medido con Capacidades habilitadas de: Firewall y Control de Aplicaciones		
	Conexiones Concurrentes: 1'000,000 sesiones o conexiones concurrentes, o 300,000 de sesiones o conexiones concurrentes en caso se analice a través de transacciones HTTP.		
	Conexiones por segundo: 15,000 conexiones o sesiones por segundo, o 10,000 de conexiones o sesiones por segundo en caso se analice a través de transacciones HTTP.		
Consideraciones Generales	En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan publicado y/o anunciado el "End-of-life" y/o "End-of-Support", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos. Esto requerimiento deberá ser respaldado con una carta del fabricante adjuntando la documentación publica de Internet que la respalde.		
	Las versiones de sistema operativo y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) altas o críticas (acumuladas entre sus diferentes versiones) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas. Esto requerimiento deberá ser sustentando con documentación publica en Internet del fabricante.		
Funcionalidades de Red	Soporte de rutas estáticas, IPSec Routing, RIP, OSPFv2 y OSPFv3(IPv6), IGMP, PIM SM, PIM DM PIM SSM, BGP, EBGp Multihop y IPv6 BGP-4		
Control de Aplicaciones y URL Filtering	Solución debe soportar como mínimo 70 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, Botnets y/o Command and Control, Anonymizer, Hacking y Spyware/ Malicious Sites.		
Anti-Bot y/o Antispyware / DNS Security	La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA) y DNS Tunneling, empleando protección basada en Machine Learning. Estas funcionalidades deben emplear las fuentes de inteligencia de amenazas en nube del propio fabricante.		
Prevención de Amenazas	Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en el repositorio la clasificación y/o reputación de direcciones IP, Dominios, URL, redes de Comando y Control y ataques DoS.		
VPN IPSec	Deben soportar encriptación AES-128 y AES-256 para las fases I y II de IKE. Deben soportar integridad en MD5, SHA1, SHA-256, SHA-512, AES-XCBX para las fases I y II de IKE		
Prevención de Amenazas Desconocidas o de Día Cero	La solución debe ser capaz de emular los archivos identificados en el firewall de forma automática, a través del envío y posterior análisis en la nube del propio fabricante de la solución de firewall para la Emulación de Malware (SandBox). La nube de emulación de amenazas del fabricante debe tener certificación SOC2 Tipo II.		
	El motor de emulación debe analizar y emular los URL contenidos en documentos Microsoft Office y PDF, para detectar y prevenir descargas maliciosas de malware.		

7.1.5: Consola de Administración de Firewalls.

Marca y/o Fabricante:

Modelo:

CARACTERISTICAS QUE SE DEBEN ACREDITAR	CUMPLE / NO CUMPLE	N.° DE FOLIO /Pag. / Enlace URL
La consola de administración debe ser ofrecido en modalidad SaaS, en la nube del propio fabricante de los firewalls ofertados.		
Los servicios de nube SaaS provistos por el fabricante deben cumplir con la certificación SOC 2 Type II		
Capacidad de almacenamiento y/o indexación de 70 Gb por día, con una retención mínima de 03 meses en línea		
Debe tener capacidad de revisión histórica de políticas, identificando las revisiones y cambios que fueron instalados y quien realizó los cambios. Debe tener capacidad de revertir a una versión específica de política		
La herramienta debe permitir sesiones concurrentes de diferentes usuarios o dispositivos para los cambios de políticas		
La herramienta debe permitir la creación de perfiles de administradores, basados en roles, que accedan a secciones parciales de administración o a la totalidad, indicando también si los perfiles son de solo lectura o lectura/escritura		
Debe contar con un módulo de cumplimiento basado en estándares internacionales, para la evaluación de la configuración y política de seguridad de los firewalls implementados. Esta evaluación debe comparar en base los siguientes estándares regulatorios como mínimo: ISO27001:2022, ISO27002:2022, NIST 800-41, NIST 800-53 y Cobit 5.0. En caso el fabricante no cuente con esta funcionalidad, el portor podrá ofertar una herramienta externa, licenciada para todos los firewalls, que cumpla con dichas características.		
La consola de administración deberá estar alojada en nube provista por el fabricante de la solución ofertada y el acceso a consola de administración en nube debe soportar doble factor de autenticación (MFA) a través de Google Authenticator y Microsoft Authenticator		
El acceso a consola de administración en nube debe soportar integración con proveedores de identidad (IdP) tales como: Microsoft Azure AD (Entra ID), Google Workspace, Okta, DUO y otros adicionales basados en SAML.		

7.1.6: Correlación de Eventos, Logs y Reportes de Firewalls.

Marca y/o Fabricante:

Modelo:

CARACTERISTICAS QUE SE DEBEN ACREDITAR	CUMPLE / NO CUMPLE	N.° DE FOLIO /Pag. / Enlace URL
La consola de correlación de eventos, Logs y reportes debe ser ofrecido en modalidad SaaS, en la nube del propio fabricante de los firewalls ofertados.		
Los servicios de nube SaaS provistos por el fabricante deben cumplir con la certificación SOC 2 Type II		
Capacidad de almacenamiento y/o indexación de 70 Gb por día, con una retención mínima de 03 meses en línea		
Debe tener capacidad de revisión histórica de políticas, identificando las revisiones y cambios que fueron instalados y quien realizó los cambios. Debe tener capacidad de revertir a una versión específica de política		
Los logs de emulación de malware del firewall deben estar tener información detallada de los ataques, exponiendo las técnicas y tácticas de MITRE ATT&CK que fueron empleadas y revisar los incidentes de seguridad de la red de una manera que se expongan las principales técnicas y tácticas utilizadas por los atacantes. Debe tener la capacidad de realizar búsqueda en base a técnicas o tácticas específicas		
Debe tener una vista de la emulación de amenazas, indicando el número de archivos maliciosos prevenidos, top de fuentes origen y número de archivo maliciosos descargados		
Debe tener una vista de los ataques detectados, con la siguiente información: <ul style="list-style-type: none"> e. Número de host en la red infectados con malware. f. Top de conexiones maliciosas de Command and Control, IP del sitio de C&C y número de conexiones, dirección IP origen. g. Número de ataques prevenidos. h. Número de archivos maliciosos bloqueados 		

7.2. Solución de Firewall de Aplicaciones Web – WAF

Marca y/o Fabricante:

Modelo:

DESCRIPCIÓN	CARACTERÍSTICAS QUE SE DEBEN ACREDITAR	CUMPLE / NO CUMPLE	N.º DE FOLIO /Pag. / Enlace URL
Características Generales Funcionalidades para la protección Anti-bot	Se requiere una solución para la protección automatizada de aplicaciones web y API, la misma debe incorporar las siguientes tecnologías de protección. <ul style="list-style-type: none"> • Web Application Protection • API Security • Bot Prevention • Intrusion Prevention (IPS) (opcional). • File Security y/o Antimalware • Prevencion DDoS 		
	La solución deberá brindar en conjunto una protección de al menos 180 Millones de solicitudes HTTP/S Web Request por año, y no debe tener un límite en la cantidad de aplicaciones y/o subdominios a ser protegidas. En caso la solución proteja a nivel de tráfico, se deberá considerar una capacidad mínima de protección de 1.5 Gbps de tráfico limpio hacia la entidad.		
Funcionalidades para la seguridad de archivos (File Security o Antimalware)	La solución debe contar con un motor de análisis de archivos maliciosos, que eviten que se carguen archivos maliciosos en los servidores de la organización. El motor de seguridad de archivos escanea el tráfico HTTP que ingresa a la organización		
	La solución debe proteger contra archivos maliciosos en formatos comprimidos en el tráfico HTTP entrante, analizando su contenido extraído, como mínimo en: ZIP, RAR, TAR y 7Z.		
Funcionalidades para la seguridad WEB	La solución deberá ser capaz de configurar reglas custom para poder aceptar (Accept), rechazar (drop) y exceptuar análisis (skip) en el tráfico web, empleando operadores lógicos (and, or) y condiciones tales como igual (equals), no igual (not equals) y existe (exists) entre las diversas reglas creadas, de acuerdo a lo siguientes parámetros: URI, IP Origen (source IP), Identificador de Origen (XFF, Header Key, JWT Key, Cookie, Source IP), Nombre de parámetro (expresión regular en el HTTP Reques o JSON File), Valor de parámetro (expresión regular en el HTTP Reques o JSON File), Código o Nombre de País (Ej. PE para el caso de Perú - geolocalización), Método HTTP (GET, POST, PUT, DELETE, PATC), Valor de Header (expresión regular) y Nombre de Header (expresión regular).		
Funcionalidades para la protección Anti-bot	La solución deberá poder inyectar scripts en páginas de aplicaciones web, como páginas de inicio de sesión o utilizar algún otro mecanismo para recopilar datos sobre patrones de entrada y canalice secuencias de pulsaciones de teclas, movimientos del ratón y toques con los dedos. Esto con el fin de poder diferenciar a un humano de un bot		
	La solución debe poder detener el relleno de credenciales (credential stuffing), los ataques de fuerza bruta y el site scraping con la protección avanzada de bots.		

7.3. Solución de Seguridad de nube Google Workspace

Marca y/o Fabricante:

Modelo:

DESCRIPCIÓN	CARACTERÍSTICAS QUE SE DEBEN ACREDITAR	CUMPLE / NO CUMPLE	N.º DE FOLIO /Pag. / Enlace URL
Características Generales Funcionalidades para la protección Anti-bot	El servicio debe operar desde la propia nube del fabricante de seguridad e integrarse de manera nativa y con capacidad de prevención en línea (in-line) mediante tecnologías API, con la nube del proveedor de servicios de correo electrónico (Google Workspace). No se aceptarán soluciones basadas en "Security Email Gateway" o similares, y no debe ser necesario ningún cambio disruptivo en el servicio de correo, tales como cambios de registro DNS (MX) para envío del correo a plataformas externas, relay SMTP o cualquier otra modificación a nivel de tráfico SMTP antes de que ingrese a la nube del Google Workspace		
	La solución deberá proporcionar protección contra los siguientes ataques cibernéticos: Amenazas de Phishing y Spam, Detección de Malware no conocido de "día cero" en correo electrónico de Google Workspace mediante emulación de amenazas (Sandboxing), Extracción de amenazas (CDR) (opcional), Reputación y Emulación de URLs maliciosas, Reescritura URLs para protección de phishing de día-cero, Protección contra ataques de Phishing basado en códigos QR, Identificación y alerta del uso de aplicaciones SaaS públicas no autorizadas, Detección de anomalías de usuarios y prevención de robo de cuentas, Protección contra archivos protegidos o cifrados con contraseña y Prevención de Fuga de Información – DLP.		
Capacidades requeridas de prevención de malware y phishing en Google Workspace Funcionalidades para la seguridad WEB	La solución deberá emplear algoritmos entrenadas de Inteligencia Artificial para identificar phishing avanzado o phishing de día-cero y compromiso en el correo electrónico (Business Email Compromise), tanto en el tráfico de correo entrante, saliente e interno		
	La solución debe tener la capacidad de ejecutar emulación de amenazas (Sandboxing) en la propia nube del fabricante, para identificar y prevenir de archivos maliciosos en los correos electrónicos. La capacidad de Sandboxing debe ser resistente a malware que intente realizar evasión por CPU. Las capacidades de antimalware deben poder analizar todos los archivos que ingresan en el flujo de correo en la nube de Google Workspace, tanto para malware conocido (motor antivirus) y malware no conocido o malware de día-cero empleando emulación (Sandbox) en la propia nube del fabricante		
	La solución debe tener capacidad de reescritura de URLs para prevenir el phishing conocido y no conocido (phishing de día-cero). Debe tener las siguientes acciones: Reemplazar los enlaces URL en el cuerpo del correo electrónico y en los archivos adjuntos (Microsoft Office y Adobe PDF), La capacidad de reemplazo de enlaces URL debe operar tanto en reputación URL, como en emulación de URL (URL Sandbox) para detectar sitios web de phishing de día cero, Debe tener capacidad forense. Debe registrar el momento que el usuario hace clic en el enlace reemplazado, Sobre cada correo donde se reemplazaron los enlaces, debe tener la capacidad de ver los enlaces reemplazados, y la actividad del usuario sobre esos enlaces (User Clicks) y la inspección de los enlaces URL, debe ser tanto basado en reputación (Se sabe que la URL es maliciosa o contiene referencias maliciosas), como en emulación (Emula el sitio web URL para detectar phishing de día cero).		
Capacidades requeridas de detección de comportamiento anómalo para identificar robo o compromiso de cuentas en Google Workspace	Debe analizar el comportamiento, utilizando un algoritmo de aprendizaje automático, para crear un perfil basado en eventos históricos que incluyen ubicaciones y horas de inicio de sesión, comportamiento de transferencia de datos y patrones de mensajes de correo electrónico.		
	La solución deberá detectar anomalías del comportamiento todos los usuarios de Google Workspace, tales como: <ul style="list-style-type: none"> Detección de comportamiento anómalo basado en motor de Inteligencia Artificial (AI). Geolocalización, detecta si el usuario ha iniciado sesión de sitios distantes geográficamente en un corto tiempo. Detecta si el usuario ha iniciado sesión en un país, en el cual nunca se había iniciado sesión antes. Detecta si el usuario ha iniciado sesión desde una dirección IP pública que sea categorizada como maliciosa o como fuente de envío de correos phishing. Correo electrónico inusual, detecta si el usuario tiene reglas de correos electrónicos que podrían indicar una intención maliciosa. Auto reenvío a correo externos, cuando se crean reglas de reenvío hacia dominios externos. Fallas de autenticación de multi-factor MFA, analizando el número de eventos fallidos y satisfactorios de un usuario, para reducir la tasa de falsos-positivos. Anomalía de restablecimiento de contraseña, detecta cuando un usuario ha recibido tres o más correos de restablecimiento de contraseña diferentes en un periodo corto de tiempo. 		

DESCRIPCIÓN	CARACTERÍSTICAS QUE SE DEBEN ACREDITAR	CUMPLE / NO CUMPLE	N.º DE FOLIO /Pag. / Enlace URL
	<p>Si se logró validar a través de los motores de anomalías, que la cuenta de un usuario está comprometida, la solución debe permitir tomar remediación desde la propia consola donde se registran los eventos anómalos, mediante las acciones de:</p> <ul style="list-style-type: none"> • Bloquear la cuenta del usuario comprometido (flujo de remediación automático). • Poner en lista negra todos los correos salientes de la cuenta comprometida (flujo de remediación automático). • Restablecimiento de la contraseña de una cuenta de usuario (flujo de remediación manual). • Desbloquear una cuenta de usuario bloqueada (flujo de remediación manual). • Restablecer contraseña y desbloquear una cuenta de usuario bloqueada. 		
Prevención de Fuga de Información - DLP	La solución debe ser capaz de escanear correos electrónicos y archivos en busca de información confidencial para prevención de fuga de información (DLP).		
	prevención de fuga en base palabras claves o diccionarios, y en base a Expresiones Regulares (RegEx) en el correo, esta característica también se empleará para las expresiones regulares en el asunto del correo		
	Debe permitir crear tipos de datos (data types) personalizados basados en expresiones regulares y diccionarios. Los diccionarios pueden ser importados desde archivos CSV		

7.4. Servicio de Inteligencia de Amenazas y Automatización

Marca y/o Fabricante:

Modelo:

CARACTERISTICAS QUE SE DEBEN ACREDITAR	CUMPLE / NO CUMPLE	N.º DE FOLIO /Pag. / Enlace URL
La solución de Inteligencia de Amenazas debe ser ofertada en modalidad SaaS. Esta solución debe almacenar y correlacionar todos los registros (logs) de seguridad de las herramientas ofertadas: Firewall NGFW Tipo I, II, III y IV, y de la solución de protección de Correo para Google Workspace.		
La solución de Inteligencia de Amenazas debe tener capacidad de respuesta, integrada a través de API y/o a través de IoC (indicadores de compromiso), con las soluciones ofertadas. Debe contar detecciones basadas en Advanced User Entity Behavioral Analytics (UEBA).		
Debe crear incidentes de seguridad, donde un incidente, es una colección de eventos de uno o más productos que juntos representan una historia de ataque. Para ellos, debe utilizar la inteligencia artificial (IA) y aplicar modelos de aprendizaje automático (ML) para correlacionar los eventos de los productos integrados (eventos benignos y de seguridad) en incidentes unificados		
Debe permitir crear respuesta automática en base al nivel de confianza y severidad de los indicadores de compromiso (IoC) sobre la base de cada uno de los incidentes, para que estos puedan ser habilitados en el gestor de IoC y su posterior aplicación automática en las soluciones ofertadas tales como: Firewall NGFW Tipo I, II, III y IV, de la solución Web Application Firewall y de la solución de protección de Correo para Google Workspace.		
Las capacidades de análisis de cada incidente deben permitir tener una vista detallada de: <ul style="list-style-type: none"> • Información y análisis forense para ver procesos, archivos, URL, dominios y registros involucrados en la información y relacionados con el incidente. • Indicadores (IoC) y artefactos para ver los indicadores y artefactos relacionados con el incidente. • Árbol de ataque para ver una representación gráfica del informe forense generado por la solución de Endpoint para cada detección realiza. • MITRE para conocer las tácticas MITRE ATT&CK utilizadas en el incidente. 		

II REQUISITOS DE CALIFICACION

B	CAPACIDAD TECNICA Y PROFESIONAL
B.3	CALIFICACIONES DEL PERSONAL CLAVE
B.3.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>Para el Jefe de proyecto</p> <ul style="list-style-type: none"> Ingeniero TITULADO en las carretas de Electrónica y/o Eléctrica y/o Telecomunicaciones y/o informática y/o sistemas y/o computación y sistemas del personal clave requerido como Jefe de proyecto. <p>Para el Supervisor de Operaciones</p> <ul style="list-style-type: none"> Ingeniero TITULADO en las carretas de Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería de Telecomunicaciones. <p>Para el/los Especialistas en Seguridad</p> <ul style="list-style-type: none"> Técnico titulado o bachiller en las carreras de Electrónica, Informática y de Sistemas, o en Telecomunicaciones, o en Redes y Comunicaciones de Datos, o Sistemas, o Informática, o de Sistemas de Información, o de Seguridad y Auditoría informática o de Software o Empresarial. <p>Para el Especialista Residente</p> <ul style="list-style-type: none"> Técnico titulado o bachiller en las carreras de Electrónica, Informática y de Sistemas, o en Telecomunicaciones, o en Redes y Comunicaciones de Datos, o Sistemas, o Informática, o de Sistemas de Información, o de Seguridad y Auditoría informática o de Software o Empresarial. <p><u>Acreditación:</u> EI GRADO o TÍTULO¹⁰, será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link http://www.titulosinstitutos.pe/, según corresponda.</p> <p>En caso el TÍTULO no se encuentre inscrito en los referidos registros, el postor deberá presentar copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
B.4	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>Para el Jefe de proyecto – Personal clave</p> <ul style="list-style-type: none"> Debe contar con una experiencia de tres (03) años como mínimo Gestión de Proyectos de TI y/o Proyectos de Seguridad Perimetral. Del personal clave requerido como Jefe de proyecto. <p>Para el Especialista en Seguridad</p> <ul style="list-style-type: none"> Debe contar con una experiencia de dos (02) años como mínimo Implementador de soluciones de seguridad y/o ciberseguridad. Del personal clave requerido como Especialista en Seguridad <p>Para el Supervisor de Operaciones</p> <ul style="list-style-type: none"> Debe contar con una experiencia de dos (02) años como mínimo Encargado y/o supervisor de Centro de Operaciones de Seguridad (SOC). Del personal clave requerido como Supervisor de Operaciones

¹⁰ En el caso de que el postor oferte Ingenieros para el presente servicio deberá tener en cuenta lo siguiente: En concordancia con el artículo No 1 de la Ley 28858, los Ingenieros, deberán estar colegiados y encontrarse habilitados por el Colegio de Ingenieros del Perú para el ejercicio profesional. En ese sentido, la colegiatura y habilitación de los profesionales se requerirá para el inicio de su participación efectiva en el contrato, tanto para aquellos titulados en el Perú o en el extranjero, y no en un momento anterior

Para el Especialista Residente

- Debe contar con una experiencia de **dos (02) años** como mínimo:
- Administrador de soluciones de seguridad y ciberseguridad. Del personal clave requerido como **Especialista Residente**

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Importante

- *Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.*
- *En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.*
- *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*
- *Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.*

C

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a **S/ 6'000,000.00 (Seis millones con 00/100 soles)**, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes:

- Servicios de ciberseguridad
- Servicios de seguridad perimetral
- Servicios de licenciamiento o seguridad gestionada
- Servicios y/o adquisición de soluciones de seguridad perimetral y/o Firewall y/o seguridad gestionada.
- Servicio de Soporte y Mantenimiento al equipo de seguridad Firewall

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago¹⁰, correspondientes a un máximo de veinte (20) contrataciones.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo** correspondiente referido a la Experiencia del Postor en la Especialidad.

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo correspondiente**.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo correspondiente** referido a la Experiencia del Postor en la Especialidad.

Importante

- *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.*
- *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*



"Esta es una copia auténtica imprimible de un documento electrónico archivado por el OEFA, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. N° 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sistemas.oefa.gob.pe/verifica> e ingresando la siguiente clave: 05525491"



05525491