TÉRMINOS DE REFERENCIA

CONTRATACION DEL SERVICIO DE ALQUILER DE SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED-FIREWALL PARA LA SEDE DE SAN ISIDRO

1. ÁREA USUARIA Y/O ÁREA TÉCNICA ESTRATÉGICA

Oficina de Sistemas

2. FINALIDAD PÚBLICA

Se requiere contratar el Servicio de alquiler de sistema de protección y seguridad para red – Firewall, con la finalidad de garantizar la seguridad, integridad y confidencialidad de su infraestructura tecnológica y de las comunicaciones de la sede San Isidro. Este servicio tiene como fin implementar un mecanismo avanzado de defensa perimetral que mitigue riesgos frente a ciberamenazas, accesos no autorizados y vulnerabilidades informáticas.

La contratación permitirá la protección de los activos digitales institucionales, el tráfico de datos seguro y la disponibilidad de los servicios informáticos, garantizando la continuidad operativa de la entidad y resguardando de forma óptima la información crítica que soporta la atención oportuna y eficiente a los ciudadanos.

3. OBJETO DE LA CONTRATACIÓN

Contratar el servicio de alquiler de un sistema de protección y seguridad para red Firewall para la Sede de San Isidro, con el objetivo de preservar la continuidad operativa de los servicios que COFOPRI brinda a la ciudadanía.

Los sistemas de información institucional están expuestos a diversas vulnerabilidades y amenazas provenientes del ciberespacio, por lo que contar con una solución robusta de seguridad perimetral permitirá proteger eficazmente los servicios digitales, garantizar la integridad de los datos y fortalecer la infraestructura tecnológica de la entidad.

4. ACTIVIDAD DEL POI

- **ACTIVIDAD PRESUPUESTAL:** Gestión Administrativa
  - **ACTIVIDAD OPERATIVA:** C0091 “ATENCIÓN DE LA CONTINUIDAD Y OPERATIVIDAD AL DATA CENTER”
  - **SECUENCIA FUNCIONAL:** 125

5. ALCANCES Y DESCRIPCIÓN DE LA CONTRATACIÓN

5.1. CARACTERÍSTICAS MÍNIMAS QUE DEBE TENER EL EQUIPO:

El Contratista deberá proveer dos (02) Equipos Firewall de nueva generación de la misma marca y modelo, los cuales deberán ser implementados en un esquema de Alta Disponibilidad (HA - High Availability) en modo Activo/Pasivo, para garantizar la tolerancia a fallos y la continuidad operativa del servicio de manera automática y sin intervención manual.

5.1.1. Requisitos del Next Generation Firewall:

- Cada uno de los dos (02) dispositivos de la solución de alta disponibilidad deberá ser de propósito específico tipo appliance, no serán aceptables servidores de propósito genérico, el equipo deberá encontrarse licenciado durante la vigencia del servicio.
  - La solución ofertada debe contar con Efectividad de Seguridad superior al 98%, ello respecto al último reporte de Miercom NGFW Security Benchmark 2024.

- El appliance deberá utilizar procesadores de arquitectura de 64 bits desarrollados por el fabricante o de propósito específico para funciones de seguridad (ASIC, SoC, ARM o x86), optimizados para procesamiento de tráfico y protección avanzada.
- El dispositivo debe contar con fuentes de poder redundantes con la capacidad de funcionamiento 110-240 AC.
- La solución deberá contar con almacenamiento local para logs, reportes y archivos de configuración de al menos 512 GB SSD o tecnología equivalente provista por el fabricante.
- El sistema operativo deberá ser propietario del fabricante, endurecido (hardened) y mantenido por éste durante la vigencia del servicio.
- Se requiere que el dispositivo cuente como mínimo:
  - Una (01) interfaces para WAN 10/100/1000 Base-T RJ45, para conectividad a internet.
  - Dos (02) interfaces para conexión a LAN a 2.5 Gbps RJ45 Multi-gigabit
  - Cuatro (04) interfaces de fibra SFP+ (10 Gbps)
  - Ocho (08) puertos 10/100/1000 Base-T RJ45 como mínimo.
  - Un (01) puerto consola tipo USB o USB-C, o RJ45
- Las interfaces Ethernet deben permitir ser utilizadas también como puertos independientes y/o agrupados con las siguientes características:
  - Interface modo switch.
  - Interface modo bridge.
  - Interface modo vlan.
  - Interface modo alias.
  - Interface modo túnel
  - Interface modo bond o Link Aggregation.
- Las interfaces Ethernet deben:
  - Permitir habilitar un servidor DHCP IPv4
  - Deberá poder permitir excluir un rango de IP’s o actuar como un DHCP Relay
  - Asignar tres (3) DNS Servers
  - Asignar el default Gateway
  - Modificar el tiempo de asignación de IP
  - Asignar dos servidores NTP
  - Asignar el dominio de DHCP
  - Debe permitir como medida de seguridad asignar IP’s a objetos de host creados asociados a una Mac Address.
- Poder modificar el tamaño de MTU.
- El dispositivo deberá poder hacer ruteo estático IPv4.
- El dispositivo deberá tener un filtro de acceso a la red mediante una lista blanca de Mac address.
- El Dispositivo deberá poder actuar como un DNS Proxy.
- El dispositivo ofertado deberá tener las siguientes capacidades de procesamiento de trafico medido con trafico real de producción:
  - Threat Prevention mínimo 2.8 Gbps, que incluya módulo de Firewall, Application control, URL Filtering, IPS, Antivirus, Anti-Bot o Anti-Spyware y Sandboxing.
  - IPS mínimo 5 Gbps.
  - Firewall mínimo 20 Gbps.
- Capacidades de manejo de procesamiento de trafico de VPN y conexiones:
  - VPN AES-128 05 Gbps.
  - Conexiones por segundo 90,000
  - Conexiones concurrentes 3,000,000
- El dispositivo deberá poder actualizarse el firmware/sistema operativo mediante la interface gráfica de administración, pudiendo hacer una actualización cargando el firmware de manera manual (offline) y tener opción a regresar a la versión anterior.

- El firmware/sistema operativo deberá ofrecer un mecanismo de backup de configuración el cual podrá ser manual y/o automático con backups programados, pudiendo ser estos colocados de manera automática en un servidor ftp autenticado, los backups deberán poder cifrarse utilizando cifrado de archivos, los backups deberán poder ser programados diario, semanal o mensual en horarios específicos. El equipo deberá poder ofrecer un mecanismo de recuperación de backup mediante la interface gráfica.

5.1.2. Funciones base de Firewall:

- La solución deberá permitir operar bajo políticas de seguridad predeterminadas y políticas personalizadas, incluyendo la posibilidad de denegar todo el tráfico por defecto y permitir únicamente el tráfico autorizado mediante reglas
- La solución deberá ser capaz de limitar el consumo de ancho de banda de los aplicativos, tanto de download como upload.
- El equipo deberá poder hacer reglas de NAT para publicación de servidores utilizando PAT y siendo esto configurado de manera manual y mediante un asistente de configuración, indicando el tipo de servidor y su puerto de publicación.
- El IPS debe permitir la captura de paquetes, para propósitos forenses, para firmas específicas
- Debe tener soporte de Kerberos (principalmente en Directorio Activo), para poder realizar procesos de autenticación transparente y garantizar Single Sign- On.
- La solución debe ser capaz construir reglas de Filtrado URL, que involucren varias categorías de forma simultánea.
- La solución debe permitir tener reglas que involucren usuarios y grupos de estos en las políticas de navegación y/o uso de aplicaciones.
- La solución debe categorizar aplicaciones y URL por un Factor de Riesgo.
- La Solución debe proveer un mecanismo que permita re-categorizar los sitios WEB.
- La solución provista, debe tener integrados servicios de protección contra ataques bot, y antivirus/antimalware.
- El componente de control de Bots, debe tener la capacidad de detectar y detener, eventos anormales a nivel de red.
- Los componentes de Control de Bots y AntiMalware, deben tener la capacidad de evitar ataques de Spear Phishing.
- El antivirus debe tener la capacidad de inspeccionar malware en tráfico cifrado SSL.
- El antivirus debe ser capaz de escanear archivos descargados.
- El antivirus será capaz de inspeccionar tráfico pasando por el protocolo CIFS (carpetas compartidas), entre vlans de servidores y usuarios.
- La solución debe detectar comunicaciones hacia sitios de comando & control, basados entre otros en direcciones IP, URL & Reputación de Dominios.
- La solución debe actuar en modo prevención, en caso de malware paciente ‘0’ (cero) en los procesos de navegación.
- La solución debe tener la capacidad de emular archivos Office (doc, docx, ppt, pptx, dot, xls,) archivos de empaquetamiento (tar, 7z, zip, gz)
- La base de datos de aplicaciones y URLs debe ser actualizado por un servicio basado en Nube.
- La solución de filtrado de aplicaciones y URLs, debe permitir excepciones de red en su configuración, sin aumentar el número de reglas de control.
- La solución debe contar con funcionalidad de MAC Filtering.

- La solución deberá incorporar mecanismos de detección y prevención de ransomware mediante análisis de comportamiento, inteligencia de amenazas, detección de Command & Control (C2), bloqueo de cifrado malicioso y análisis de archivos desconocidos utilizando sandboxing en la nube y/o local.
- La solución deberá contar con DNS Security que permita detectar dominios maliciosos, dominios recién creados (Newly Registered Domains), dominios generados mediante algoritmos (DGA), DNS Tunneling y conexiones hacia infraestructura de Command & Control.
- La solución deberá soportar Deep SSL Inspection para tráfico TLS 1.2 y TLS 1.3, permitiendo inspección selectiva por categorías, aplicaciones, usuarios o certificados.
- La solución deberá incorporar mecanismos de protección frente a ataques DoS y DDoS de capa 3, 4 y 7, incluyendo SYN Flood, UDP Flood, ICMP Flood, HTTP Flood y ataques volumétricos.
- La solución deberá permitir bloquear tráfico por país (Geo-IP Filtering). Debe poder bloquear:
  - IOC
  - IP
  - SHA256
  - dominios
  - URL
  - certificados
  - CVE
  - explotación
  - riesgo
  - MITRE ATT&CK
  - Todo cambio deberá: Documentarse aprobarse contar con plan de reversa .

- El contratista deberá ejecutar el servicio alineado con los controles de la Norma ISO/IEC 27001:2022 e ISO/IEC 27002:2022 relacionados con control de acceso, gestión de vulnerabilidades, registros de auditoría, continuidad del negocio, gestión de incidentes, administración segura de cambios y protección de la información.

- El contratista realizará una revisión trimestral de:
  - reglas obsoletas
  - reglas duplicadas
  - reglas shadow
  - reglas sin uso
  - optimización
- La solución deberá incluir, durante toda la vigencia del servicio, el licenciamiento original del fabricante que habilite la totalidad de las funcionalidades de seguridad ofertadas, incluyendo como mínimo los servicios de prevención de intrusiones (IPS), control de aplicaciones, filtrado web, antivirus, antimalware, protección contra botnets, reputación de IP y dominios, inteligencia de amenazas, análisis de archivos sospechosos mediante sandboxing (en la nube o local), protección frente a amenazas de día cero (Zero-Day), protección contra ransomware, inspección de tráfico cifrado (SSL/TLS), seguridad DNS (DNS Security), actualización automática de firmas y mecanismos de protección, así como cualquier otra funcionalidad necesaria para el correcto funcionamiento de la solución ofertada.

- El licenciamiento deberá ser emitido por el fabricante de la solución y mantenerse vigente durante toda la ejecución del contrato, incluyendo las actualizaciones del sistema operativo, firmware, firmas de seguridad, bases de reputación e inteligencia de amenazas, sin generar costos adicionales para la Entidad.

5.1.3. Administración y manejo de identidades:

- El equipo deberá poder ofrecer la integración con Microsoft Active Directory, dicha configuración deberá ser mediante un asistente de configuración.

5.1.4. Administración de Firewall:

- El fabricante deberá ofrecer una consola cloud desde la cual poder administrar el appliance solicitado.
- El equipo deberá ofrecer la posibilidad de ser administrado de forma central mediante una consola central en premisas o con opción a consola Cloud.
- El equipo deberá ofrecer el poder crear múltiples administradores los cuales podrán administrar el equipo de manera simultánea únicamente bloqueando los objetos que un administrador tenga en uso.
- El equipo deberá ofrecer por lo menos cuatro (04) roles de administración, modo de acceso completo, modo de administrador de red, modo lectura para auditores y modo de administración móvil.

5.1.5. Soportar la entrega de logs, monitoreo, alertas y reporteria:

- La solución ofertada deberá presentar los logs de manera separada en donde se muestren logs de sistema en un apartado diferente a los logs de seguridad, para un mejor y pronto análisis.
- Debe contar con una consola para identificar actividades sospechosas, rastrear tendencias e investigar y mitigar eventos de seguridad, a través de plantillas gráficas y reportes.
- Debe tener capacidad de mitigación (reacción) automatizada, en base a los eventos de seguridad identificados. Las capacidades deben ser tales como:
  - Enviar un correo electrónico de alerta, bloquear por política la IP origen o múltiples IP Origen (ataque distribuido) relacionados al evento de seguridad en una ventana de tiempo configurable y generar un SNMP Trap.
- Debe permitir exportar en formato XLSX o PDF los reportes generados.
- El sistema de reportes debe proveer información consolidada sobre al menos:
  - Eventos por Origen, Destino o Usuario.
  - Eventos en una línea de tiempo.
  - Lista de ataques por severidad y producto.

El equipo a instalar debe ser encontrarse en vigencia tecnológica y no estar catalogado como EOL y EOS, asimismo, el modelo de equipo debe ser de la última versión de hardware disponible por el fabricante.

El equipo debe contar con la licencia que incluya una opción de sandboxing (cloud), que permita la protección contra ransomware, amenazas de día cero y nuevo tipo de malware.

El equipo debe contar con la licencia para la conexión a través de VPN para ciento veinte (120) usuarios conectados en simultáneo como mínimo, configurado con autenticación de doble factor (2FA), que permita al personal realizar el trabajo remoto.
El Contratista deberá brindar dos (02) transceivers 10G SFP+ SR para el equipo firewall y dos (02) transceivers 10 SFP+ SR para la conexión al equipo Aruba 3810 (equipo de Cofopri) y sus respectivos patch cords OM3/OM4. En ambos casos deben ser compatibles y/o certificados para operar con los equipos mencionados.

5.2. CONSIDERACIONES GENERALES

- La entidad proporcionará el establecimiento de conexiones a nivel de comunicaciones para lograr el desarrollo del servicio de soporte y garantía, por parte del Contratista.
- El Contratista deberá asegurar el correcto funcionamiento físico y lógico del equipo de seguridad perimetral provisto, posterior al soporte técnico brindado.
- El Contratista deberá asegurar la continuidad del servicio, una vez realizado el soporte técnico, para la actualización de firmware, cambio de equipo físico y/o actualizaciones de la base de firmas del equipo de seguridad perimetral.
- El Contratista deberá presentar en su informe mensual, el detalle de las actividades realizadas durante el servicio de soporte y actualización del equipo.

5.3. PRESTACIONES ACCESORIAS

5.3.1. Soporte y Actualización

- El Contratista deberá de migrar las configuraciones del equipo del servicio actual CheckPoint cuya versión R81.10.15 (996003913) al equipo en alquiler, COFOPRI le brindara una copia de la configuración del equipo actual.
- El Contratista deberá verificar la configuración integral del equipo Firewall en alquiler, brindando recomendaciones para la seguridad perimetral de la red institucional, como soporte gestionado con ciberseguridad.

5.3.2. Del Soporte Técnico:

- Modalidad de Atención
  On-line vía telefónica, y mediante correo electrónico, cuando un incidente o solicitud no comprometa la continuidad del servicio.
  Soporte Presencial On-Site, cuando el incidente comprometa el correcto funcionamiento de los servicios, bajo riesgo para la seguridad de la información institucional.
- El soporte técnico debe contemplar la actualización del equipo de seguridad perimetral (Filtrado Web, Definición de Sistema de Prevención de Intrusión, control de aplicaciones, como mínimo), parches de software y firmware contra nuevas vulnerabilidades.
- Servicio es del tipo 24x7x365 (24 horas al día, los 7 días de la semana, los 365 días del año).
- El tiempo de respuesta deberá sujetarse a los niveles de servicio (SLA) establecidos.
- El tiempo de solución deberá cumplir los plazos establecidos en el SLA.
- El Contratista deberá registrar todas las incidencias y requerimientos atendidos durante la ejecución del servicio.
- El contratista deberá contar con un SOC (Security Operation Center), para la atención del soporte técnico.
- El tiempo de respuesta para incidentes y problemas con la continuidad del servicio, deberá estar de acuerdo a los niveles de servicio establecidos.

Características Mínimas del SOC:

Disponibilidad:
El Centro de Operaciones de Seguridad (SOC) deberá brindar atención y monitoreo continuo bajo un esquema de operación de veinticuatro (24) horas al día, siete (7) días a la semana y trescientos sesenta y cinco (365) días al año (24x7x365).

Capacidad Técnica: El SOC deberá contar con capacidad para realizar actividades de monitoreo, detección, análisis, gestión y

respuesta ante incidentes de seguridad de la información, con énfasis en la protección y seguridad perimetral objeto de la presente contratación.

Herramientas: El SOC deberá disponer de una plataforma de gestión de incidentes o mesa de ayuda (ticketing), que permita el registro, seguimiento, control, escalamiento y cierre de los incidentes de seguridad reportados o detectados durante la prestación del servicio.

- El contratista debe contar con un mecanismo o sistema de tickets para la atención y registro de incidentes o solicitudes. De tal forma que cuando reciba una notificación de solicitud o incidente el contratista, registrará y notificará un número de ticket a la entidad.

- Se considera incidente a todo evento o situación que afecte la operatividad, disponibilidad, desempeño o funcionalidad del equipo o de alguno de sus módulos e impida o degrade la prestación normal del servicio de seguridad.

- Un incidente puede originarse por causas de hardware, software, configuración, rendimiento o actualización. Asimismo, se clasifican como incidentes los siguientes casos:

    - Falla total o parcial del equipo que imposibilite el tráfico o análisis de las aplicaciones protegidas.
    - Degradación significativa del rendimiento o incremento anómalo de latencia.
    - Fallas en los módulos de protección.
    - Fallas en la comunicación.
    - Malfuncionamiento derivado de errores del firmware o sistema del equipo.

- El contratista deberá registrar, atender y resolver todo incidente reportado conforme a los tiempos de respuesta y resolución de acuerdo a la siguiente definición:

NIVELES DE SERVICIO SLA

El Contratista debe cumplir con los siguientes niveles de servicios (SLA):

Nivel de prioridad	Definición / impacto	Tiempo máximo de respuesta	Tiempo máximo de solución
Critico	Incidente que ocasiona la indisponibilidad total del firewall, pérdida de conectividad, interrupción de servicios institucionales o afectación a la seguridad de la información	Hasta quince (15) minutos contados desde la notificación del incidente o solicitud	Hasta dos (2) horas contadas desde la notificación del incidente.
Alto	Incidente que afecta funcionalidades críticas del firewall sin interrumpir totalmente la operación institucional.	Hasta treinta (30) minutos contados desde la notificación del incidente o solicitud	Hasta seis (6) horas contadas desde la notificación del incidente o solicitud

Medio	Incidente que afecta parcialmente funcionalidades del servicio, sin comprometer la continuidad operativa.	Hasta una (01) horas contadas desde la notificación del incidente o solicitud	Hasta doce (12) horas contadas desde la notificación del incidente.
Bajo	Requerimientos de configuración o asistencia técnica que no afectan la operación del servicio.	Hasta dos (02) horas contadas desde la notificación del incidente o solicitud	Hasta veinticuatro (24) horas contadas desde la notificación del incidente.

Mecanismo de Validación y Cierre de Incidentes:

Una vez resuelto el incidente, el contratista notificará inmediatamente al área usuaria por correo electrónico o plataforma de tickets para su validación; ante esto, el área usuaria evaluará el correcto funcionamiento y, de encontrarse conforme, emitirá la aprobación para el cierre definitivo del ticket; caso contrario, se rechazará la solución y el contratista deberá continuar con la atención de inmediato acumulando el tiempo de retraso.

- En caso exista un incidente donde el equipo de seguridad se encuentre inoperativo total o parcialmente, el soporte técnico será presencial.

- Se considera solicitud de servicio a todo requerimiento formal efectuado por personal autorizado de la Oficina de Sistemas orientado a la ejecución de actividades de administración, configuración, optimización o mejora del equipo de seguridad Firewall Perimetral.

- Entre otras, comprende la creación, modificación o eliminación de políticas y perfiles de protección, ajustes de configuración, activación o desactivación de funcionalidades, generación de reportes, análisis de seguridad, implementación de recomendaciones técnicas y demás actividades que no constituyan incidentes, pero que resulten necesarias para mantener, optimizar o fortalecer la seguridad de la infraestructura tecnológica.

- Toda modificación deberá ser autorizada por la Oficina de Sistemas, debidamente registrada en un ticket, y ejecutada por personal especializado del contratista, garantizando que los cambios no afecten la estabilidad o la continuidad del servicio.

- El contratista deberá realizar respaldos de la configuración del equipo, o parámetros críticos en coordinación con la Oficina de Sistemas, para facilitar restauraciones.

- El proveedor debe contar obligatoriamente con personal especialista y calificado para brindar de forma directa el soporte técnico del equipo, garantizando la disponibilidad, idoneidad y una rápida atención a los incidentes reportados por la Entidad.

- La Oficina de Sistemas designará a un representante para coordinar con el contratista en todo lo referente a las tareas administrativas que conlleven a la ejecución del servicio.

- El contratista deberá efectuar la actualización del firmware del equipo cada vez que el fabricante publique nuevas versiones y sean estables, o

en caso incluyan mejoras de seguridad, o para realizar la corrección de vulnerabilidades, u optimización del rendimiento o solución de errores (bugs) identificados y/o reportados por el mismo proveedor o por la Oficina de Sistemas.

- Dichas actualizaciones deberán realizarse en coordinación con la Oficina de Sistemas, sin afectar la disponibilidad del servicio, asegurando la compatibilidad con las configuraciones vigentes.

- La actualización del firmware deberá ejecutarse de manera presencial.

- El contratista deberá asegurar el correcto funcionamiento físico y lógico, del equipo posterior al soporte técnico brindado.

- COFOPRI proporcionará acceso físico y lógico al equipo para que el contratista realice los trabajos de actualización, soporte o sustitución.

- El contratista deberá asegurar la atención de incidentes o solicitudes que no han sido resueltas.

- El personal de soporte técnico que atenderá los incidentes y solicitudes deberá contar con conocimientos avanzados en la gestión, configuración y resolución de problemas en el equipo.

- El contratista deberá asegurar la continuidad del servicio, una vez realizado el soporte técnico, ya sea en la actualización de firmware, cambio de equipo físico, entre otros que realice.

5.4. GARANTÍA DEL SERVICIO:

La garantía es por el tiempo de vigencia del servicio.

6. REQUISITOS DEL PROVEEDOR Y/O PERSONAL

6.1. Del Proveedor:

- Ser persona jurídica
- Contar con RNP vigente (de corresponder).
- RUC activo y habido (el proveedor deberá contar con actividad económica relacionada al objeto de la contratación)
- Contar con cuenta interbancaria CCI afiliado al RUC.
- No deberá tener impedimento para contratar con el estado.

6.1.1. Experiencia:

El proveedor debe acreditar un monto facturado acumulado equivalente a S/.100.000,00 (cien mil 00/00 soles), por servicios iguales o similares al objeto de la convocatoria, durante los tres (03) 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:

- Servicio de Seguridad Perimetral Administrada
- Firewall como Servicio (FWaaS)
- Servicio de Protección de Red Corporativa
- Alquiler de Equipos de Seguridad de Red
- Servicio de Gestión de Firewall Empresarial
- Sistema de Prevención de Intrusiones (IPS) como Servicio
- Servicio de Filtrado Web y Control de Aplicaciones

- Monitoreo y Gestión de Seguridad de Red
- Protección de Infraestructura Tecnológica en Sede
- Servicio de Seguridad de Red para Oficinas Remotas

Acreditación:
La experiencia del proveedor 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 constancia 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 pago.

6.2. Del Personal

El contratista debe contar como mínimo un (01) especialista en soporte técnico.

Especialista – Soporte Técnico

Formación Académica	Grado de Bachiller y/o Título profesional en Ingeniería de Sistemas y/o Ingeniería Informática, y/o Ingeniería de Computación y/o Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial o carreras afines de las tecnologías de la información. **Acreditación:** Acreditar la formación académica con copia del grado académico u otro documento que demuestre fehacientemente lo solicitado.
Experiencia	Experiencia laboral mínima de un (01) año realizando soporte técnico y/o administración y/o implementación en firewall de la marca Ofertada. Acreditación: La experiencia será acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos o ordenes y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia, el cual deberá presentar en su propuesta económica).
Especialización	El especialista responsable del soporte técnico deberá contar con certificación vigente, emitida por el fabricante. Se acreditará mediante la presentación de copia simple del certificado vigente emitido por el fabricante del firewall ofertado.
Actividades a desarrollar	Se encargarán de la atención y solución de incidentes, así como de las solicitudes relacionadas con el objeto de la contratación, garantizando la continuidad operativa y el adecuado funcionamiento de la solución implementada.

7. LUGAR Y PLAZO DE EJECUCIÓN DEL SERVICIO:

7.1. LUGAR

El servicio se llevará a cabo en las instalaciones de COFOPRI, ubicada en la sede de San Isidro, en Av. Paseo de la República N° 3135, San Isidro 15047.

El soporte técnico se realizará de manera presencial y/o remota para las atenciones de incidentes o requerimientos de los servidores el cual el proveedor deberá considerar el despliegue de su personal sin generar ningún costo adicional al COFOPRI

7.2. PLAZO

El plazo de ejecución del servicio de alquiler será de doce (12) meses, contabilizados a partir del día siguiente de la culminación del contrato vigente, previa suscripción del Acta de Instalación e Inicio del Servicio

El contratista deberá realizar la instalación, configuración, migración, pruebas de funcionamiento y producción del equipo Firewall en un plazo máximo de diez (10) días calendario, contados a partir del día siguiente de la suscripción del contrato o de la notificación de la Orden de Servicio, según corresponda.

8. ENTREGABLE

El contratista deberá presentar un informe mensual que detalle las actividades realizadas en el marco del servicio para la sede de San Isidro, adjuntando el registro de las atenciones de soporte técnico efectuadas durante el período informado.

Cada entregable deberá ser presentado por el contratista en un plazo máximo de cinco (05) días calendario, contados a partir del día siguiente de culminado el periodo mensual del servicio.

9. LUGAR DE PRESENTACIÓN DE LOS ENTREGABLES

El Contratista deberá entregar toda la documentación dirigida a la Oficina de Sistemas del COFOPRI, a través de la Mesa de Partes Virtual del COFOPRI (http://mpv.cofopri.gob.pe). Alternativamente, también puede entregarse en la Mesa de Partes Presencial del Organismo de Formalización de la Propiedad Informal (COFOPRI) ubicada en Av. Paseo de la República N° 3135 - 3137, distrito de San Isidro, provincia y departamento de Lima.

Horario de atención, registro y trámite de la Mesa de Partes Virtual se encuentra habilitado durante las 24 horas del día; se consideran presentados en el día, aquellos documentos o solicitudes ingresados por la MPV entre las 00:00 horas hasta las 23:59 del día. De esta manera para el cómputo de los plazos inicia a partir del día hábil siguiente de la fecha en la cual presentó su documento o solicitud. El horario de atención de Mesa de partes presencial es de lunes a viernes de 8:00 a.m. a 4:30 p.m.

10. CONFORMIDAD DEL SERVICIO

La Oficina de Sistemas otorgara la conformidad, quien verifica el cumplimiento del servicio de acuerdo a lo solicitado en el punto 5.1 del presente Término de Referencia, en un plazo máximo de siete (7) días calendarios desde la presentación del entregable.

11. FORMA DE PAGO

El pago por la prestación se efectuará en soles y se realizará de forma mensual en partes iguales, de acuerdo al plazo de ejecución del servicio.

Para el trámite COFOPRI deberá contar con la siguiente documentación

- Entregable del contratista que acrediten la ejecución del servicio.
- El comprobante de pago.
- La conformidad del servicio estará a cargo de la Oficina de Sistemas

El pago se realizará con abono en la cuenta "Código de Cuenta Interbancaria" (CCI) del contratista, dentro de los (10) días hábiles siguientes de otorgada la conformidad del servicio por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles.

12. PENALIDADES APLICABLES:

- **Penalidades por mora:** Penalidades por mora: Se aplicará a el/la proveedor/a la penalidad establecida en el artículo 120° del Reglamento de la Ley N° 32069 Ley General de Contrataciones Públicas.

- **Otras Penalidades**

N°	SUPUESTOS	FORMAS DE CALCULO	PROCEDIMIENTO DE VERIFICACIÓN
01	Incumplimiento de los tiempos establecidos en el numeral 5.3.2 (SLA) de los Términos de Referencia.	5% de la UIT vigente Por cada hora o fracción, cuando se supere el tiempo establecido en el numeral 5.3.2 de los TDR en: ○ Tiempo máximo de respuesta para la notificación del ticket ○ Tiempo máximo de solución .	Notificación de solicitudes o incidentes o cualquier otro medio formal utilizado para la gestión del incidente o solicitudes.
02	Incumplimiento en la entrega del Informe Mensual	10% de la UIT vigente del contrato del servicio por cada día calendario de retraso.	Cargo de presentación del informe y verificación del área usuaria.

La suma de la aplicación de las penalidades por mora y de otras penalidades no debe exceder el 10% del monto vigente del contrato o, de ser el caso, del ítem correspondiente.
Estas penalidades se deducen de los pagos a cuenta, pagos parciales o del pago o liquidación final, según corresponda; o si fuera necesario, se descuenta del monto resultante de la ejecución de la garantía de fi el cumplimiento

13. GARANTIA

No aplica de acuerdo al inciso a) del Artículo 139 del Reglamento de la Ley General de Contrataciones Públicas.

14. CONFIDENCIALIDAD Y PROPIEDAD INTELECTUAL

La información y material producido bajo los términos de este servicio, tales como escritos, medios magnéticos, digitales, y demás documentación generados por el

servicio, pasará a la propiedad del COFOPRI. El/La proveedor deberá mantener la confidencialidad y reserva absoluta en el manejo de la información y documentación a la que se tenga acceso relacionada con la prestación.

15. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado por un plazo no menor de un (01) año, contado a partir de la conformidad otorgada por la Entidad.

16. CLAUSULA DE CUMPLIMIENTO

16.1. **Conflicto de intereses (Ley N° 31564)**
Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

16.2. **Declaración Jurada de Intereses**
Conforme al Artículo 2 de la Ley N° 31227 y su reglamento aprobado con Resolución de Contraloría Nº 158-2021-CG, constituye la presentación de la Declaración Jurada de Intereses, requisito indispensable para el ejercicio del cargo o función pública y demás situaciones que regula la presente ley, por lo que, su presentación debe realizar en los plazos establecidos, bajo sanción establecida en la Ley y su Reglamento.
En el marco de la Ley 31227, los sujetos considerados obligados, deberán presentar la declaración jurada de intereses a través del Sistema de Declaraciones Juradas para la Gestión de Conflictos de Intereses de la Contraloría General de la República, tanto al inicio como al cese de la contratación.

17. CLAUSULA ANTICORRUPCION Y ANTISOBORNO

El contratista declara conocer los compromisos antisoborno del COFOPRI, el cual se estable en su Política del Sistema Integrado de Gestión y se encuentra disponible en el portal web del COFOPRI: https://cdn.www.gob.pe/uploads/document/file/2201691/RD%20N%C2%BA%20D000130-2021-DE.pdf.pdf

EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante. Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE. Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. En ningún caso, dichas medias impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

18. MATERIAL DE ORIENTACIÓN PARA DENUNCIAR ACTOS DE CORRUPCION

En el COFOPRI promovemos la ética e integridad de la función pública, por lo que, si conoces de algún acto de corrupción ejercido por un/a servidor/a del COFOPRI, comunícanos tu denuncia ingresando de manera virtual a la Plataforma Digital Única de Denuncias del Ciudadano (https://denuncias.servicios.gob.pe/)

19. SOLUCION DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, según el acuerdo de las partes; de conformidad con lo dispuesto en el artículo 81 de la Ley General de Contrataciones Públicas y del artículo 330 del Reglamento.

Cualquiera de las partes tiene derecho a iniciar la conciliación a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley N° 32069, Ley General de Contrataciones Públicas, y su Reglamento.

20. RESOLUCION DE CONTRATO POR INCUMPLIMIENTO

El COFOPRI puede resolver el contrato, en los siguientes casos:

a) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
b) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
c) Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
d) Por incumplimiento de la cláusula anticorrupción y antisoborno.
e) Por la presentación de documentación falsa o inexacta durante la ejecución contractual y/o en la presentación de su cotización.
f) Cuando la suma de la aplicación de las penalidades por mora y de otras penalidades exceda el 10% del monto del contrato menor correspondiente.
g) Por agotamiento de la necesidad, previo sustento del área usuaria y/o área estratégica.

21. GESTION DE RIESGOS

Las partes realizan la gestión de riesgos de acuerdo con lo establecido en el presente requerimiento, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

22. DOCUMENTOS PARA LA FIRMA DEL CONTRATO

- Certificación o Carta de Autorización del Fabricante (MAFs): Un documento emitido por la marca del Firewall que certifique que el postor es un canal autorizado (Partner) para vender, alquilar y dar soporte técnico a esos equipos.

- Declaración Jurada de Cumplimiento de Características Técnicas: Donde garantice que el equipo entregado cumple estrictamente con el rendimiento (Throughput), puertos y licencias solicitadas en el TDR.

Firmado digitalmente por LEON INFANTES Leonardo Victor FAU 20306484479 soft
Motivo: Soy el autor del documento
Fecha: 24.07.2026 08:04:14 -05:00