ESPECIFICACIONES TÉCNICAS

ADQUISICIÓN E IMPLEMENTACIÓN DE SISTEMA DE PROTECCIÓN DE TRÁFICO WEB

1. OBJETO DE LA CONTRATACIÓN

Adquirir un sistema de Protección de Tráfico Web para garantizar la seguridad y disponibilidad de los sistemas y/o aplicativos del CENARES minimizando los ataques externos.

2. AREA USUARIA

Oficina de Tecnologías de la Información e Innovación – OTII

3. FINALIDAD PÚBLICA

La finalidad del presente requerimiento es adquirir e implementar un sistema de Protección de Tráfico Web en modalidad Cloud para garantizar la seguridad de los sistemas y/o aplicaciones web y así brindar plataformas tecnológicas con una mayor disponibilidad en los servicios que brinde CENARES.

4. ACTIVIDADES DEL POI

AOI00134500444 Implementación del Operador Logístico

5. ALCANCE Y DESCRIPCIÓN DEL BIEN

Se requiere la adquisición, instalación, configuración e implementación de un sistema de Protección de Tráfico Web.

PRESTACIÓN PRINCIPAL

5.1. Características técnicas mínimas

5.1.1. Generalidades

5.1.1.1. Se requiere un sistema de protección web brindado desde la nube para la protección de los sitios web de la organización, ante ataques a la capa aplicativa (Web Application Firewall) capaz de contener ataques como SQLi, XSS, RCE.

5.1.1.2. La solución ofertada debe ser provista en un esquema 100% de nube, sin la necesidad de implementación de elementos (tanto de hardware como de software) en las instalaciones de CENARES.

5.1.1.3. La solución debe soportar esquemas de implementación híbridos, mediante la integración de controles on-premise de la misma marca.

5.1.1.4. La solución ofertada debe ser capaz de mitigar ataques de denegación de servicio en la capa 7 hacia las aplicaciones de manera automatizada.

5.1.1.5. La solución ofertada debe poder acelerar el delivery del contenido de las aplicaciones de CENARES.

5.1.1.6. La solución ofertada deberá operar sin mayores cambios en la infraestructura de CENARES, pudiendo redireccionarse el tráfico de los clientes aplicativos mediante el uso de cambios en los servidores DNS de CENARES.

5.1.1.7. La solución ofertada para la protección de aplicaciones en nube debe ser operada 100% desde la nube, mediante portal web proporcionado por el proveedor.

5.1.1.8. La solución debe permitir incluir los certificados y llave SSL originales de los sitios, o bien generar automatizada mente (mediante mecanismos integrados con validaciones de CA) certificados válidos para los sitios a proteger.

5.1.1.9. La solución debe permitir crear Certificados SSL sin ningún costo adicional para la entidad en la consola de administración y asignar a al sitio protegido.

5.1.1.10. La solución debe integrarse con autoridades certificantes para la emisión de certificados válidos SSL mediante métodos de validación mediante cambios en las zonas DNS, o contacto mediante email válido (por ejemplo, admin@dominio o postmaster@dominio).

5.1.1.11. La solución debe permitir "enforzar" u obligar el uso de HTTPS de manera optativa por sitio.

5.1.1.12. La solución debe permitir la administración de los DNS.

5.1.1.13. La solución debe permitir monitoreo de protocolo SSL en los sitios protegidos.

5.1.2. Dimensionamiento

5.1.2.1. La solución requerida tiene como propósito proteger treinta (30) aplicaciones o sitios de CENARES. Las aplicaciones web están desarrolladas en lenguaje de programación .NET, Java y alojados en servidores en versión Windows Server 2012/2012R2,2019/2022, Ubuntu 22 y Linux Debian 6.0.

5.1.2.2. Se estima que el tráfico total de las aplicaciones a proteger es de 200 Mbps.

5.1.2.3. La solución provista debe contemplar asistencia o generación de reglas personalizadas bajo una administración del fabricante con disponibilidad 7x24 los 365 días, sin limitaciones o cargos extra.

5.1.2.4. La solución debe garantizar una disponibilidad mínima 99.99%.

5.1.3. Dashboards y Gestión

5.1.3.1. La solución debe permitir indagar en tiempo real los distintos eventos de seguridad, incluyendo los datos de los request individuales que han sido bloqueados o permitidos, los criterios evaluados y el detalle del request particular, con la posibilidad de buscar y filtrar por diferentes criterios.

5.1.3.2. La solución debe permitir agregar usuarios de gestión y visualización de CENARES, para que tengan acceso a la consola.

5.1.3.3. Los usuarios deben poder integrar múltiples factores de autenticación para loguearse/firmarse a la plataforma.

5.1.3.4. La solución debe generar reportes periódicos de seguridad.

5.1.3.5. La solución debe permitir la gestión mediante interface WEB como así también integración mediante API tanto para cambios de configuración como para monitoreo de estado, permitiendo alcanzar las mismas funcionalidades mediante ambos métodos de acceso.

5.1.3.6. La solución debe registrar e informar los cambios realizados por cada uno de los usuarios, con la finalidad de permitir la trazabilidad de actividades de gestión.

5.1.3.7. La solución debe contar con una herramienta que analice todos los eventos de seguridad y les aplique algoritmos de Machine Learning e Inteligencia Artificial para entregar los incidentes derivados del procesamiento de los eventos. Estos incidentes deberán estar clasificados por severidad (alta, media y baja) y entregarán todo el detalle relacionado como información de IPs, tipos de ataques, distribución, herramientas utilizadas, para que el equipo de seguridad de la entidad pueda procesarlos de manera eficiente, disminuyendo así la carga operativa y administrativa a la entidad.

5.1.4. Seguridad – WAF

5.1.4.1. La solución debe detectar ataques aplicativos de seguridad, incluyendo los mencionados en los informes de OWASP (SQL Injection, Command Injection, Remote File Inclusion, Cross Site Scripting, Cross Site Request Forgery).

5.1.4.2. La solución debe informar y alertar ataques a los aplicativos, pudiendo definir por política para cada aplicación, qué acciones tomar ante dichos eventos (ejemplo: bloquear el request individual, sólo alertar, bloquear la IP, etc.)

5.1.4.3. La solución debe proteger ante ataques de día cero, sin impacto de falsos positivos.

5.1.4.4. La solución debe incluir la posibilidad de definir reglas personalizadas de seguridad, utilizando los criterios necesarios y sintaxis lógica para definición de los casos particulares. Estos criterios deben incluir sin limitarse, al menos los siguientes:

- Dirección IP de origen
- País de origen (geolocalización)
- Existencia de header particular, evaluación de valores
- Existencia y valor de cookies
- Tipo de cliente (tipo de bot, humano, api client, etc)
- Método HTTP utilizado
- Número de request dentro de la sesión
- Parámetros y valores
- URL y URIs
- Cantidad de hits
- User Agent
- Referer
- Post Data
- Tamaño del Request
- Session request rate
- ASN de origen

5.1.4.5. La solución debe permitir tomar acciones personalizadas para las reglas de seguridad, incluyendo bloqueos de sesión, request, envío de Captchas, etc.

5.1.4.6. La solución debe llevar métricas y contadores, así como contabilizar en las alertas en tiempo real, los eventos identificados mediante las reglas personalizadas de seguridad.

5.1.4.7. Las reglas y cambios de configuración de seguridad deben propagarse en tiempo real o "near-real time" con un tiempo máximo para tomar efecto a nivel global de 1 minuto.

5.1.4.8. La solución debe permitir especificar whitelists o exclusiones para los controles, incluyendo parámetros como URLs, direcciones IP de origen, países, etc.

5.1.4.9. La solución provista debe tener su propia fuente de detección y creación de firmas y métodos de reconocimiento de ataques.

5.1.4.10. La solución debe ser propietaria y no estar basada en soluciones OpenSurce o depender de firmas de ModSecurity.

5.1.4.11. La solución debe garantizar por su cuenta la reducción de falsos positivos, revisando las firmas y políticas de detección de ataques antes de generar bloqueos, sin la necesidad de intervención por parte de personal de CENARES.

5.1.4.12. La solución deberá contar con funcionalidades que permitan:

- Rastrear e identificar las fuentes de los ataques originadas desde proxies anónimos, direcciones ip maliciosas, botnets y sitios de phishing.
- Actualizar las fuentes de ataque para identificar y bloquear el tráfico malicioso.
- Ajustar dinámicamente las políticas de seguridad con base en la identificación de las fuentes de ataque o de las fuentes que denoten actividad sospechosa.
- Bloquear solicitudes de acceso basado en la reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por Botnet, DDoS, Phishing o redes de Anonimización (TOR y Proxies Anónimos).
- Bloquear solicitudes de acceso basado en el país de origen de la conexión.
- Realice un análisis automático de distribución de alertas en relación al país de origen, con opción a representar la información a través de un mapa mundial
- Detallar y analizar los eventos de seguridad ocurridos, orígenes y método del ataque, dirección IP y localización geográfica del ataque.

5.1.5. Seguridad – Bots

5.1.5.1. La solución debe ser capaz de identificar bots (scripts automatizados sin interacción humana) accediendo a los sitios de manera transparente (sin afectar la experiencia de usuario original).

5.1.5.2. La solución debe clasificar los bots por tipo y permitir tomar acciones diferentes en base a este criterio, así como llevar estadísticas por sitio o aplicativo protegido

5.1.5.3. La solución debe permitir la detección de bots sin la necesidad de integrar código en las aplicaciones de CENARES.

5.1.5.4. La solución debe contar con algoritmos complejos y actualizados de detección y clasificación de bots y herramientas automatizadas, excediendo controles básicos de soporte de javascript y cookies.

5.1.5.5. La solución debe informar el porcentaje de bloqueos en tiempo real y acciones tomadas ante la presencia de Bots y herramientas automatizadas.

5.1.5.6. La solución debe prevenir el uso de bots del estilo "comment spammers"

5.1.5.7. La solución debe proteger ante el uso de herramientas de escaneo automatizadas

5.1.5.8. La solución debe proteger ante ataques automatizados mediante herramientas de scripting y librerías de hacking.

5.1.6. Seguridad - DDoS Aplicativo

5.1.6.1. La solución debe ser capaz de detectar DDoS aplicativo, específico para cada aplicación protegida para hasta 1 Gbps

5.1.6.2. Se deben poder excluir bots "benignos" como motores de búsqueda, Site Helpers, B2B API clients, etc.

5.1.6.3. La solución de detección y mitigación de ataques de DDoS aplicativo debe detectar no sólo ataques volumétricos y de protocolo, sino el abuso de objetos aplicativos que consuman recursos (como RAM o CPU) en los servidores, mediante análisis de comportamiento aplicativo, detección de anomalías, reputación de IP y clasificación de clientes.

5.1.6.4. La solución debe proteger de ataques de DDoS de manera distribuida y transparente, sin necesidad de redireccionar el tráfico a POPs o puntos de presencia específicos ante ataque, generando latencias y problemas de propagación y ruteo. Todos los POPs deben cumplir todas las funciones (Aceleración, WAF, Protección DDoS, etc).

5.1.6.5. La mitigación de los ataques de DDoS debe ser automatizada y "multi-vector".

5.1.6.6. Protección contra ataques DDoS en capa 3,4 y 7; y actualización virtual para proteger aplicaciones tipo legacy.

5.1.7. Seguridad - Inteligencia de ataques y análisis automatizado

5.1.7.1. La solución debe incluir sus propias métricas de reputación de IP, incluyendo detalles como tipos de ataques perpetrados por dichos orígenes en el pasado.

5.1.7.2. La solución debe mantener información de geo-localización de los orígenes.

5.1.7.3. La solución debe hacer análisis de malware y hacer eliminación automatizado del mismo.

5.1.7.4. Virtual Patching and Hardening para servidores de aplicaciones web en Windows IIS, Apache, NGINX, Nodo.js y Lighttpd.

5.1.7.5. La solución debe hacer análisis de los ataques, agregando eventos y alertas individuales en incidentes o ""narrativas"" de ataques y amenazas, incluyendo detalles útiles para el análisis de los ataques dirigidos, por ejemplo:

- ✓ Herramientas utilizadas

- ✓ Direcciones IP de origen y porcentaje de ataque por cada una
- ✓ Vectores de ataque
- ✓ Aplicaciones y recursos atacados
- ✓ Historial en el tiempo, incluyendo eventos bloqueados y/o alertados
- ✓ Muestra de eventos
- ✓ Análisis estadístico
- ✓ Integración con información de inteligencia (geolocalización, ataques previos a otros clientes, etc).

5.1.8. Aceleración de contenido

5.1.8.1. La solución debe brindar la posibilidad de acelerar el contenido mediante caché de elementos estáticos y dinámicos.

5.1.8.2. La solución debe perfilar y aprender automatizadamente (Machine Learning) las políticas de caching para cada elemento, en manera especial para contenido dinámico generado para cada cliente en particular.

5.1.8.3. La solución debe manipular activa y automáticamente el caché en los dispositivos de cliente en base a lo aprendido del comportamiento de la aplicación. Esta funcionalidad debe poder activarse y desactivarse por aplicación.

5.1.8.4. La solución debe permitir la definición del/los puntos de presencia más cercanos a los datacenters de origen para cada aplicación, con el fin de utilizar algoritmos de caché de capas múltiples, ruteo dinámico inteligente del contenido y reutilización del backbone de la CDN para acelerar el contenido a clientes remotos, reduciendo el RTT desde puntos de presencia (POPs) lejanos. La Infraestructura debe tener más de 40 POPs.

5.1.8.5. La solución debe permitir configurar y personalizar CDN de terceros.

5.1.8.6. La solución debe permitir medición de la performance de la aceleración del contenido, pudiendo revisar los tiempos, decisiones de caching o forward-to-origin para cada elemento particular de cada página. Esta información deberá incluir métricas como TTFB del servidor de origen, cache hits/miss, etc.

5.1.8.7. La propagación global de actualizaciones y reglas de cache debe ser en tiempo real o "near real time", nunca excediendo el minuto, al igual que las directivas de purga de caché.

5.1.8.8. Las técnicas combinadas de caché y aceleración deben incluir al menos:

- ✓ Validación asíncrona

MINISTERIO DE SALUD - A. CORDOVA

- ✓ Minificación de contenido CSS, JS y HTML
- ✓ Compresión de imágenes
- ✓ Compresión de contenido ""on the fly""
- ✓ Pre-Pooling de conexiones TCP"

5.1.8.9. Debe incluir opciones de configuración avanzadas como:

- ✓ Cumplir optativamente con directrices de ""no-cache"" o ""max-age"" de parte de los clientes
- ✓ Cumplir con headers ""Vary""
- ✓ Utilizar la duración mínima de cache ante conflictos
- ✓ Preferir ""last modified"" por sobre ""eTag""
- ✓ Deshabilitar la posibilidad de caching en el cliente
- ✓ Cachear las respuestas de headers 3XX (ej. redirecciones perpetuas)
- ✓ Caching basado en headers de respuesta.

5.1.8.10. La solución debe permitir configurar almacenamiento de caché inteligente.

5.1.8.11. La solución debe permitir configurar en modo de compresión Gzip.

5.1.8.12. La solución debe soportar HTTP/2 y permitir transformar automáticamente a este protocolo aplicaciones legacy HTTP/1.1

5.1.8.13. La solución debe soportar las últimas versiones de TLS y permitir la definición de protocolos soportados de manera estricta.

5.1.8.14. La solución debe soportar "geo-fencing", o la posibilidad de definir en qué regiones se almacena la data de las aplicaciones protegidas

5.1.8.15. La solución debe soportar HSTS

5.1.8.16. La solución debe permitir múltiples opciones de almacenamiento en caché para cada tipo de sitio web.

5.1.8.17. La solución debe permitir protección y optimización de velocidades combinadas de acuerdo al almacenamiento en caché para cada tipo de sitio web.

5.1.9. Aceleración – Monitoreo

5.1.9.1. La solución debe permitir configurar los parámetros de monitoreo para customizarlos por aplicación, incluyendo qué URLs monitorear, qué respuesta esperar, cuánto tiempo de timeout, intervalos de verificación, etc.

5.1.9.2. La solución debe alertar ante eventos de caída de los servicios o falta de llegada a los servidores protegidos del Cenares.

5.1.9.3. La solución debe contar con herramientas nativas de analítica basadas en AI (Inteligencia Artificial) y aprendizaje de máquina, que permitan crear un perfil de tráfico para la red de origen que se usa

como una línea de base para detectar ataques de todo tipo, XSS, DDoS, etc. A partir de ese momento, La herramienta deberá comparar la información de tráfico en tiempo real con la línea de base establecida para detectar ataques, así como la actualización de la línea de base en función de los nuevos perfiles de tráfico que se identifican.

5.1.10. Protección de APIs

5.1.10.1. La solución debe contar para los sitios protegidos la capacidad de proteger las APIs asociadas.

5.1.10.2. La solución debe permitir proporcionar la seguridad de APIs para el archivo de la misma, generando un modelo positivo automático para la protección de los riesgos de seguridad asociados.

5.1.11. Sistema de Administración

5.1.11.1. El sistema debe permitir descargar localmente la información generada de registros relacionados al funcionamiento de la solución, así como de las configuraciones de todos los módulos administrados y las políticas establecidas.

5.1.11.2. El sistema de administración permitirá crear los usuarios del sistema de acuerdo a los roles y/o funciones dentro del CENARES.

5.2. Instalación y configuración

Por cuanto la modalidad de ejecución es llave en mano, el contratista debe realizar todas las actividades que pongan en correcto funcionamiento la solución en su conjunto por adquirir.

Será responsabilidad del Contratista efectuar las tareas necesarias para la solución tecnología de Sistema de Protección de Tráfico Web.

La instalación y configuración del Sistema de Protección de Tráfico Web ofertada se realizará en 30 aplicaciones web, debe incluir la personalización de acuerdo a las mejores prácticas adoptadas para la entidad y la infraestructura.

Antes del inicio de la instalación y configuración, el contratista deberá entregar el Plan de Trabajo.

A la finalización correcta, la entidad debe emitir el acta de conformidad de instalación y configuración.

5.3. Embalaje y rotulado

No aplica

5.4. Transporte y seguros

No aplica

5.5. Garantía Comercial

- La garantía de la solución del sistema de Protección de Tráfico Web será de treinta y seis (36) 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.
- Se debe entender que dentro del periodo de garantía el contratista aceptará los cambios relación de los sitios a proteger inicialmente configurados, el cual deberán atender en un plazo máximo de diez (10) días calendario luego de la comunicación escrita o vía correo electrónico por parte del CENARES.

6. PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL

a. Mantenimiento Preventivo

No aplica

b. Soporte Técnico

- ✓ Periodo de soporte: treinta y seis (36) 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, a ser presentado para la suscripción del contrato y deberá ser enviado al correo licencias@cenares.gob.pe.
- ✓ 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, a ser presentado para la suscripción del contrato y deberá ser enviado al correo licencias@cenares.gob.pe
- ✓ El CENARES reportará cualquier tipo de requerimiento de soporte al número telefónico o a través de una comunicación con el personal encargado designado por el CONTRATISTA, las 24 horas, todos los días incluidos feriados.

MINISTERIO DE SALUD - CENARES - Dirección de Tecnologías de la Información e Innovación - A. CÓRDOVA - V°B° - Dirección de Recursos Estratégicos en Salud

- ✓ 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 la licencia.
- ✓ 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 Nº 1 – Plazos establecidos para la resolución de requerimiento de soporte.

Nº	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. El tiempo se contabiliza desde que el CONTRATISTA llega a CENARES y/o accede al/los servidores afectados.	Hasta 120 minutos.

c. Capacitación:

El CONTRATISTA deberá brindar capacitación al personal de la Oficina de Tecnologías de la Información e Innovación en la configuración, la cual deberá ser dictada por instructores certificados en ciberseguridad y Ethical Hacking v.12.

Las características de la transferencia de conocimiento deberán considerar como mínimo, lo siguiente:

- Tipo: Curso oficial
- Número de personas a capacitar: 03
- Lugar de transferencia de conocimiento: Forma Virtual
- Curso de Ciberseguridad: Se deberá considerar una capacitación de 67 horas lectivas como mínimo de ciberseguridad aplicada con una duración cronológica de 45 minutos por hora.
- Curso de Ethical Hacking v.12: Se deberá considerar una capacitación de 53 horas lectivas como mínimo en Ethical Hacking v.11 con una duración cronológica de 45 minutos por hora.

<u>02 instructores:</u>

El especialista que se va a encargar de la capacitación al personal de la Oficina de Tecnologías de la Información e Innovación.

<u>Requisitos:</u>

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) Experiencia mínima de dos (02) años como instructor o docente brindando capacitación en los cursos de ciberseguridad y Ethical Hacking v.12.

La acreditación de los instructores en ciberseguridad y Ethical Hacking v.12 deberán ser presentado para el perfeccionamiento del contrato.

La fecha de inicio de la capacitación será programada en coordinación con el área usuaria de la OTII, deberá ejecutarse dentro de los veinte días (20) calendarios posteriores de emitida el acta de conformidad de configuración y puesta en funcionamiento de la solución propuesta. La coordinación del inicio y fin de la

capacitación deberá ser sustentada o registrada mediante correo electrónico y/o documento entre ambas partes, para efecto de establecer los plazos.

7. REQUISITOS DEL PROVEEDOR

a. Del proveedor:

- ✓ Empresa con experiencia en venta e implementación de protección de tráfico web y bienes iguales o similares a los siguientes:
  - Licencias de herramientas de seguridad perimetral en Cloud.
  - Soluciones en Seguridad Perimetral, Firewall, Web Aplication Firewall, WAF, NFGFW, Cloud WAF y/o Firewall de Aplicaciones.
  - Soluciones on premise de seguridad de control de accesos NAC y que incluya la implementación, entrenamiento, mantenimiento y soporte.
  - Soluciones on premise de Firewalls, Switches, ips, instalación, configuración y puesta en producción.
  - Soluciones de seguridad perimetral externa.

- ✓ Empresa representante autorizada por la marca, que permita la comercialización de los productos de protección de tráfico web, para lo cual deberá acreditarlo con una carta del fabricante y/o subsidiaria local y/o subsidiaria regional que acredite lo solicitado, *los documentos solicitados deben ser presentados en la propuesta, para la admisión*.

b. Del Personal:

Se precisa que el postor debe contar con un equipo de trabajo para el soporte requerido. Este personal deberá estar compuesto por dos (02) personales claves.

01 especialista en Infraestructura:

El especialista debe estar certificado en la marca ofertada, se va a encargar de la infraestructura a instalar y configurar.

Requisitos:

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) Experiencia mínima de cuatro (04) años como especialista en Infraestructura de protección de tráfico web realizando instalación y configuración de licencias de protección de tráfico web.
c) **Copia del** certificado nivel técnico oficial en la marca ofertada.

01 especialista en operaciones:

El especialista se va a encargar de la operación de la solución a instalar y configurar.

Requisitos:

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) Experiencia mínima de cuatro (04) años como especialista en operación de protección de tráfico web.
c) **Copia de la** certificación técnica oficial en la marca o producto ofertada.

MINISTERIO DE SALUD - CENAS - Dirección de Tecnologías de la Información y Telecomunicaciones - A. CORDOVA - V°B° - Departamento de Recursos Estratégicos en Salud

Para acreditar los documentos de los literales a) y c) requeridos de los especialistas en Infraestructura y operaciones, deberán ser presentados para la suscripción de contrato, para lo cual deberá presentar la copia de todos los documentos respectivos.

Para acreditar el documento del literal b) requerido de los especialistas en Infraestructura y operaciones, deberán ser presentados como requisitos de calificación, para lo cual deberá presentar la copia de los documentos respectivos.

8. ENTREGABLES

PRESTACIÓN PRINCIPAL:

8.1. Plan de Trabajo:

El plan de trabajo deberá contener lo siguiente:

a) 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

b) El CONTRATISTA deberá entregar el Acta de entrega de bienes, mediante el cual se brindará la Conformidad de Entrega de Bienes de la Prestación Principal.

Acta de Entrega de Bienes de la Solución en el Almacén de CENARES (ver numerales 9 y 10.1).

8.2. Instalación y configuración

Informe técnico final sobre la solución instalada y configurada, Deberá contener lo siguiente:

a) El CONTRATISTA deberá entregar el manual de implementación.
b) El CONTRATISTA deberá entregar el acta de conformidad de instalación y configuración (indicada en el numeral 5.2).
c) Documento digital con las credenciales de acceso a la plataforma y/o licencia de uso.
d) Documento o enlace del manual de uso de la solución en formato PDF en idioma inglés y español.
e) Archivo digital del Backup de las políticas configuradas durante el proceso de implementación.

La presentación de cada entregable indicado en los numerales 8.1 y 8.2 serán dirigidos a la Oficina de Tecnologías de la Información e Innovación mediante Mesa de partes del CENARES ubicado en Jr. Nazca 548 — Jesús María de 8:00 a.m.

a 4:30 p.m. o mediante mesa de partes digital de acuerdo a tos términos y condiciones establecidos por el CENARES, según el plazo previsto para cada uno de los entregables.

PRESTACIÓN ACCESORIA:

8.3. Entregable del soporte técnico:

El proveedor deberá presentar tres informes de incidencias del soporte técnico (informes anuales) dentro de los treinta y seis (36) 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 6.

8.4. Entregable de Capacitación:

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

La presentación de cada entregable indicado en el numeral 8.3 y 8.4 serán dirigidos a la oficina de Tecnologías de la Información e Innovación mediante Mesa de partes del CENARES, ubicado en Jr. Nazca 548 – Jesús María de 8:00 a.m. a 4:30 p.m. o mediante mesa de partes virtual de acuerdo a los procedimientos y lineamientos establecidos por el CENARES en el mismo horario, según el plazo previsto para cada uno de los entregables.

9. PLAZO DE ENTREGA

PRESTACIÓN PRINCIPAL

El plazo de la prestación principal es de treinta (30) días calendario

- ✓ **Entrega del plan de trabajo** deberá ser entregado hasta los diez (10) días calendario contados desde el día siguiente de la suscripción del contrato.
- ✓ **Entrega de los bienes:** Hasta los diez (10) días calendario, contados desde el día siguiente de la suscripción del contrato.
- ✓ **Instalación y Configuración:** Hasta veinte (20) días calendario, contados a partir del día siguiente de la Conformidad de Entrega de Bienes de la Prestación Principal.

MINISTERIO DE SALUD – A. CORDOVA – VºBº

PRESTACIÓN ACCESORIA

El plazo de la prestación accesoria es de treinta y seis (36) meses.

- ✓ **Sobre el soporte técnico:**
  Treinta y seis (36) meses contados a partir del día siguiente de emitida el acta de conformidad de la prestación principal.
- ✓ **Sobre la capacitación:**
  El plazo de la capacitación será hasta veinte (20) días calendario, contados a partir del día siguiente de emitida la conformidad de instalación, configuración y puesta en operación de la solución ofertada.

10. LUGAR DE ENTREGA E INSTALACIÓN

10.1. Lugar de Entrega

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

10.2. Lugar de Instalación

La instalación se realizará en la Sede Central Jr. Nazca Nº 548 Jesús María – 2do Piso – Data Center.

11. RECEPCIÓN Y CONFORMIDAD

11.1. RECEPCIÓN DE BIENES

Dentro del almacén del CENARES (léase numeral 10.1 de las especificaciones técnicas), debiendo contar con la presencia de un representante del Almacén, un representante de la Oficina de Tecnologías de la Información e Innovación y un representante del CONTRATISTA.

11.2. CONFORMIDAD:

DE LA PRESTACIÓN PRINCIPAL:

- La conformidad será emitida por la Oficina de Tecnologías de la Información e Innovación, en un plazo de siete (07) días calendario luego de presentado el entregable correspondiente indicado en los numerales 8.1 y 8.2.

DE LAS PRESTACIONES ACCESORIAS:

- **Sobre el Soporte Técnico**
  La conformidad será emitida por la Oficina de Tecnologías de la Información e Innovación, en un plazo de siete (07) días calendario

luego de brindado cada soporte técnico anual y presentado el entregable correspondiente indicado en el numeral 8.3.

- **Sobre la capacitación:**
  La conformidad será emitida por la Oficina de Tecnologías de la Información e Innovación, en un plazo de siete (07) días calendario luego de realizado la capacitación y presentado el entregable correspondiente indicado en el numeral 8.4 de las especificaciones técnicas.

12. OTRAS OBLIGACIONES

a) La instalación se realizará en horarios fuera de oficina y en coordinación con el personal de la Oficina de Tecnologías de la Información e Innovación.
b) No se deberá paralizar las actividades dentro de horarios de oficina.
c) De paralizar el servicio, la fecha y hora programada deberá ser coordinada con la Oficina de Tecnologías de la Información e Innovación.
d) El CENARES designará un personal responsable, quien realizará las coordinaciones y supervisión de los trabajos de instalación.

13. FORMA DE PAGO

La forma de pago se realizará de la siguiente manera:

13.1. De la prestación principal

Pago se efectuará en moneda nacional, de la manera siguiente:

El 100% del monto ofertado de los bienes del numeral 5 y luego de la conformidad de instalación, configuración e inicio de operación:

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

- Recepción de los bienes por parte del Almacén del CENARES.
- Informe del funcionario responsable de la Oficina de Tecnologías de la Información e Innovación (OTII) emitiendo la conformidad correspondiente indicada en el numeral 11.2.
- Comprobante de pago.
- Guía de remisión.

MINISTERIO DE SALUD – CENARES – Oficina de Tecnologías de la Información e Innovación – A. CÓRDOVA – V°B° – Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud

13.2. De la prestación accesoria

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

El 33% del monto ofertado en el primer pago, 33% del monto ofertado en el segundo pago y finalmente 34% del monto ofertado en el tercer 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.

Sobre la capacitación:
El 100% del pago por el monto del acta de capacitación, previa conformidad del OTII.

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 8.4 de las especificaciones técnicas.

14. ADELANTOS
No aplica

15. MODALIDAD DE EJECUCIÓN CONTRACTUAL
Llave en mano.

16. SISTEMA DE CONTRATACIÓN
Suma Alzada

17. PENALIDAD
17.1. Penalidad por Mora

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto de la contratación, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

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

Penalidad diaria: Donde F tiene los siguientes valores:

a.1) Para plazos menores o iguales a sesenta (60) días:
Bienes, servicios en general y consultorías: F= 0.40

a.2) Para plazos mayores a sesenta (60) días:
Bienes, servicios en general y consulto rías: F= 0.25

Tanto el monto como el plazo se refieren, según corresponda, la contratación o ítem que debió ejecutarse o, en caso que estos involucraran obligaciones de ejecución periódica, a la prestación parcial que fuera materia de retraso.

Para efectos del cálculo de la penalidad diaria se considera el monto de la contratación

Se considera justificado el retraso, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. Esta calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.

De ser el caso, solo se podrá aplicar hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente u Orden de Compra, así como de ser el caso, del monto vigente del ítem que debió ejecutarse.

17.2. 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 Nº 2 Otras penalidades

Nº	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	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 Nº1 - Plazos establecidos para la resolución de requerimiento de soporte del numeral 6. b	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).
2	Cuando el PROVEEDOR supere el tiempo máximo de respuesta de 120 minutos para la atención de diagnóstico del reporte de	1 % del valor de una (01) UIT, por ocurrencia sobre el	Mediante informe de la Oficina de

	soporte técnico establecidos en el Cuadro Nº 1 — Plazos establecidos para la resolución de requerimiento de soporte del numeral 6. b	pago de mantenimiento y soporte técnico.	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.

18. NORMAS ANTICORRUPCIÓN

EL PROVEEDOR acepta expresamente que no llevará a cabo, acciones que están prohibidas por las leyes locales u otras leyes anticorrupción. Sin limitar lo anterior, EL PROVEEDOR se obliga a no efectuar algún pago, ni ofrecerá o transferirá algo de valor, a un funcionario o empleado gubernamental o a cualquier tercero relacionado con la adquisición aquí establecido de manera que pudiese violar las leyes locales u otras leyes anticorrupción, sin restricción alguna.

En forma especial, EL PROVEEDOR declara con carácter de declaración jurada que no se encuentra inmerso en ningún procedimiento de carácter penal vinculado a presuntos ilícitos penales contra el Estado Peruano, constituyendo su declaración, la firma del mismo en la Orden de compra de la que estos EETT forman parte integrante.

19. NORMAS ANTISOBORNO

EL PROVEEDOR, no debe ofrecer, negociar o efectuar, cualquier pago, objeto de valor o cualquier dádiva en general, o cualquier beneficio o incentivo ilegal en relación al contrato, que pueden constituir un incumplimiento a la Ley, tales como robo, fraude, cohecho o tráfico de influencias, directa o indirectamente, o a través de socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas, en concordancia o a lo establecido en el artículo 11° de la Ley de Contrataciones del Estado, Ley N° 30225 y sus modificatorias, y el artículo 7 de su Reglamento, aprobado mediante Decreto Supremo N° 344-2018-EF.

Asimismo, el proveedor se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participantes, integrantes de los órganos de administración apoderados, representantes legales, funcionarios, asesores y personas vinculadas en virtud a lo establecido en los artículos antes citados de la Ley de Contrataciones del Estado y su Reglamento.

Asimismo, el PROVEEDOR se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviere conocimiento; así también en adoptar medidas técnicas, prácticas, a través de los canales dispuestos por el CENARES.

De la misma manera, el proveedor es consciente que, de no cumplir con lo anteriormente expuesto, se someterá a la resolución del contrato y a las acciones civiles y/o penales que el CENARES pueda accionar.

20. CONFIDENCIALIDAD

La información y material producido bajo los términos del bien, tales como escritos, medios magnéticos, digitales y demás documentos generados, pasará a propiedad del CENARES. El 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.

Otras Condicionales

- Toda información que el CENARES proporcione al proveedor, deberá mantenerse en reserva y con la confidencial del caso; de probarse y demostrar lo contrario, se deberá tomar las acciones legales correspondientes.
- El proveedor es el único responsable ante el CENARES de cumplir con la prestación de la entrega de los bienes, no pudiendo transferir dicha responsabilidad a otras entidades y a terceros en general.
- El proveedor asume plena autonomía técnica y la responsabilidad para el desarrollo de sus actividades.
- El CENARES se reserva el derecho de comprobar la veracidad de toda la información proporcionada por el postor.

21. RESPONSABILIDAD POR VICIOS OCULTOS

La responsabilidad por vicios ocultos se aplicará por un plazo máximo de tres (03) años contado a partir de la conformidad otorgada por la instalación, configuración e inicio de operación.

ING. ALFREDO CÓRDOVA ARANDIA
Director
Oficina de Tecnologías de la Información e Innovación
Centro Nacional de Abastecimiento
de Recursos Estratégicos en Salud - CENARES
MINISTERIO DE SALUD

NOMBRE Y APELLIDO
FIRMA Y SELLO DEL JEFE DEL ÁREA USUARIA

A	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/. 300,000.00 (Trecientos mil 00/100 soles, por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 75,000.00 (Setenta y cinco mil con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa. Se consideran bienes similares a los siguientes: ✓ Licencias de herramientas de seguridad perimetral en Cloud. ✓ Soluciones en Seguridad Perimetral, Firewall, Web Aplication Firewall, WAF, NFGFW, Cloud WAF y/o Firewall de Aplicaciones. ✓ Soluciones on premise de seguridad de control de accesos NAC y que incluya la implementación, entrenamiento, mantenimiento y soporte. ✓ Soluciones on premise de Firewalls, Switches, ips, instalación, configuración y puesta en producción. ✓ Soluciones de seguridad perimetral externa. Acreditación: La experiencia del postor en la especialidad se acreditará con 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 váucher 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] correspondientes a un máximo de veinte (20) contrataciones.

[1] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

> *"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"*
> *(...)*
> *"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".*

	En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N.º 8 referido a la Experiencia del Postor en la Especialidad. En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) 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. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9. 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 8 referido a la Experiencia del Postor en la Especialidad.

MINISTERIO DE SALUD - Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud - A. CORDOVA - V°B°

B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.1	**EXPERIENCIA DEL PERSONAL CLAVE**

Requisitos:

01 especialistas en Infraestructura:

- ✓ Experiencia mínima de cuatro (04) años como especialista en Infraestructura de protección de tráfico web realizando instalación y configuración de licencias de protección de tráfico web.

01 especialistas en Operaciones:

- ✓ Experiencia mínima de cuatro (04) años como especialista en operación de sistema de protección de tráfico web.

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

Acreditación:

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

Importante
El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores. *Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.* *En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.* *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*