Requerimiento
Especificaciones Técnicas

Órgano y/o Unidad Orgánica	Oficina de Tecnologías de la Información e Innovación – OTII
Actividad del POI:	AOI00134500758 Gestión de Infraestructura Tecnológica y Seguridad Informática
Denominación de la contratación:	ADQUISICIÓN E IMPLEMENTACIÓN DE LICENCIAS DE SEGURIDAD GESTIONADA PARA EL CENARES

1. FINALIDAD PÚBLICA

La contratación tiene por finalidad adquirir licencias de seguridad gestionada que permitan fortalecer la seguridad de la infraestructura tecnológica del CENARES, como parte de un esquema de operación principal y de contingencia, así como de la reestructuración de la red institucional. Ello contribuirá a garantizar la continuidad operativa de los servicios informáticos, proteger la red frente a amenazas avanzadas - incluidas aquellas que explotan el servicio DNS, optimizar la administración de usuarios y recursos, y mejorar el rendimiento general de la red.

En conjunto, estas acciones permitirán asegurar la eficiencia, disponibilidad y confiabilidad de los sistemas de información, brindando un soporte adecuado a las actividades institucionales y contribuyendo a la prestación de un servicio oportuno, seguro y eficiente al ciudadano.

2. OBJETIVO DE LA CONTRATACIÓN

La presente contratación tiene como objetivo adquirir e implementar licencias de seguridad gestionada para el Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud (CENARES), orientadas a fortalecer la protección de la infraestructura tecnológica institucional, garantizar la continuidad operativa de los servicios informáticos y mejorar la gestión integral de la seguridad de la red, tanto en escenarios de operación principal como de contingencia.

Asimismo, la contratación busca optimizar la administración de usuarios, recursos y servicios de red, mitigar riesgos asociados a amenazas informáticas avanzadas – incluidas aquellas que afectan los servicios de resolución de nombres (DNS) – y contribuir a la eficiencia, disponibilidad y confiabilidad de los sistemas de información, en concordancia con las necesidades operativas y los objetivos institucionales del CENARES.

3. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

El contratista deberá suministrar, implementar y poner en funcionamiento las siguientes licencias:

Cuadro N.º 1 Cantidad de licencias

Ítem	Sub ítem	Descripción	Cantidad	U/M
1	1.1	Licencia para NGFW de protección perimetral para acceso a internet	2	Unidad
	1.2	Licencia para NGFW de protección del Centro de Datos	2	Unidad

4. CONDICIONES DE CONTRATACIÓN

4.1. MODALIDAD DE PAGO

El contrato se rige por la modalidad A SUMA ALZADA, de conformidad con el artículo 130 del Reglamento.

4.2. SISTEMA DE ENTREGA

El contrato se rige por el sistema de entrega de LLAVE EN MANO, de conformidad con el artículo 129 del Reglamento.

4.3. PLAZO DE ENTREGA

PRESTACIÓN PRINCIPAL

El plazo de la prestación principal es de veinticinco (25) días calendario.

4.3.1. **Entrega del plan de trabajo:** Deberá ser entregado hasta los diez (10) días calendario contados desde el día siguiente de la suscripción del contrato, y deberá ser remitido a la Oficina de Tecnologías de la Información e Innovación, quien tendrá como plazo de tres (03) días calendario para la aprobación u observación de tal documento, la absolución de la observación deberá ser atendida en el plazo de acuerdo a la norma de contrataciones.

4.3.2. **Entrega de los bienes (Licencia para protección DNS):** Plazo de entrega e implementación (instalación, configuración y puesta en producción de las licencias en los equipos firewalls)): Hasta veinte (20) días calendario, contados a partir del día siguiente de la suscripción del contrato.

4.3.3. **Reestructuración e integración de políticas con Directorio Activo:** Hasta veinticinco (25) días calendario, contados a partir del día siguiente de la suscripción del contrato.

4.3.4. Restructuración de la topología de red: Hasta veinticinco (25) días calendario, contados a partir del día siguiente de la suscripción del contrato.

PRESTACIÓN ACCESORIA

El plazo de la prestación accesoria es de veinte y cuatro (24) meses.

4.3.5. Sobre Capacitación: El plazo de la capacitación será de máximo quince (15) días calendario, contados a partir del día siguiente de emitida la conformidad de instalación, configuración y puesta en operación de la solución ofertada.

4.3.6. Sorbe el mantenimiento preventivo: El mantenimiento deberá ser realizado a los doce (12) y veintitrés (23) meses, contabilizados a partir del día siguiente de emitida la conformidad de la prestación principal.

4.3.7. Sobre el soporte técnico: Veinte y cuatro (24) meses contados a partir del día siguiente de emitida el acta de conformidad de la prestación principal.

4.4. LUGAR DE ENTREGA DE LOS BIENES

4.4.1. Lugar de Entrega

El bien deberá ser entregados en el Almacén del CENARES, sito en av. Independencia Nº 1837, El Agustino, provincia y departamento de Lima. Horario de oficina (8:00 a.m. a 1:00p.m. o 2:00 p.m. a 4:00 p.m.).

4.4.2. Lugar de Instalación

La instalación se realizará en la Sede Central Jr. Nazca Nº 548 – 2do Piso – Data Center, Jesús María, provincia y departamento de Lima.

- El proveedor deberá considerar el cambio de ubicación del lugar de instalación. En el cual debe instalar los bienes sin costo alguno para el CENARES.
- Ante un cambio de sede, el CENARES notificará a la empresa contratista con una anticipación mínima de cuarenta y cinco (45) días calendario. A partir de dicha notificación, el contratista

dispondrá de un plazo máximo de diez (10) días calendario para culminar la etapa de prefactibilidad, tras lo cual se iniciará el cómputo del tiempo establecido para la reubicación. La empresa contratista deberá realizar las instalaciones del equipamiento y las configuraciones necesarias para restablecer la conectividad en la nueva sede, sin generar costo adicional alguno para el CENARES.

4.5. ADELANTO DIRECTO

No aplica.

4.6. PENALIDADES

4.6.1. Penalidad por mora

De conformidad con el artículo 120° del Reglamento de la Ley General de Contrataciones Públicas, Ley N.° 32069, señala que, en caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo}}$$

Donde F tiene los siguientes valores:
Para bienes y servicios: F = 0.40

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado.

Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de LA ENTIDAD CONTRATANTE no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme al numeral 120.4 del artículo 120° del Reglamento de la Ley General de Contrataciones Públicas, Ley N°32069.

4.6.2. Otras penalidades

Serán evaluadas durante el plazo máximo de responsabilidad del CONTRATISTA y aplicadas según el caso cuando el PROVEEDOR incurra en falta. Para tal finalidad se utilizará lo establecido en el siguiente cuadro:

Cuadro N.º 2 Otras penalidades

N.º	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento de verificación
1	Cuando el PROVEEDOR supere el plazo máximo de entrega del informe técnico final.	5% del valor de una (01) UIT. Por ocurrencia sobre el pago de la prestación principal.	Mediante informe de la Oficina de Tecnologías de la información e Innovación (OTII).
2	Cuando el PROVEEDOR supere el tiempo máximo de respuesta de 120 minutos para la atención de Asistencia remota y/o presencial establecidos en el Cuadro Nº 3 - Plazos establecidos para la resolución de requerimiento de soporte, literal b. del numeral 5.1.4.	5 % del valor de una (01) UIT, por ocurrencia sobre el pago de mantenimiento y soporte técnico.	Mediante informe de la Oficina de Tecnologías de la información e Innovación (OTII).
3	Cuando el PROVEEDOR supere el tiempo máximo de respuesta de 120 minutos para la atención de diagnóstico del reporte de soporte técnico establecidos en el Cuadro Nº 3 — Plazos establecidos para la resolución de requerimiento de soporte, literal b. del numeral 5.1.4.	1 % del valor de una (01) UIT, por ocurrencia sobre el pago de mantenimiento y soporte técnico.	Mediante informe de la Oficina de Tecnologías de la Información e Innovación (OTII).

UIT: Unidad Impositiva Tributaria

Nota: Se precisa que, para la aplicación de penalidad, el cálculo se efectuará sobre la base de la UIT vigente a la fecha de haberse producido el incumplimiento.

4.7. SUBCONTRATACIÓN

Se encuentra prohibida la subcontratación de las prestaciones objeto del contrato.

4.8. FÓRMULAS DE REAJUSTES

No aplica.

4.9. SOLUCIÓN DE CONTROVERSIAS CONTRACTUALES

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación o arbitraje.

Para el arbitraje, el postor ganador de la buena pro selecciona a uno de las siguientes Instituciones Arbitrales para administrarlo:

N.º	INSTITUCIONES ARBITRALES	RUC
1	Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú.	20155945860
2	Centro de Arbitraje de la Cámara de Comercio de Lima.	20101266819
3	The Ankawa Global Group Sociedad Anónima Cerrada	20605105514

4.10. PLAZO PARA RESPUESTAS ENTRE LAS PARTES

Para los plazos de respuesta de las partes sobre aspectos vinculados con la ejecución contractual que no han sido específicamente previstos en el Reglamento, aplica el plazo máximo de respuesta del siguiente cuadro:

Plazo máximo de respuesta	:	8 días calendario, contabilizados a partir de notificada la comunicación.

Antes del vencimiento de este plazo máximo, las partes pueden acordar su prórroga para cada situación específica considerando la cláusula de notificaciones del contrato.

5. ESPECIFICACIONES TÉCNICAS

5.1. PRESTACIÓN PRINCIPAL

El contratista deberá de suministrar, implementar y configurar las (04) licencias, dichas licencias se desplegarán para la protección de toda la infraestructura de la entidad contratante y deberán cumplir como mínimo con lo siguiente:

<table>
<tr><th colspan="2">Descripción: SEGURIDAD GESTIONADA</th></tr>
<tr><th>Característica</th><th>Especificación</th></tr>
<tr><td>Adquisición de Licencia para protección DNS</td><td>Actualmente la entidad cuenta con cuatro (04) equipos firewall para proteger la ciberseguridad del perímetro externo e interno de la red de la entidad:

<table><tr><th>MARCA</th><th>MODELO</th><th>Cantidad</th></tr><tr><td>Palo alto Network</td><td>PA-3260</td><td>2</td></tr><tr><td>Palo alto Network</td><td>PA-3220</td><td>2</td></tr></table></td></tr>
<tr><td>Protección con aprendizaje automático integrado</td><td>Deberá utilizar análisis basados en aprendizaje automático para identificar amenazas avanzadas que explotan DNS, incluyendo detección mediante la función de Detectores de DNS Security.</td></tr>
<tr><td>Base de datos en la nube</td><td>Deberá contar con una base de datos en la nube que incluya decenas de millones de dominios maliciosos conocidos, permitiendo bloquear phishing, malware y otras categorías de alto riesgo</td></tr>
<tr><td>Panel de análisis de DNS Security</td><td>Deberá ofrecer un panel que permita generar informes detallados sobre amenazas, con visibilidad completa del contexto de los eventos de seguridad y las tendencias del tráfico DNS a lo largo del tiempo</td></tr>
<tr><td>Sinkholing de DNS</td><td>Deberá incluir la técnica de sinkholing de DNS, que permita interceptar consultas DNS hacia dominios maliciosos conocidos, resolviéndolos en una dirección IP definida por el cliente. Además, deberá registrar intentos de acceso al sinkhole y permitir acciones automatizadas, como la cuarentena de hosts infectados.</td></tr>
<tr><td>Categorías de DNS Security</td><td>Deberá permitir la definición de políticas de seguridad independientes basadas en las características de las amenazas, asignando niveles de gravedad a los logs según el tipo de firma. Estas políticas deberán cubrir amenazas como comando y control, DNS dinámico, malware, dominio recién registrado, phishing, grayware, dominio aparcado y evasión de proxy y anonimizadores, ajustándose a los protocolos de seguridad de la red.</td></tr>
</table>

5.1.1. Reestructuración e integración de políticas con Directorio Activo

Se deberá brindar el siguiente restructuración e integración de políticas especializada basado en Directorio Activo, que consta de:

Evaluación inicial de la infraestructura

- El proveedor deberá realizar una evaluación exhaustiva de la infraestructura del Directorio Activo, analizando la configuración de dominios, controladores de dominio, políticas de grupo (GPO), objetos de usuarios y equipos, y la replicación entre sitios.

Diagnóstico de vulnerabilidades y propuestas de mejora

- Deberá realizarse un análisis de seguridad para identificar vulnerabilidades en la estructura del Directorio Activo, proponiendo mejoras. Esto incluirá la revisión de permisos, políticas de acceso, autenticación multifactor (MFA) y protección de cuentas privilegiadas.

Optimización de la gestión de identidades

- Se deberá incluir la optimización del manejo de identidades, incluyendo la automatización de procesos de aprovisionamiento, desactivación y gestión de usuarios, así como la implementación de políticas sólidas de contraseñas y autenticación.

Migración y actualización

- Deberá contemplarse la posibilidad de planificar e implementar la migración a versiones más recientes del Directorio Activo o a entornos híbridos (on-premise y en la nube), garantizando la continuidad del servicio y la integridad de los datos.

Integración con otras soluciones de TI

- Se deberá asegurar la integración del Directorio Activo con otras soluciones tecnológicas, como servicios en la nube (Azure AD), aplicaciones de seguridad y sistemas de gestión de identidades (IDM/IAM) y el firewall perimetral y del centro de datos para configurar las políticas basado en los grupos de Directorio Activo.

Creación y gestión de certificados digitales

- El proveedor deberá ser capaz de implementar y gestionar infraestructuras de clave pública (PKI) y certificados digitales necesarios para autenticar y asegurar las comunicaciones en el Directorio Activo. Esto incluye:
  - Configuración de Certificados de Autenticación para servicios como LDAP, RADIUS o autenticación de servidores.

Implementación de Certificados SSL/TLS para asegurar el tráfico en redes internas y la comunicación con servicios en la nube.

5.1.2. Restructuración de la topología de red

Se deberá brindar la siguiente reestructuración de red, que consta de:

Evaluación de la infraestructura de red actual

- Análisis completo de la topología de red: Realizar un mapeo de la estructura existente, identificando dispositivos, conexiones y flujos de tráfico para comprender la configuración actual.

- Revisión del rendimiento: Evaluar el rendimiento actual de la red, incluyendo velocidad, latencia y ancho de banda utilizado, para identificar cuellos de botella y áreas de mejora.
- Identificación de vulnerabilidades: Examinar los puntos débiles en la seguridad de la red, así como los riesgos asociados a la infraestructura actual, y proponer recomendaciones para mitigarlos.
- Se deberá realizar un análisis de gestión de vulnerabilidades y priorización de riesgos considerando lo siguiente:
  - Se deberá utilizar una plataforma web/Cloud y considerar al menos 50 dispositivos de la entidad (PCs y/o SERVIDORES)
  - La plataforma debe tener visibilidad y cobertura en tiempo real para los sistemas operativos y aplicaciones de la entidad, es decir, cualquier cambio en el inventario (instalación / desinstalación / cambio de aplicaciones y / o activos debe reflejarse instantáneamente en su panel de control)
  - La plataforma debe proporcionar una solución integrada para la gestión de vulnerabilidades, la priorización de riesgos y la corrección en una plataforma.
  - El servicio debe brindar el reconocimiento automático de aplicaciones, la priorización de amenazas basada en activos, priorización de vulnerabilidades combinada con inteligencia interna, priorización y reparación de vulnerabilidades de un extremo a otro, proceso de clasificación de riesgos para priorizar la corrección de vulnerabilidades descubiertas, clasificación de riesgo basada en activos, clasificación de riesgo por aplicaciones.
  - Debe brindar Administración de parches para Windows OS, Administración de parches para aplicaciones de terceros en Windows, Administración de parches para Linux OS, Administración de parches para aplicaciones de terceros en Linux, Administración de parches para Mac OS, Detección de vulnerabilidades en tiempo real, Detección de la explotación de software en tiempo real.
  - Debe tener la funcionalidad para agregar protección contra una vulnerabilidad, sin necesariamente aplicar el parche ("parche virtual").
  - Posibilidad de generar scripts en la misma plataforma para Windows, Linux y Mac, Ejecución de scripts de corrección en toda la plataforma y Permitir el despliegue de los agentes por la línea de comandos.

- El proveedor deberá entregar un informe detallando las acciones realizadas, las evidencias encontradas y las soluciones implementadas.
- Se debe presentar documentación técnica en la etapa de propuesta que indique el cumplimiento con la herramienta o software a utilizar
- Estas licencias deberán estar instaladas por el mismo tiempo de duración de las licencias de los firewalls.

Diseño de la nueva arquitectura de red

- Propuesta de un diseño escalable: Desarrollar un diseño que contemple la escalabilidad, permitiendo que la red se adapte a nuevas demandas futuras sin comprometer el rendimiento.
- Integración de segmentación de red: Sugerir la segmentación adecuada para mejorar la seguridad y el rendimiento, dividiendo la red en diferentes subredes según las necesidades de la organización.
- Plan de redundancia: Recomendar la creación de un sistema que incluya caminos redundantes para asegurar la continuidad del servicio en caso de fallos en la infraestructura.

Desarrollo de políticas de seguridad de red

- Establecimiento de políticas de acceso: Proponer controles de acceso claros para usuarios y dispositivos, asegurando que solo el personal autorizado tenga acceso a áreas críticas de la red.
- Configuración de protocolos de seguridad: Recomendar la implementación de protocolos de seguridad como VPN, autenticación multifactor (MFA) y cifrado de datos para proteger la información en tránsito.
- Se debe ofrecer un servicio donde se pueda proporcionar información sobre amenazas activas durante los últimos 2 meses como mínimo:
  - La solución debe utilizar una red global de sensores como fuente de inteligencia para los feeds;
  - La solución debe ofrecer colecciones de IoC especialmente creadas para soluciones de NGFW, y éstos puedan mejoran de forma considerable el nivel de protección de seguridad de la red corporativa, sin necesidad de una integración o configuración complicadas y conservando la topología de red actual.
  - La solución debe proporcionar información a través de protocolos de comunicación seguros (HTTPS) y vía API token;

- Los feeds de amenazas deben contener listas de direcciones IP con el puntaje de amenaza más alto y dominios de primer y segundo nivel de recursos que se conocen por distribuir malware, funcionar como centros de comando y control (C&C) de botnets o alojar recursos de phishing.
- Los feeds de amenazas deben tener una frecuencia de actualización promedio de:
- El feed de reputación IP: 20 minutos;
- El feed de URL maliciosas y phishing: 20 minutos;
- El feed de URL de botnet C&C: 60 minutos;
- Los feeds de amenazas debe tener soporte nativo para los NGFW más populares como: FortiGate, Palo Alto, Checkpoint y Cisco.
- Los feeds de amenazas debe someterse a pruebas exhaustivas y aplicar filtros antes de publicar sus fuentes, garantizando la distribución de datos 100 % validados.

5.1.3. Instalación, configuración y puesta en marcha de las licencias de seguridad gestionada

Por cuanto la modalidad de ejecución es llave en mano, el CONTRATISTA debe realizar todas las actividades que pongan en correcta operación las licencias en su conjunto por adquirir, de manera tal que se obtenga el mayor aprovechamiento de las licencias.
Será responsabilidad del CONTRATISTA efectuar las tareas necesarias de integración para la puesta en operación de las licencias ofertadas.
La instalación, configuración puesta en marcha de las licencias ofertadas debe ser realizada por el personal certificado en la marca ofertada. La configuración de las licencias a nivel de software ofertado debe ser realizada por personal experto certificado en la marca de las licencias ofertados, en conjunto con el personal especialista que designe la entidad.
La omisión en la oferta de algún bien o componente que al momento de instalación, configuración y puesta en marcha resulte necesario para el normal funcionamiento de los equipos licenciados o para el cumplimiento de las especificaciones técnicas ofrecidas, obligará al CONTRATISTA a proveerlo de inmediato y sin costo alguno para la Entidad, pues se entiende que las licencias en su conjunto es una solución de seguridad gestionada que comprenden (los equipos firewalls de marca Palo Alto Networks).
Para iniciar deberá presentar correspondiente (Plan de trabajo).
A la finalización correcta implementación, la entidad y el contratista deberán emitir el acta de conformidad de instalación. Configuración y puesta en marcha de las licencias.

5.1.4. PRESTACIONES ACCESORIAS

a. Mantenimiento Preventivo

- Deberá realizarse dos (02) mantenimientos preventivos de hardware y software de los equipos licenciados, dentro de la vigencia del contrato, los mismos que se harán efectivos en los siguientes periodos:
  - Primer mantenimiento Preventivo: a los doce (12) meses contabilizados desde el día siguiente de la conformidad de la prestación principal, contando con un plazo máximo de 10 días calendario para realizar el mantenimiento.
  - Segundo mantenimiento Preventivo: a los veintitrés (23) meses contabilizados desde el día siguiente de la conformidad de la prestación principal, contando con un plazo máximo de 10 días calendario para realizar el mantenimiento.

- Las actividades que se realizarán en los mantenimientos preventivos deberán estar acorde a las condiciones de soporte provistas por el fabricante, esperándose las siguientes:
  - Limpieza física interna (de corresponder) y externa de los equipos licenciados.
  - Actualización del firmware, BIOS, drivers, portal de administración o parches de los equipos licenciados, las mimas que deberán tener el aval de los especialistas de la marca antes de llevarse a cabo los trabajos.
  - Upgrade a la última versión disponible y estable del software y componentes, el mismo que debe tener aval de los especialistas de la marca antes de realizarse (vía correo electrónico), para evitar fallas o bug posteriores a la actualización.
- Identificación de eventos que puedan afectar la operación de los equipos licenciados.
- Análisis de brecha de seguridad, que debe tener las acciones siguientes:
  - El análisis podrá efectuarse mediante herramientas propias del contratista o de terceros, siempre que cumpla con el alcance mínimo requerido y genere evidencia técnica verificable.
  - La Solución propuesta debe simular escenarios reales de ciberataque dirigidos a la entidad desde una consola en la nube

- El objetivo de la Solución propuesta no es escanear contra vulnerabilidades sino evaluar continuamente el desempeño de seguridad en las soluciones de seguridad con las que cuente la Entidad. utilizando una base de datos de amenazas cibernéticas actualizada diariamente.
- Una vez que la solución propuesta identifica que un ataque cibernético no puede detenerse en el nivel de controles de seguridad, la plataforma de soluciones revela esta información junto con las posibles
- alternativas de remediación que puede propiciar para el equipo firewall que tiene la entidad.
- La solución propuesta debería poder evaluar el nivel de seguridad que proporciona el equipo firewall que tiene la entidad, considerando como mínimo 3 segmentos de la red a fin de detectar vulnerabilidades y
- amenazas que no cuenten con un bloqueo.
- No debe dirigirse ni interactuar con el servidor de producción de la entidad.
- Debe contar como mínimo con una biblioteca de 30,000 amenazas y 15,000 acciones Debe brindar visibilidad granular de amenazas en más de cien categorías de amenazas, familias de malware, tipos de aplicaciones y
- otros criterios con la finalidad de aumenta la visibilidad de la preparación ante amenazas cibernéticas para una acción rápida.
- Al finalizar cada mantenimiento preventivo, el contratista deberá entregar un informe en formato impreso y digital en el cual indique las acciones realizadas durante el mantenimiento (Fechas, reportes, eventos, alertas, estado de salud del hardware o Software, etc. de toda la solución). El plazo para la entrega del informe será de siete (07) días calendario, contabilizados a partir del día siguiente de haber concluido cada mantenimiento preventivo.

b. Soporte Técnico

- Periodo de soporte: veinte y cuatro (24) meses contados a partir del día siguiente de emitida la conformidad de la prestación principal.
- El CONTRATISTA deberá contar con sistema de Mesa de Ayuda, Mesa de Servicio, para recibir solicitudes de atención vía teléfono, correo electrónico con soporte ON SITE y ON LINE dependiendo de la severidad del caso.

- El CONTRATISTA deberá indicar un número telefónico, el cual será el primer nivel de escalamiento para el reporte de soporte técnico sobre toda la solución ofertada.
- El CONTRATISTA deberá indicar una lista con la información (nombre, número telefónico, correo electrónico) del personal que será el segundo nivel de escalamiento para el reporte de soporte técnico sobre toda la solución ofertada.
- El CENARES reportará cualquier tipo de requerimiento de soporte al número telefónico gratuito o a través de una comunicación con el personal encargado designado por el CONTRATISTA, las 24 horas, todos los días incluidos feriados.
- Ante un reporte de soporte técnico, el CONTRATISTA debe garantizar la disponibilidad de personal técnico, las 24 horas, todos los días incluido feriados, durante el periodo de garantía de los equipos.
- Atención integral in-situ, de soporte técnico de la solución, sin costo alguno para la institución, en caso sea necesario.
- El CONTRATISTA deberá cumplir el siguiente plazo de atención ante algún requerimiento:

Cuadro N.º 3 – Plazos establecidos para la resolución de requerimiento de soporte

N.º	Descripción	Detalle	Tiempo Máximo de atención (Minutos)
1	Tiempo de asistencia remota y/o presencial	Tiempo empleado por el CONTRATISTA para atender de manera remota y/o presencial en las instalaciones del CENARES.	Hasta 120 minutos.
2	Tiempo de diagnóstico de reporte de soporte técnico	Tiempo empleado por el CONTRATISTA para identificar la causa del reporte de soporte técnico y brindar un primer reporte al personal encargado que la Oficina de Tecnologías de la Información e Innovación del CENARES determine.	Hasta 60 minutos.

		El tiempo se contabiliza desde que el CONTRATISTA llega a CENARES y/o accede al/los equipos afectados.	
3	Tiempo de resolución de avería	Tiempo empleado por el CONTRATISTA para restablecer la operatividad del/los equipos licenciados.	Hasta 180 minutos

c. Capacitación

El contratista deberá realizar una capacitación de veinte y cuatro (24) horas lectivas, dirigida a un máximo de tres (03) participantes que designe la Entidad. La capacitación deberá ejecutarse dentro de un plazo máximo de cinco (05) días calendario, contados a partir del día siguiente de la suscripción del "Acta de Implementación y Configuración", y deberá ser dictada por el Especialista en Ciberseguridad. Para tal efecto, el contratista deberá considerar lo siguiente:

- Diseño de arquitectura segura
- Alta disponibilidad (HA)
- Segmentación y zonas
- Best practices de hardening
- Optimización de performance
- Respuesta ante incidentes
- Integración con SIEM / SOC

El contratista deberá entregar los certificados o constancias de la capacitación a cada uno de los participantes al finalizar la transferencia de conocimiento. Dicha capacitación se deberá llevar a cabo bajo la modalidad de acuerdo a las condiciones acordadas para ello.
Adicionalmente el CONTRATISTA deberá entregar el material en pdf y video por cada participante, toda la documentación que contenga todo el contenido de la instrucción.

5.2. ENTREGABLES

PRESTACIÓN PRINCIPAL

5.2.1. ENTREGA DEL BIEN

Los bienes objetos de la contratación deberán ser entregados en el almacén central.

5.2.2. PLAN DE TRABAJO

El plan de trabajo deberá contener lo siguiente:

Plan de trabajo a seguir con los responsables tanto del CONTRATISTA como del CENARES, el cual deberá contener como mínimo los siguientes puntos:

- Descripción del proyecto
- Acciones a realizar
- Tiempo de ejecución
- Estrategias para implementar
- Participantes del proyecto
- Responsables de las acciones
- Lineamientos de comunicación
- Matriz de riesgos
- Restricciones del proyecto

5.2.3. IMPLEMENTACIÓN Y CONFIGURACIÓN

El Postor deberá presentar un informe técnico final sobre la implementación las licencias en los equipos firewalls en el gabinete del Centro de Datos del Cenares, el cual debe ser presentado dentro de los cinco (05) días calendario contados a partir del día siguiente de la firma del acta de la instalación y puesta en marcha de los equipos licenciados. Deberá contener lo siguiente:

a) El CONTRATISTA deberá entregar el procedimiento para la gestión de incidentes de los equipos ofertados mediante la mesa de ayuda del CONTRATISTA.
b) El CONTRATISTA deberá entregar el manual de instalación, configuración y administración de los equipos licenciados paso a paso.
c) El CONTRATISTA deberá entregar un documento en el cual se muestre la vigencia de la garantía comercial y soporte de los equipos licenciados.
d) El CONTRATISTA deberá entregar un inventario de todos los equipos licenciados.
e) El CONTRATISTA deberá entregar el resultado de las pruebas de esfuerzo, conectividad y tolerancia a fallos, que se realizarán durante el proceso de instalación y configuración, los cuales serán definidos previamente en coordinación con el área técnica de la OTII.
f) El CONTRATISTA deberá entregar la topología lógica y física de la nueva reestructuración de configuración de los equipos licenciados.
g) El CONTRATISTA deberá entregar la configuración realizada en los equipos licenciados.

h) El CONTRATISTA deberá entregar un acta de implementación y despliegue de los equipos licenciados.

La presentación del entregable indicado en el numeral 5.2.1., 5.2.2. y 5.2.3. serán dirigidos a la Oficina de Tecnologías de la Información e Innovación mediante Mesa de partes del CENARES (Ubicado en Jr. Pachacútec Nº 900 – Jesús María) o mesa de partes digital al siguiente correo: mesadepartesdigital@cenares.gob.pe o a través de la plataforma digital las veinticuatro (24) horas y los siete (07) días de la semana, sin embargo, se consideran como recepcionadas el día siguiente hábil, según el plazo previsto para cada uno de los entregables.

PRESTACIÓN ACCESORIA:

5.2.4. ENTREGABLE DE CAPACITACIÓN

Al término de la capacitación deberá presentar el acta de capacitación, a entregarse contra la ejecución de la capacitación.

5.2.5. ENTREGABLE DE CADA MANTENIMIENTO PREVENTIVO

Al término de cada mantenimiento, que se efectuará conforme lo indicado el literal a) del numeral 5.1.4. de la presente especificación técnica, el CONTRATISTA deberá entregar un informe dirigido a la Oficina de Tecnologías de la Información e Innovación, en el cual indique las acciones realizadas durante el mantenimiento y los tiempos llevados a cabo por cada actividad. El plazo para la entrega del informe será de siete (07) días calendario, contabilizados a partir del día siguiente de haber concluido cada mantenimiento preventivo.

5.2.6. ENTREGABLE DEL SOPORTE TÉCNICO

El proveedor deberá presentar dos informes de incidencias del soporte técnico (informes anuales) dentro de los veinte y cuatro (24) meses contados a partir del día siguiente de emitida la conformidad de la prestación principal. el CONTRATISTA deberá entregar un informe dirigido a Oficina de Tecnologías de la Información e Innovación, en el cual indique las acciones realizadas durante el soporte técnico y los tiempos llevados a cabo por cada actividad, adjuntando las actividades realizadas respecto del literal b) del numeral 5.1.4. de la presente especificación técnica.
Informe de soporte técnico sobre la solución instalada y configurada, deberá contener lo siguiente:

- Registro y categorización de incidentes
- Resolución de incidentes por el soporte de nivel 1
- Resolución de incidentes por el soporte de nivel 2

- Gestión de incidentes graves
- Monitorización y escalado de incidentes
- Cierre y evaluación de incidentes
- Información proactiva a usuarios

La presentación de cada entregable indicado en el numeral 5.2.4, 5.2.5. y 5.2.6. serán dirigidos a la oficina de Tecnologías de la Información e Innovación mediante Mesa de partes del CENARES, (Ubicado en Jr. Pachacútec Nº 900 – Jesús María) o mesa de partes digital al siguiente correo: mesadepartesdigital@cenares.gob.pe o a través de la plataforma digital las veinticuatro (24) horas y los siete (07) días de la semana, sin embargo, se consideran como recepcionadas el día siguiente hábil, según el plazo previsto para cada uno de los entregables.

5.3. MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

Área que coordina con el contratista: La Oficina de Tecnologías de la Información e Innovación - OTII del CENARES.

Área responsable de las medidas de control: La Oficina de Tecnologías de la Información e Innovación - OTII del CENARES.

Área que otorgará la conformidad: La Oficina de Tecnologías de la Información e Innovación - OTII del CENARES.

5.4. RECEPCIÓN Y CONFORMIDAD DE LOS BIENES

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N.° 32069, Ley General de Contrataciones Públicas. La recepción será otorgada por el Almacén del CENARES y la conformidad será otorgada por la Oficina de Tecnologías de la Información e Innovación (OTII) en el plazo máximo de siete (7) días computados desde el día siguiente de producida la recepción.

5.5. CONFORMIDAD DE LA PRESTACIÓN

La conformidad de la prestación se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N.° 32069, Ley General de Contrataciones Públicas. La conformidad será otorgada por la Oficina de Tecnologías de la Información e Innovación (OTII) en el plazo máximo de siete (7) días, computados desde el día siguiente de producida la recepción de los entregables definidos en el numeral 5.2. de la presente especificación técnica.

5.6. FORMA DE PAGO

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.

5.6.1. De la prestación principal

La entidad contratante se obliga a pagar la contraprestación a el contratista en PAGO ÚNICO a cuenta, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 144 del Reglamento de la Ley N.° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N.° 009-2025-EF, de acuerdo al siguiente detalle.

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

- Comprobante de pago.
- Guía de remisión.
- Un (01) Informe técnico de implementación y configuración y de capacitación de las licencias de seguridad gestionada, conteniendo la documentación descrita en el numeral 5.2.1., 5.2.2. y 5.2.3. de la presente Especificación técnica.

Para tal efecto, el responsable de otorgar la conformidad de la prestación deberá hacerlo en un plazo que no excederá de los siete (7) días del día siguiente de recibido el bien.

5.6.2. De la prestación accesoria

Sobre la capacitación

El 100% del pago por el monto del acta de Capacitación, previa conformidad del servicio.
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 e Innovación (OTII) emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Presentación del entregable correspondiente indicado en el numeral 5.2.4. de la presente especificación técnica.

Sobre el mantenimiento preventivo

El pago se efectuará en moneda nacional, en dos pagos parciales e iguales del monto ofertado para el mantenimiento preventivo, previa conformidad del mantenimiento preventivo.

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 e Innovación (OTII) emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Presentación del entregable correspondiente indicado en el numeral 5.2.5. de la presente especificación técnica.

Sobre el soporte técnico

El pago se efectuará en moneda nacional, en dos pagos parciales del monto ofertado luego de efectuado cada soporte técnico.

El 50% del monto ofertado en el primer pago, y finalmente 50% del monto ofertado en el segundo pago.

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 e Innovación (OTII) emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Presentación del entregable correspondiente indicado en el numeral 5.2.6. de la presente especificación técnica.

5.7. REQUISITOS DEL PERSONAL DEL CONTRATISTA (PERSONAL CLAVE)

a. Del Proveedor

- Empresa dedicada a la venta e instalación de licencias de seguridad gestionada (Adquisición de licencias e instalación de firewalls).
- El postor ganador debe contar con un Centro de Operaciones de Seguridad (SOC – Security Operation Center) propio o un Centro de Soporte y atención a clientes propio, precisando que el medio de atención de este SOC es remoto y deba pertenecer al contratista, acreditándose mediante una constancia firmada por el representante legal de la empresa, lo cual deberá ser presentada como documento adicional para la firma de contrato.
- El postor ganador debe contar con una herramienta de mesa de ayuda para la atención de la garantía ofertada, en modalidad 24x7, la herramienta debe registrar las incidencias o solicitudes del CENARES en un ticket de atención mediante una línea de telefonía fija o 0800, correo electrónico y/o vía online para la

gestión del incidente, que deberá acreditarse mediante una constancia, lo cual deberá ser presentada como documento adicional para la firma de contrato.

b. Del Personal

Un (01) jefe de Proyecto:
Estará a cargo de la implementación de las licencias ofertadas. Será el único que coordine con el personal de la Oficina de tecnologías de la Información e Innovación del CENARES, la implementación de las licencias ofertadas.

Actividades del jefe del Proyecto:

1. Gestión y planificación del proyecto
    - Elaborar y aprobar el plan de trabajo y cronograma de implementación.
    - Definir alcance, hitos, entregables y responsables del proyecto.
    - Coordinar con la Entidad la ventana de implementación y pruebas.
    - Gestionar riesgos, dependencias y contingencias del proyecto.
2. Coordinación técnica
    - Coordinar con el equipo técnico del contratista y el personal designado por la Entidad.
    - Validar el levantamiento de información de la infraestructura existente.
    - Supervisar la correcta integración del firewall con la red actual (LAN, WAN, DMZ, VPN).
    - Coordinar pruebas de interoperabilidad con sistemas existentes.
3. Supervisión de la implementación
    - Supervisar la instalación lógica de licencias del firewall Palo Alto.
    - Verificar la configuración base: zonas, interfaces, routing, NAT.
    - Supervisar la implementación de políticas de seguridad (App-ID, User-ID, Content-ID).
    - Asegurar la correcta activación de licencias y servicios de seguridad.
4. Seguridad avanzada y hardening
    - Validar la configuración de Threat Prevention, WildFire, URL Filtering y Antivirus.

- Supervisar la configuración de VPN (IPSec / GlobalProtect).
- Asegurar la aplicación de buenas prácticas de hardening y segmentación.
- Verificar la correcta configuración de logs, monitoreo y alertas.

5. Pruebas y validación
   - Coordinar y supervisar las pruebas funcionales y de rendimiento.
   - Validar la continuidad operativa durante la puesta en producción.
   - Gestionar la corrección de observaciones detectadas.
   - Aprobar el Acta de Implementación, Configuración y Puesta en Operación.
6. Documentación y entregables
   - Revisar y validar la documentación técnica de la configuración de la licencia de firewall implementado.
   - Verificar la entrega de diagramas, respaldos de configuración y manuales.
   - Validar el informe final de implementación.
   - Custodiar la documentación entregada a la Entidad.
7. Capacitación y transferencia de conocimiento
   - Coordinar y supervisar la capacitación al personal designado por la Entidad.
   - Verificar el cumplimiento de horas, contenidos y perfiles del capacitador.
   - Validar la entrega de materiales y acta de capacitación.
8. Cierre del proyecto
   - Coordinar el cierre formal del proyecto.
   - Verificar la conformidad de todos los entregables.
   - Elaborar o validar el informe de cierre del proyecto.
   - Asegurar la transferencia completa de la solución a la Entidad.

Formación Académica:

a) Copia del Título profesional o Bachiller en Ingeniería de Sistemas, Ingeniería de Sistemas e Informática, Ingeniería Electrónica y Telecomunicaciones, Ingeniería Industrial, Ingeniería Eléctrica, Ingeniería Electrónica, Ingeniería Electricista, Ingeniería Mecánico Electricista, Ingeniería de Telecomunicaciones, Ingeniería Electrónica con mención las Telecomunicaciones, Ingeniería Sistemas Empresariales, Ingeniería de Software, Ingeniería de Sistemas de

Información, Ingeniería de Telecomunicaciones y Redes, Ingeniería de Computación y Sistemas, Ingeniería Informática y Sistemas, Ingeniería de Redes y Comunicaciones, Ingeniería de Seguridad Informática, Ingeniería Informática o Ingeniería de Auditoría Informática.

b) Certificaciones
Certificado de estudios como mínimo de 30 horas en el curso de Gestión de Proyectos y/o Certificación de PMP y/o certificación SCRUM.

c) Experiencia
Deberá ser acreditada como requisito de calificación.

Un (01) Personal Técnico:
El personal técnico será el responsable de la instalación, configuración y puesta en operación del licenciamiento.

Formación Académica:

a) **Copia** del Título profesional o Bachiller en Ingeniería de Sistemas, Ingeniería de Sistemas e Informática, Ingeniería Electrónica y Telecomunicaciones, Ingeniería Industrial, Ingeniería Eléctrica, Ingeniería Electrónica, Ingeniería Electricista, Ingeniería Mecánico Electricista, Ingeniería de Telecomunicaciones, Ingeniería Electrónica con mención las Telecomunicaciones, Ingeniería Sistemas Empresariales, Ingeniería de Software, Ingeniería de Sistemas de Información, Ingeniería de Telecomunicaciones y Redes, Ingeniería de Computación y Sistemas, Ingeniería Informática y Sistemas, Ingeniería de Redes y Comunicaciones, ingeniero Civil electrónico, Ingeniería de Seguridad Informática, Ingeniería Informática o Ingeniería de Auditoría Informática.

b) Certificaciones
Certificado en la marca de firewall como mínimo que cuente administrador asociado o acreditado, emitido por el fabricante de los equipos ofertados, que será acreditado con copia simple del certificado

c) Experiencia
Deberá ser acreditada como requisito de calificación.

Importante:
El contratista deberá presentar, como documentos para el perfeccionamiento del contrato, copia simple de toda documentación que acredite fehacientemente el perfil mínimo señalado (Formación académica y capacitaciones), en caso del profesional Titulado deberá de presentar además la colegiatura y habilitación profesional.

NOTA:
En caso de presentar Ingenieros, y en concordancia con el artículo N° 1 de la Ley N° 28858, los Ingenieros, deben 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. En caso la titulación obtenida sea en el extranjero, dicha titulación obtiene validez en el Perú, cuando es otorgada por la autoridad competente, a través de los procedimientos de "revalidación" o "reconocimiento" regulados en normativa especial en la materia.

El contratista se encuentra en la obligación de ejecutar el servicio con el personal ofertado en el procedimiento de selección, pudiendo efectuar el reemplazo, siempre y cuando el personal propuesto reúna iguales o superiores características a las previstas en el presente requerimiento, debiendo para ello contar con la autorización y aprobación favorable de la OTII, quien verificará el cumplimiento dentro de los tres días (3) anteriores al día de reemplazo prevista.

A efectos de verificar que el personal reemplazante cumple con las características del personal a ser reemplazado, se debe considerar las características determinadas en el presente requerimiento; independientemente de las características técnico–profesionales del personal reemplazado. Para tal efecto, el contratista deberá presentar a través de Mesa de Partes de la Entidad toda documentación que acredite de forma fehaciente el cumplimiento del perfil mínimo precisado en el presente requerimiento por el personal reemplazante, dirigida al jefe de la OTII, con una anticipación de cinco (5) días hábiles de la fecha que pretende realizar el reemplazo del personal.

5.8. RESPONSABILIDAD POR VICIOS OCULTOS

La recepción conforme de la prestación por parte de la entidad contratante no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la Ley N.° 32069, Ley General de Contrataciones Públicas y el artículo 144 de su Reglamento. El plazo máximo de responsabilidad del contratista es de no menor de un (1) año contado a partir de la conformidad otorgada por la entidad contratante.

5.9. CONFIDENCIALIDAD

Toda información del CENARES a la que tenga acceso el contratista, así como todo su personal es estrictamente confidencial. El contratista y su personal designado al servicio deben comprometerse a mantener las reservas del caso y no transmitirla a ninguna persona (natural o jurídica) sin la autorización expresa y por escrito del CENARES.
Asimismo, el operador de conformidad con lo establecido en el artículo 13 del Decreto Supremo 020-2007-MTC que aprobó el Reglamento General de la Ley de Telecomunicaciones, está obligada a salvaguardar el secreto de las telecomunicaciones y la protección de datos personales, así como adoptar las medidas y procedimientos razonables para garantizar la inviolabilidad y el secreto de las telecomunicaciones cursadas a través de tales servicios.

La obligación de confidencialidad no aplicará a la siguiente información:

- Resulte accesible al público por causa distinta del incumplimiento de la obligación de confidencialidad por la parte receptora (Se debe considerar que aun cuando la información confidencial se haga pública, esta no debe perder la condición de confidencialidad por parte del contratista).
- Haya sido publicada con anterioridad a la fecha de la firma de contrato (Se precisa que será de aplicación únicamente y sólo si la publicación en mención haya sido autorizada por el CENARES).
- Se encuentre en poder de la parte receptora y no esté sujeta a cualquier otro impedimento o restricción puesta de manifiesto a la otra parte en el momento de la revelación o luego de ella (Toda información proporcionada al contratista se encuentra bajo impedimento y/o restricción salvo autorización previa y expresa del CENARES).
- Cuando la información haya sido recibida de terceros sin restricciones y sin que implique incumplimiento de contrato. (Toda información proporcionada a la contratista relacionada al servicio contratado con el CENARES mantiene su condición de "confidencial" por lo tanto se encuentra bajo impedimento y/o restricción de publicación por parte del contratista, salvo autorización previa y expresa del CENARES, de lo contrario recaerá en incumplimiento de contrato).
- Cuando la información sea independientemente desarrollada por la parte receptora, siempre que no hubiese utilizado para ello información confidencial proporcionada por la Institución. (De conformidad con el ordenamiento legal vigente).
- Deba ser revelada para dar cumplimiento de una orden de naturaleza judicial o administrativa, en cuyo caso la parte receptora deberá informar a la otra parte en forma inmediata a la sola recepción de la citada orden. (De aplicación únicamente cuando el requerimiento provenga de la autoridad judicial competente y en el caso de orden de naturaleza administrativa se otorgará la información previa autorización expresa del CENARES).

5.10. OBLIGACIONES DEL CONTRATISTA

- El contratista es responsable de notificar a la OTII sobre cualquier cambio o actualización que realice, ya sea en la herramienta implementada, en su personal propuesto o información proporcionada con relación a su oferta técnica.
- Si el contratista cambia a algún miembro de su personal (jefe de proyecto o personal técnico) durante el periodo de la implementación y/o Configuración de la presente prestación,

tendrá que realizar la comunicación del cambio de personal como mínimo 5 días calendario antes de realizar dicho cambio, debiendo comunicar mediante documento dirigido a la OTII, a través de la Mesa de Partes del CENARES.

a. Tener en cuenta que el nuevo personal debe cumplir como mínimo con los requisitos indicados en el numeral 4.8 de la presente Especificación Técnica (que incluye los requisitos de calificación), por lo que en esta solicitud de cambio debe adjuntar la documentación que acredite ello.
b. La aceptación de este cambio deberá ser aprobada por la OTII, que tendrá como máximo dos (02) días calendario para brindar la respuesta de aceptación o rechazo en caso no cumpla con los requisitos solicitados.
c. De ser rechazado el personal de reemplazo por no cumplir con los requisitos mínimos solicitados, el contratista no podrá realizar el cambio de personal hasta que presente a un personal que sí cumpla con lo solicitado.
d. Por lo tanto, el personal que propone para reemplazo no podrá participar en ninguna etapa del presente requerimiento, si previamente no ha sido aprobado.

- El personal de reemplazo no podrá participar en el período de implementación y/o configuración si previamente no ha sido aprobado por la OTII.

5.11. GARANTÍA

- La garantía comercial de las licencias será de veinte y cuatro (24) meses, contado a partir de emitida la conformidad por la prestación principal. Se deberá presentar carta de fabricante en la cual avale la garantía de los bienes ofertados, y deberán ser presentados por el CONTRATISTA al momento de la entrega de los bienes.
- Soporte por parte del fabricante y el derecho a las actualizaciones de firmware pueda salir durante la vigencia de la garantía por el período de dos (02) años contabilizados a partir del día siguiente de emitida la conformidad por la prestación principal.

5.12. DOCUMENTOS PARA EL PERFECCIONAMIENTO DEL CONTRATO.

- Para acreditar los documentos de formación académica y certificaciones requeridos para el jefe de proyecto y personal técnico, deberán ser presentados la copia de todos los documentos respectivos.

- Para acreditar que el postor ganador cuenta con una herramienta de mesa de ayuda para la atención de la garantía ofertada, en modalidad 24x7, la herramienta debe registrar las incidencias o solicitudes del CENARES en un ticket de atención mediante una línea de telefonía fija o 0800, correo electrónico y/o vía online para la gestión del incidente, deberá acreditarse mediante una constancia.
- Para acreditar que el postor ganador cuenta con un Centro de Operaciones de Seguridad (SOC – Security Operation Center) propio o un Centro de Soporte y atención a clientes propio, precisando que el medio de atención de este SOC es remoto y deberá acreditar mediante una constancia firmada por el representante legal de la empresa.
- Para acreditar que el postor ganador se dedicada a la venta e instalación de licencias de seguridad gestionada (Adquisición de licencias e instalación de firewalls), deberá presentar carta del fabricante.

CENARES

Firmado digitalmente por CORDOVA ARANDIA Alfredo FAU 20538298485 soft
Motivo: Soy el autor del documento
Fecha: 18.02.2026 17:46:14 -05:00

_____

NOMBRE Y APELLIDO
FIRMA Y SELLO DEL JEFE DEL ÁREA USUARIA

6. REQUISITO DE CALIFICACIÓN

6.1. REQUISITOS DE CALIFICACIÓN OBLIGATORIOS

A. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 1,295,000.00 (Un millón doscientos noventa y cinco mil con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los diez años anteriores a la fecha de la presentación de ofertas, que se computan desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran bienes similares a los siguientes: venta de licencias de firewall, venta de soluciones de seguridad perimetral, venta de firewall para centro de datos.

Acreditación:

La experiencia del postor en la especialidad se acredita con un máximo de veinte contrataciones, mediante copia simple de: (i) contratos u órdenes de compra, 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[1], o comprobante de retención electrónico emitido por SUNAT por la retención del IGV[2]. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados[3], para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

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 asume que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considera, para la evaluación, las veinte primeras contrataciones indicadas en el **Anexo Nº 11** referido a la Experiencia del Postor en la Especialidad.

[1] El solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación fehaciente de la cancelación. Es válido el sello colocado por el cliente del postor (sea utilizando el término "cancelado" o "pagado").

[2] De acuerdo con el Régimen de Retenciones del Impuesto General a las Ventas (IGV).

[3] Se entiende "privados" como aquellos que no son entidades contratantes.

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

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de 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 N° 14.**

Las personas jurídicas resultantes de un proceso de reorganización societaria no pueden acreditar como experiencia del postor en la especialidad aquella que le hubieran transmitido como parte de dicha reorganización las personas jurídicas sancionadas con inhabilitación vigente o definitiva.

Cuando en los contratos, órdenes de compra 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 compra o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 11** referido a la Experiencia del Postor en la Especialidad.

En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que ejecutan conjuntamente el objeto del contrato.

6.2. REQUISITOS DE CALIFICACIÓN ADICIONALES

B. CAPACIDAD TÉCNICA Y PROFESIONAL

B.1. EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

Un (01) jefe de Proyecto:

- ✓ Experiencia mínima de dos (02) años como gestión de proyectos, como gestor de proyecto y/o supervisor de proyecto y/o administrador de proyectos; contabilizados desde la obtención del título profesional.

Un (01) Personal Técnico:

- ✓ Experiencia mínima de dos (02) años en implementación y/o soporte de equipos de seguridad perimetral, como especialista y/o implementador y/o técnico; contabilizados desde la obtención del título profesional.

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

Acreditación:

El postor debe señalar la denominación del puesto, cargo y/o posición, y tiempo de experiencia del personal clave propuesto (años, meses y días) en el **Anexo N° 19**, adjuntando en su oferta copia simple de cualquiera de los siguientes documentos: (i) contratos y su respectiva conformidad; (ii) constancias; (iii) certificados; o (iv) cualquier otra documentación que, de manera fehaciente, demuestre la experiencia del personal propuesto.

Estos documentos deben señalar los nombres y apellidos del personal clave; el cargo desempeñado 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 que acreditan la experiencia establezcan esta en meses sin especificar los días se debe considerar el mes completo. Se considera aquella experiencia que no tenga una antigüedad mayor a veinticinco años anteriores a la fecha de la presentación de ofertas. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo de la misma solo se considera una vez el periodo traslapado. En ningún caso corresponde exigir que el mismo personal clave acredite experiencia en más de un cargo.

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 debe validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.