

ESPECIFICACIONES TÉCNICAS

ADQUISICIÓN DE UNA SOLUCIÓN DE BALANCEO DE CARGA Y MITIGACIÓN DE ATAQUES PARA APLICACIONES WEB CRÍTICAS DEL INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA, CORRESPONDIENTE A LA IOARR CON NÚMERO 2577341

1. ÁREA SOLICITANTE

Oficina Técnica de Informática del Instituto Nacional de Estadística e Informática – INEI.

2. OBJETO DE LA CONTRATACION

El presente proceso de selección tiene por objeto la Adquisición de Infraestructura Tecnológica de un sistema integral de balanceador de carga y firewall de aplicaciones web en alta redundancia que permitan al Instituto Nacional de Estadística e Informática mejorar la experiencia de uso de las aplicaciones web publicadas para uso de la ciudadanía.

3. FINALIDAD PUBLICA

Proteger la información del Instituto Nacional de Estadística e Informática para garantizar la continuidad de operación, así como la disponibilidad, integridad y confiabilidad de la información que acceden los ciudadanos a los diferentes sistemas del INEI.

4. REQUERIMIENTO

ITEM	DESCRIPCIÓN	UNIDAD DE MEDIDA
Paquete	Balanceador de Carga	Unidad
	Firewall de Aplicaciones Web (WAF)	Unidad

5. ESPECIFICACIONES TÉCNICAS

5.1 Solución de Balanceo de Carga para Aplicaciones Web Críticas

5.1.1 Características de la Solución

- 5.1.1.1 Throughput mínimo de Capa 4 de 8 Gbps.
- 5.1.1.2 Throughput mínimo de Capa 7 de 4 Gbps.
- 5.1.1.3 Debe tener al menos 120 GB de disco
- 5.1.1.4 Tener al menos 02 interfaces gigabit ethernet RJ-45 habilitados
- 5.1.1.5 Tener al menos 4 interfaces SFP 1 Gb, incluir 2 transceivers multimodo más patch cord de fibra ó 2 cables DAC/AOC de 5m por equipo.
- 5.1.1.6 Tener al menos 2 interfaces SFP+ 10 GE, incluir 2 transceivers multimodo más patch cord de fibra ó 2 cables DAC/AOC de 5m por equipo.
- 5.1.1.7 Debe contar con doble fuente de poder redundante activas

5.1.2 Requisitos Mínimos de Funcionalidad

- 5.1.2.1 Los dispositivos deben ser un equipo de propósito específico de balanceador.
- 5.1.2.2 Hardware de tipo appliance diseñado exclusivamente para la función específica de balanceador.
- 5.1.2.3 Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-ofsale o end-ofsupport (Fin de Vida o Fin de Ventas o Fin de Soporte) y no deberán tener reemplazo tecnológico anunciado. Se deberá adjuntar la ficha técnica (datasheet). El postor deberá presentar una declaración jurada de que los equipos ofertados, no tienen más de un año de fabricación en el mercado internacional hasta la fecha que se otorgue la buena pro en su propuesta.
- 5.1.2.4 Los equipos deben ser nuevos y de primer uso, evidenciándose con la carta del fabricante, la misma que se requerirá para el perfeccionamiento del contrato.
- 5.1.2.5 Debe soportar configuración en alta disponibilidad (HA), trabajando en un esquema de alta redundancia, para no permitir la pérdida de conexiones (2 equipos).
- 5.1.2.6 Debe soportar la creación de cuentas de administrador con diferentes perfiles y derechos de acceso basado en roles (RBAC);
- 5.1.2.7 El perfil de los administradores debe definirse sobre la base de los derechos a las diferentes funcionalidades de balanceo de carga.
- 5.1.2.8 Los derechos de acceso deben ser: Lectura, Escritura (y Lectura) y Sin acceso.
- 5.1.2.9 La solución debe soportar como mínimo un entorno de administración en los idiomas inglés o español.

5.1.3 Funcionalidades de Balanceo de Servidores

- 5.1.3.1 Debe soportar balanceo de Capa 7 para los siguientes protocolos HTTP, HTTPs.
- 5.1.3.2 Debe balancear el tráfico entre los servidores reales utilizando algoritmos propios y utilizando información de salud de los servidores.
- 5.1.3.3 Debe permitir la configuración de los perfiles que determinan el cifrado del tráfico entre el equipo (ADC) y los servidores reales.
- 5.1.3.4 Cuando existe comunicación cifrada, esta debe ser controlada por los protocolos SSL / TLS y la lista protocolos de cifrado.
- 5.1.3.5 Debe ser compatible con el protocolo TLS (v1.0, v1.1, v1.2).
- 5.1.3.6 Debe soportar por lo menos una suite de ciframiento.
- 5.1.3.7 Opcionalmente, debe ser capaz de reutilizar las sesiones SSL
- 5.1.3.8 Para cada uno de los servidores que participan en el algoritmo de balanceo de carga, debería ser posible configurar al menos dos de los siguientes: "Round Robin, Weighted Round, Robin, IP Hash, Least Connection".
- 5.1.3.9 El equipo proporcionado debe ser capaz de balancear las nuevas sesiones, pero preservando las sesiones existentes en el mismo servidor, usando persistencia de sesión.
- 5.1.3.10 Debe poderse configurar timeouts de conexión sobre las persistencias
- 5.1.3.11 El sistema debe permitir la selección del servidor real basado en la información de cabecera de paquetes TCP / IP y HTTP.

- 5.1.3.12 Debe permitir la selección del servidor real basado en el valor del campo de encabezado HTTP.
- 5.1.3.13 El sistema debe permitir la re-escritura de mensajes de HTTP request, HTTP response.
- 5.1.3.14 El sistema debe permitir la compresión de datos incluyendo: aplicaciones CSS, HTML, JavaScript.
- 5.1.3.15 El sistema debe permitir páginas de error enviadas a los clientes en caso de fallo en los servidores. Opcionalmente, estas páginas de error deben tener la opción para ser editadas.
- 5.1.3.16 Debe poderse implementar NAT, NAT64 y NAT46 (los dos últimos para permitir NAT en IPv4 e IPv6 entre clientes y servidores);
- 5.1.3.17 Debe soportar alta disponibilidad.

5.1.4 Funcionalidades de Red

- 5.1.4.1 Debe ser compatible con PPPoE
- 5.1.4.2 Debe soportar VLAN
- 5.1.4.3 Debe permitir el enrutamiento entre VLAN diferentes
- 5.1.4.4 Debe soportar la configuración de rutas estáticas
- 5.1.4.5 Debe ser posible configurar políticas de enrutamiento basado en direcciones IP de origen y / o destino
- 5.1.4.6 Debe ser compatible con OSPF v2 - RFC 2328
- 5.1.4.7 Debe poderse implementar NAT (Network Address Translation), de los siguientes tipos: Source NAT (cambiar la dirección IP de origen), mapeo 1-1 y traslado de puertos (TCP o UDP)
- 5.1.4.8 Debe asignar políticas de ancho de banda, teniendo en cuenta la dirección de origen, destino y el servicio (puertos TCP y UDP)

5.1.5 Funcionalidades de Global Server Load Balancing

- 5.1.5.1 Debe ofrecer servicio DNS o SmartDNS
- 5.1.5.2 Debe ofrecer servicios como un DNS Autoritativo
- 5.1.5.3 Debe soportar DNS64 para permitir la comunicación entre clientes IPv4 con servidores IPv6 en el contexto de balanceo de carga global
- 5.1.5.4 Debería permitir establecer los sitios basados en la ubicación geográfica de configuración (países). La base de datos que asocia direcciones IP a los países debe ser desarrollado y gestionado por el fabricante (opcional).
- 5.1.5.5 Debe soportar la creación de políticas de DNS. Se entiende por políticas de DNS la forma en que el balanceador interpreta y responde a una petición DNS
- 5.1.5.6 Para cada uno de los posibles sitios remotos debe ser posible asignar peso a estos, para que este parámetro se tenga en cuenta en la secuencia de distribución de la respuesta de DNS.
- 5.1.5.7 Debe permitir el cambiar los puertos HTTP, HTTPS, Telnet y SSH para fines de acceso remoto del equipo por el administrador
- 5.1.5.8 Debe ser compatible con la sincronización de hora a través de NTP
- 5.1.5.9 Debe permitir la actualización programada de firmas y de Base de Datos a través de la línea de comandos o de la interfaz gráfica
- 5.1.5.10 Debe permitir proceso de upgrade de firmware

5.1.5.11 Debe ser compatible con la configuración de un servidor de correo para el envío de alertas o logs por correo electrónico (SMTP)

5.1.5.12 Debe contar con servicio de agente SNMP v1, V2c y 3

5.1.6 Funcionalidades de Reportes y Logs

5.1.6.1 El sistema debe tener un panel, a través de la interfaz gráfica que permite al administrador ver la información sobre el sistema, incluyendo al menos: el estado del sistema (uso de CPU, uso de memoria, número de conexiones actuales, ancho de banda utilizado, últimos registros) y el balanceo de carga.

5.1.6.2 Debe mostrar los registros de eventos y el tráfico de datos o log de red, incluidas las actividades de los administradores del sistema o log de configuraciones.

5.1.6.3 Permitir configurar un servidor syslog el cual será proporcionado por el INEI.

5.1.6.4 Debe permitir los siguientes estados de log: Emergencia, Alerta, crítico, error, advertencia, notificación, información y Debug.

5.1.6.5 Debe permitir seleccionar el tipo de registro para ser enviados al servidor syslog

5.1.6.6 La solución debe ser compatible con el envío de alertas o logs a través de mensajes de correo electrónico.

5.2 Solución Firewall de Aplicaciones Web (WAF)

5.2.1 Características de la solución:

5.2.1.1 Throughput mínimo para HTTP de 1.2 Gbps

5.2.1.2 Mínimo de 4 interfaces de 1Gbps RJ-45 habilitados

5.2.1.3 Mínimo de 4 interfaces de 1Gbps SFP, incluir 2 transceivers multimodo más patch cord de fibra ó 2 cables DAC/AOC de 8m por equipo.

5.2.1.4 Tener al menos 2 interfaces SFP+ 10 GE, incluir 2 transceivers multimodo más patch cord de fibra ó 2 cables DAC/AOC de 8m por equipo.

5.2.1.5 Almacenamiento de 450 GB SSD

5.2.1.6 Debe contar con doble fuente de poder redundante activas.

5.2.1.7 Los dispositivos deben ser un equipo de propósito específico.

5.2.1.8 Hardware de tipo appliance diseñado exclusivamente para la función específica de protección de aplicaciones web (WAF).

5.2.1.9 Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.

5.2.1.10 Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support (Fin de Vida o Fin de Ventas o Fin de Soporte) y no deberán tener reemplazo tecnológico anunciado. Se deberá adjuntar la ficha técnica (datasheet).

5.2.1.11 Los equipos deben ser nuevos y de primer uso, evidenciándose con la carta del fabricante, la misma que se requerirá para el perfeccionamiento del contrato.

5.2.1.12 Debe soportar configuración en alta disponibilidad (HA), trabajando en un esquema de alta redundancia, con todas las licencias de software habilitadas para no permitir la pérdida de conexiones (2 equipos).

5.2.2 Funcionalidades de Red:

- 5.2.2.1 La solución debe de ser capaz de ser implementada en modo Proxy (Transparente y Reverso).
- 5.2.2.2 Sistema operacional / firmware debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadores disponibles gratuitamente y protocolo HTTPS, y también por CLI (interface de línea de comando), accediendo localmente por puerto de consola, o remotamente vía SSH
- 5.2.2.3 Debe de proveer, en la interfaz de gestión, las siguientes informaciones del sistema para cada equipo: consumo de CPU y estadísticas de conexión
- 5.2.2.4 Debe de ser posible visualizar en la interfaz de gestión la información de consumo de memoria y los discos de log
- 5.2.2.5 Debe de incluir herramienta dentro de la interfaz gráfica de gestión (dashboard) que permita visualizar los últimos logs de ataques detectados/bloqueados
- 5.2.2.6 Debe proveer las siguientes informaciones en la interfaz gráfica de gestión: estadísticas de throughput HTTP en tiempo real, estadísticas de eventos de ataques detectados/bloqueados, y los últimos logs de eventos del sistema o de configuración
- 5.2.2.7 Debe soportar los protocolos de monitoreo SNMP v1, SNMP v2c e SNMP v3
- 5.2.2.8 Debe ser capaz de realizar notificación de eventos de seguridad a través de e-mail, traps SNMP y Syslog
- 5.2.2.9 La solución deberá de soportar almacenar logs localmente en disco y en servidor externo vía protocolo SYSLOG
- 5.2.2.10 La solución debe tener la capacidad de enviar alertas o logs por email
- 5.2.2.11 La solución debe tener datos conteniendo la localización geográfica de los clientes web.
- 5.2.2.12 Debe tener la capacidad de generar reportes

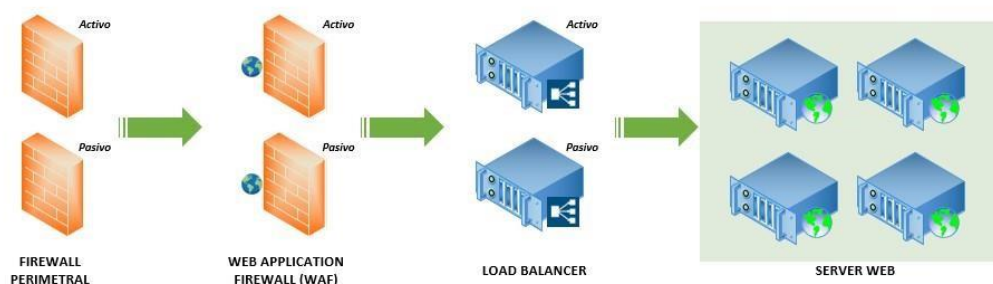
5.2.3 Funcionalidades de Web Application Firewall

- 5.2.3.1 Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de virus y reputación IP, actualizado de forma automática.
- 5.2.3.2 La solución debe permitir utilizar la base de datos completa de protección del fabricante contra virus.
- 5.2.3.3 Tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs.
- 5.2.3.4 Tener la capacidad de protección contra ataques del tipo SQL Injection, Botnet, acceso por fuerza bruta, Data leakage, Cross Site Request Forgery (CSRF), cross site scripting (XSS), Remote File Inclusion (RFI), DoS Protection, cambios de cookie o cookie tampering, Directory Traversal.
- 5.2.3.5 Debe tener protección contra ataques de Denial of Service (DoS);
- 5.2.3.6 Tener la capacidad de protección contra ataques del tipo SYN flood
- 5.2.3.7 Contar con algún mecanismo de protección contra ataques de días cero.
- 5.2.3.8 Tener la capacidad de configurar protección del tipo TCP SYN flood-style para prevención de DoS.
- 5.2.3.9 Debe soportar crear políticas de geo-localización, permitiendo que el tráfico de determinado país sea bloqueado

- 5.2.3.10 Permitir configurar listas negras de bloqueo y listas blancas de confianza, basadas en dirección IP de origen
- 5.2.3.11 Tener la funcionalidad de proteger el website contra acciones de defacement, con recuperación automática y rápida del website en caso de fallo
- 5.2.3.12 Debe ser capaz de hacer aceleración de SSL
- 5.2.3.13 La solución debe tener la capacidad de almacenar certificados digitales o cadenas de confianza
- 5.2.3.14 La solución debe de tener un sistema de reputación de direcciones IP públicas conocidas como origen de ataques de DDoS y botnets.
- 5.2.3.15 La solución debe permitir crear reglas definiendo el orden con que las páginas deben de ser accedidas para prevenir ataques como cross-site request forgery (CSRF).
- 5.2.3.16 La solución debe de tener la capacidad de definir restricción a determinados métodos HTTP
- 5.2.3.17 Debe de ser capaz de hacer compresión, para reducir la cantidad de información enviada al cliente
- 5.2.3.18 Permitir redirección de requisiciones HTTP para HTTPS
- 5.2.3.19 Permitir añadir el campo X-Forwarded-For para identificación de la dirección IP real del cliente.
- 5.2.3.20 La solución debe de soportar reglas para definir si las requisiciones HTTP serán aceptadas en función de la URL o URI y origen de la petición.
- 5.2.3.21 La solución debe de soportar políticas de control de acceso.
- 5.2.3.22 Tener capacidad de web cache.
- 5.2.3.23 La solución deberá actualizar la base de datos de firmas
- 5.2.3.24 La solución debe incluir la funcionalidad de balanceo de carga entre servidores web
- 5.2.3.25 Soportar algoritmos para balanceo de carga entre servidores tales como Round Robin, Weighted Round Robin, Least Connection o Weighted Least Connection.
- 5.2.3.26 Permitir prueba de disponibilidad del servidor web.
- 5.2.3.27 La solución o alguno de sus métodos de balanceo debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor.

5.3 Diagrama referencial de la solución a implementar

Los postores, deberán ofrecer equipos separados para garantizar una alta redundancia, con una configuración Activo-Pasivo. La solución no podrá ser ofertada 2 en 1 (WAF y Balanceador).



6. REQUISITOS DEL POSTOR:

- 6.1 El postor debe ser partner autorizado en la marca de la solución ofertada en el Perú. Esto se deberá acreditar mediante carta de fabricante dirigida al proceso.
- 6.2 El postor deberá contar con un Centro de Operaciones de Red (NOC) y Centro de Operaciones de Seguridad (SOC) y/o CyberSOC el cual deberá operar 24x7 y estar instalado en Perú que brinde soporte a los equipos configurados dentro del servicio. Esto se deberá acreditar mediante copia de documentos que sustenten la propiedad, posesión, el compromiso de compra venta o alquiler u otro documento que acredite la disponibilidad de la infraestructura estratégica requerida.
- 6.3 El postor deberá sustentar en su propuesta el cumplimiento de CARACTERÍSTICAS Y ESPECIFICACIONES TÉCNICAS mediante declaración jurada según ANEXO 1 y mediante Brochure y/o datasheet y/o documentos y/o manuales técnicos del fabricante, se aceptará carta del fabricante dirigido al proceso.
- 6.4 El postor deberá presentar una declaración jurada acompañada con una carta de fabricante de los equipos ofertados no tienen más de un año de fabricación en el mercado internacional hasta la fecha que se otorgue la buena pro en su propuesta.

7. PRESTACIÓN ACCESORIA A LA PRESTACIÓN PRINCIPAL:

7.1 CAPACITACIÓN

Deberá incluirse la capacitación y certificación oficial del fabricante de la solución ofertada a todo costo de manera remota o presencial para cuatro (4) personas:

- Configuración y administración de la solución ofertada.
- Laboratorios prácticos.

El contratista deberá entregar un voucher, certificado, cupón o constancia de asistencia del curso oficial certificado de la marca para cuatro (4) personas para que se programen en base al cronograma del curso oficial. Todos los cursos deberán ser dictado en español.

Material didáctico y/o certificados deberán ser brindados de manera electrónica a cada participante. El curso deberá ser basado en las horas determinadas por el syllabus oficial del fabricante de mínimo 24 horas lectivas.

7.2 MANTENIMIENTO PREVENTIVO

El proveedor deberá efectuar un (01) servicio de mantenimiento preventivo por cada año que dure la garantía ofrecida, la misma que será comunicará vía correo electrónico por parte de OTIN, el contratista deberá confirmar la ejecución de la prestación dentro de las 24 horas de recibido el correo. Esta consiste en actualización de BIOS, firmware y drivers, identificación de eventos que puedan afectar la operación de la solución, entre otros.

Al finalizar cada mantenimiento preventivo, el contratista deberá hacer entrega de un informe en formato digital que será dirigido a la Oficina Técnica de Informática el cual indique las acciones realizadas durante el mantenimiento (Fechas, reportes, eventos, alertas, estado de salud del hardware o Software de toda la solución).

7.3 SOPORTE TÉCNICO

- 7.3.1 El proveedor deberá tener un centro de operaciones de seguridad (SOC), ubicado en Lima, en modalidad 24x7.
- 7.3.2 No deberá haber límite en la cantidad de tickets que se puedan solicitar para las atenciones.
- 7.3.3 Se deberá contar con atención vía remota (vía telefónica o por correo electrónico), o vía presencial en caso de ser necesario.
- 7.3.4 El proveedor proporcionará las actualizaciones de firmware y de la solución en general durante la vigencia del contrato y/o servicio de soporte.
- 7.3.5 Siendo los tiempos de atención definitiva, de acuerdo a la siguiente clasificación
- 7.3.6 De la atención: (las prioridades son ajustadas acorde a la naturaleza de la solicitud y/o criticidad de la misma)
- 7.3.7 Tiempo de atención de un ticket de prioridad *alta (Indisponibilidad total del equipamiento o de los servicios soportados por la misma), en un plazo no mayor a 04 horas, posteriores a la solicitud realizada por teléfono o correo electrónico.
- 7.3.8 Tiempo de atención de un ticket de prioridad *media (Afectación parcial del equipamiento o de los servicios soportados por la misma), en un plazo no mayor a 08 horas, posteriores a la solicitud realizada por teléfono o correo electrónico.
- 7.3.9 Tiempo de atención de un ticket de prioridad *baja (Afectación mínima del equipamiento de los servicios soportados por la misma), en un plazo no mayor a 24 horas, posteriores a la solicitud realizada por teléfono o correo electrónico.

Se considera un SLA mínimo de 99.95%, para la atención en el soporte técnico el cual se detalla a continuación.

DESCRIPCIÓN DE PRIORIDAD	TIEMPO MAXIMO DE ATENCIÓN
Prioridad alta	no mayor a 4 horas
Prioridad media	no mayor a 8 horas
Prioridad baja	no mayor a 24 horas

Y se aplicaran otras penalidades según el numeral 15.2

- 7.3.10 En caso el ticket de atención debe ser atendido o escalado al fabricante, el tiempo que se requiera para la atención debe estar dentro de numeral 7.3.9.
- 7.3.11 Garantizar en toda circunstancia la posibilidad de escalamiento del servicio con el Fabricante.
- 7.3.12 Soporte técnico especializado y/o local por parte del contratista y/o del fabricante durante el período de garantía (5 años).
- 7.3.13 El contratista deberá realizar un informe de atención de incidencias cada 3 meses en formato digital la cual será dirigido a la OFICINA TECNICA DE INFORMATICA

8. MODALIDAD DE EJECUCIÓN CONTRACTUAL

Llave en mano y a todo costo.

9. ENTREGABLES DE LA PRESTACION PRINCIPAL

- a) Guía de Remisión de los bienes ofertados.
- b) Guía de Remisión y documento que acredite el licenciamiento de toda la solución ofertada a nombre del INEI.
- c) Guía de Remisión de los Materiales utilizados.
- d) Informe técnico final de la implementación (Instalación, configuración y puesta en funcionamiento) del sistema integral de balanceador de carga y firewall de aplicaciones web, con el siguiente detalle:
 - ✓ Arquitectura final de la solución implementada.
 - ✓ Configuración y puesta en operación de toda la solución ofertada, que incluya las pruebas de failover donde se demuestre la operatividad.
 - ✓ Entrega de Credenciales de la solución implementada.
 - ✓ Pruebas de Conectividad y puesta en producción.
 - ✓ Plan de Proyecto de la ejecución de la prestación debidamente foliado y visado por el responsable del proyecto
- e) Plan de Mantenimiento Preventivo, que indique los trabajos y cronogramas anuales a realizar durante los cinco (05) años de su ejecución.
- f) Acta de garantía de la solución ofertada.

9.1 PRESTACIÓN ACCESORIA A LA PRESTACIÓN PRINCIPAL

9.1.1 CAPACITACIÓN

Certificado del curso oficial certificado de la marca hasta a los cincuenta (50) días, previamente el Contratista a los 30 días calendarios de suscrito el contrato deberá entregar el voucher, certificado, cupón o constancia de inscripción al curso oficial para cuatro (04) personas, a través de un documento dirigido a la Oficina Ejecutiva de Abastecimiento y Servicios - OEAS.

9.1.2 MANTENIMIENTO PREVENTIVO

Informe del mantenimiento preventivo, por cinco (05) veces, los cuales deberán ser entregados a los 368; 733; 1,098; 1,463 y 1,828 días calendarios contabilizados del día siguiente de otorgada la conformidad de la prestación principal.

9.1.3 SOPORTE TÉCNICO

Informe de soporte técnico que incluya los reportes de incidencias solucionadas describiéndose el número de incidencias, fecha de inicio, hora de inicio, descripción de la incidencia, descripción de la solución, fecha de finalización, hora de finalización y otros datos relevantes que requieran adjuntarse, los cuales deberán ser entregados a los 93, 183, 273, 363, 453, 543, 633, 723, 813, 903, 993, 1083, 1173, 1263, 1353, 1443, 1533, 1623, 1713, 1803 días.

10. LUGAR DE LA PRESTACIÓN

10.1 PRESTACIÓN PRINCIPAL

10.1.1 ENTREGA DE LOS BIENES

La entrega se realizará en días calendario en el almacén central del INEI sito en Jr. Juan Antonio Ribeyro N° 142- Jesús María; en el horario de 09:00 a 12:00hrs y de 14:00 a 17:00hrs de lunes a viernes; el INEI no está obligado a recibir equipos en horarios no programados. En caso de feriados la recepción del bien será al primer día siguiente laborable.

10.1.2 LUGAR DE INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO

Toda la solución debe ser instalada, configurada y puesta en funcionamiento por el CONTRATISTA en el Data Center de la Sede Central del INEI, ubicada en Jr. General Garzón 654658 Jesús María; previa coordinación con la Oficina Técnica de Informática, para su instalación y configuración de la solución ofertada.

10.2 PRESTACIÓN ACCESORIA A LA PRESTACIÓN PRINCIPAL

10.2.1 CAPACITACION

La capacitación se dará en el centro de instrucción o entrenamiento de la marca de forma presencial o virtual. Así mismo previa coordinación con la entidad podría darse en la Sede Central del INEI, ubicada en la Av. General Garzón 654-658 Jesús María.

10.2.2 MANTENIMIENTO PREVENTIVO

El mantenimiento preventivo, se dará a la solución adquirida instalada, configurada y puesto en funcionamiento en el Data Center de la Sede Central, ubicada en la Av. General Garzón 654658 Jesús María, previa coordinación con la Oficina Técnica de Informática.

10.2.3 SOPORTE TÉCNICO

El soporte técnico se dará de forma remota y/o presencial a la solución adquirida instalada, configurada y en pleno funcionamiento en el Data Center de la Sede Central, ubicada en la Av. General Garzón 654-658 Jesús María, previa coordinación con la Oficina Técnica de Informática.

11. PLAZO DE EJECUCIÓN DE LA PRESTACIÓN

11.1 PRESTACIÓN PRINCIPAL

11.1.1 PLAZO DE ENTREGA DE LOS BIENES

El plazo de entrega de los equipos para la solución requerida será de hasta sesenta (60) días calendarios contabilizados desde el día siguiente a la suscripción del contrato.

11.1.2 PLAZO DE INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO

El plazo de implementación de la solución ofertada será de hasta treinta (30) días calendarios, contabilizados a partir del día siguiente de la fecha de la entrega del hardware en el Almacén Central del INEI, para lo cual al finalizar la implementación deberán entregar Acta de Implementación de la solución.

11.2 PRESTACIÓN ACCESORIA A LA PRESTACIÓN PRINCIPAL

11.2.1 CAPACITACION

La capacitación (curso oficial) por la marca deberá llevarse a cabo en un plazo máximo de cincuenta (50) días calendarios, contados a partir del día siguiente de entregados los

vouchers, certificados, cupones o constancias de inscripción al curso oficial para cuatro (04) personas.

11.2.2 MANTENIMIENTO PREVENTIVO

El Mantenimiento preventivo deberá realizarse durante los mil ochocientos veinticinco (1,825) días calendarios, contabilizado a partir del día siguiente de otorgada la conformidad de la prestación principal.

11.2.3 SOPORTE TÉCNICO

El plazo del soporte técnico será de mil ochocientos veinticinco (1,825) días calendarios contados a partir del día siguiente de la conformidad de prestación principal.

12. GARANTÍA COMERCIAL DEL BIEN

- Garantía mínima de cinco (05) años como mínimo sobre el equipamiento propuesto
- Deberá incluir cambio de equipo/partes y apertura de casos con el fabricante y/o contratista, la cual deberá ser atendida.

Para los casos de falla de componentes, partes y/o piezas el contratista deberá brindar la solución en un plazo no mayor de 8 horas contados a partir de la respuesta del ticket, para el caso de cambio de equipos el reemplazo se debe realizar en un plazo no mayor de 48 horas contados a partir de la respuesta del ticket.

- La garantía se contabilizará a partir del día de la conformidad de la solución ofertada.

13. PAGOS

- La Entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad de la prestación principal y/o accesorias, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.
- En el caso que se haya suscrito contrato con un consorcio, el pago se realizará de acuerdo a lo que se indique en el contrato de consorcio.

14. FORMA DE PAGO

14.1 PRESTACIÓN PRINCIPAL:

El pago se efectuará en un único pago en soles, dentro del plazo de los diez (10) días calendarios siguientes de presentada los entregables completos detallados en el **numeral 9** (finalizada la implementación de la solución y puesta en producción) de las especificaciones técnicas, factura y la conformidad respectiva de acuerdo al Art. 171 Reglamento de la Ley de Contrataciones del Estado.

14.2 PRESTACIÓN ACCESORIA A LA PRESTACION PRINCIPAL:

Los pagos de las prestaciones accesorias se realizarán de la siguiente manera:

Descripción	Forma de Pago
Capacitación	01 Pago único
Soporte Técnico	20 Pagos trimestrales

Mantenimiento Preventivo	05 Pagos anuales
--------------------------	------------------

Para otorgar la respectiva conformidad se verificará la calidad, cantidad y cumplimiento de las condiciones establecidas en las Especificaciones Técnicas, debiendo realizar las pruebas necesarias para tal efecto. En caso de existir observaciones se procederá a no dar brindar la conformidad del mismo.

15. PENALIDADES POR MORA

15.1 POR MORA:

Si el contratista incurre en retraso injustificado en la entrega del bien y/o servicio, el INEI le aplicará una penalidad por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente o de ser el caso, del monto del Ítem que debe ejecutarse, en concordancia con el artículo 162° del Reglamento de la Ley de Contrataciones del Estado.

En todos los casos, la penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente formula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{Monto del contrato}}{F \times \text{Plazo en días}}$$

Donde F tiene los siguientes valores:

- a) Para plazos menores o iguales a sesenta (60) días, F= 0.40.
- b) Para plazos mayores a sesenta (60) días: F = 0.25

15.2 OTRAS PENALIDADES

Estas penalidades se calculan de forma independiente a la penalidad por mora, siendo estos los siguientes:

SUPUESTO DE APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO DE VERIFICACIÓN DE SUPUESTOS A PENALIZAR SEGÚN ART. 163 DEL RLCE.
Por incumplimiento en el plazo de la implementación de la solución. Tal como se describe en el numeral 11.1.2.	Penalidad aplicada será de 3 % de la UIT por cada día de retraso.	Documento de entrega Acta de Implementación de la solución ofertada.
Por incumplimiento de la capacitación para cuatro (04) personas. Según lo estipulado en el numeral 7.1 Capacitación de las Especificaciones Técnicas.	Penalidad aplicada será de 3 % de la UIT por cada día de retraso.	Documento de entrega de certificados y material exclusivo de la solución implementada.

Cuando supere el tiempo máximo de atención de incidentes, según lo estipulado en el numeral 7.3 de las Especificaciones Técnicas.	Penalidad aplicada será de 3 % de la UIT por hora o fracción	Documento de entrega de un informe de atención
Por incumplimiento de la fecha programada previa coordinación con la OTIN al mantenimiento preventivo en el plazo estipulado en el numeral 7.2 de las Especificaciones Técnicas.	Penalidad aplicada será de 3 % de la UIT por cada día de retraso	Documento de entrega de un informe en formato digital.
Por incumplimiento de acuerdo a lo establecido en el numeral 7.3.9 SLA 90% <= 99.94 %	Penalidad aplicada será de 3 % de la UIT por cada día de retraso	Documento de entrega de un informe en formato digital.
Por incumplimiento de acuerdo a lo establecido en el numeral 7.3.9 SLA 80% <= 89.9 %	Penalidad aplicada será de 4 % de la UIT por cada día de retraso	Documento de entrega de un informe en formato digital.
Por incumplimiento de acuerdo a lo establecido en el numeral 7.3.9 SLA menor a 79%	Penalidad aplicada será de 5 % de la UIT por cada día de retraso	Documento de entrega de un informe en formato digital.

16. CONFORMIDAD

La conformidad será emitida por la OTIN, luego de haber recibido los entregables correspondientes a cada prestación.

16.1 PRESTACIÓN PRINCIPAL

La conformidad será emitida por la OTIN, dentro de un plazo máximo de siete (07) días calendarios de producida la recepción de bienes y entregables finales indicados en el **numeral 9.d** de la prestación principal. Salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en caso la conformidad se emite en un plazo máximo de quince (15) días calendarios.

16.2 PRESTACIÓN ACCESORIA A LA PRESTACION PRINCIPAL

16.2.1 Prestación accesoria: Capacitación

La conformidad será emitida por la OTIN, dentro de un plazo máximo de siete (07) días calendarios de producida la recepción de los entregables emitidos por el contratista indicados en los **numerales 9.1.1 y 11.2.1**.

16.2.2 Prestación accesoria: Mantenimiento Preventivo

La conformidad será emitida por la OTIN, dentro de un plazo máximo de siete (07) días calendarios de producida la recepción de los entregables emitidos por el Contratista, indicados en el **numerales 9.1.2 y 11.2.2**

16.2.3 Prestación accesoria: Soporte técnico

La conformidad será emitida por la OTIN, dentro de un plazo máximo de siete (07) días calendarios de producida la recepción de los entregables emitidos por el Contratista, indicados en el **numerales 9.1.3 y 11.2.3**

La recepción conforme de la ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos de acuerdo con el Art. 173 Reglamento de la Ley de Contrataciones del Estado.

17. REQUERIMIENTOS DE LA EMPRESA

17.1 DEL PERSONAL

17.1.1 Un (01) Jefe de Proyecto

Encargado de la realización de la reunión de inicio de servicio, desarrollo de cronograma de actividades, provisión del equipamiento propuesto, gestión de tiempos de instalación, elaboración de documentación administrativa y gestión de coordinaciones con el área correspondiente de la Entidad

Requisitos:

TITULO PROFESIONAL en Ingeniería de sistemas, Electrónica, Informática, Computación e Informática, Telecomunicaciones y/o carreras afines del personal clave requerido como Jefe de Proyecto.

Acreditación:

El TITULO PROFESIONAL, será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <https://enlinea.sunedu.gob.pe/> o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: <http://www.titulosinstitutos.pe/>, según corresponda.

En caso el TITULO PROFESIONAL, no se encuentre inscrito en el referido registro, el postor ganador de la buena pro debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida para la suscripción del contrato.

17.1.2 Dos (02) Especialistas Técnicos de la solución ofertada

Encargado de la configuración de características de capa 2, capa 3 y políticas de seguridad de la solución, migración de configuración existente, conexión a nivel de puertos y enlaces de red hacia infraestructura existente, realización de pruebas de conectividad y correcto funcionamiento para solución de Balanceo de Carga y Firewall de Aplicaciones Web (WAF), elaboración de informe de instalación.

Requisitos:

Título Técnico en computación, Sistemas o Computación e Informática o de Redes o Telecomunicaciones o Electrónica y/o Bachiller ingeniería de sistemas, electrónica o Telecomunicaciones, Grado de bachiller en Ingeniería Electrónica y/o Telecomunicaciones del personal clave requerido como Implementador de la Solución.

Acreditación:

El Título Técnico, será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <https://enlinea.sunedu.gob.pe/> o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: <http://www.titulosinstitutos.pe/>, según corresponda.

En caso el Título Técnico, no se encuentre inscrito en el referido registro, el postor ganador de la buena pro debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida para la suscripción del contrato.

17.2 CAPACITACIÓN

17.2.1 Jefe de Proyecto Requisitos:

Certificación en Gestión de proyectos PMP vigente emitido por PMI y/o Certificación oficial en buenas prácticas de Servicio Certificación ITIL Foundation **Acreditación:**
Se acreditará con copia simple de los certificados para la firma del contrato.

17.2.2 Dos (02) Especialistas Técnicos de la solución ofertada

Contar con certificación técnica a nivel profesional vigente en equipos de seguridad en la marca de la solución ofertada o Certificación técnica a nivel profesional en Seguridad de Red vigente en la marca propuesta y entrenamiento técnico oficiales en las soluciones propuestas.

Acreditación:

Se acreditará con copia simple del certificado para la firma del contrato.

18. CONFIDENCIALIDAD

Toda información del INEI a que tenga acceso el contratista, producto del desarrollo del bien contratado es estrictamente confidencial. El contratista y su personal, deben comprometerse a mantenerse las reservas del caso y no tramitarla a ninguna persona (natural o jurídica) sin la autorización expresa y por escrito por la Oficina Técnica de Informática – OTIN.

19. CLÁUSULA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

El CONTRATISTA deberá adherirse a la cláusula de seguridad de la información y protección de datos personales del bien contratado por lo que declara:

- ✓ Que adoptará las medidas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información a la que acceda, las cuales mantendrán congruencia con la Política de Seguridad de la Información del INEI.
- ✓ Ejecutará las prestaciones, en cumplimiento de la Ley 29733 – Ley de Protección de Datos Personales y su Reglamento.
- ✓ Acepta que los recursos que el INEI pone a su disposición, están disponibles exclusivamente para cumplir las obligaciones y propósitos operativos relacionados a la ejecución de la bien materia de la contratación; cuya información no podrán ser divulgada, revelada, entregada o puesta a disposición de terceros, total o parcialmente, dentro o fuera del centro laboral, salvo autorización expresa de INEI.

En ese sentido, será responsable de notificar al INEI ante cualquier evento o incidente asociado a la vulneración de la información confidencial, que pueda ser detectado en el marco de ejecución del bien contratado.

20. VICIOS OCULTOS

La recepción conforme, no enerva el derecho a reclamar posteriormente por defectos o vicios ocultos u otras situaciones anómalas no detectables o no verificables durante la recepción de los bienes, por causales no atribuibles al Contratista, debiendo proceder a la reposición o canje total de los bienes que se hayan detectado en las situaciones descritas. El plazo máximo de responsabilidad del Contratista será de cinco (05) años, a partir del día siguiente de la conformidad de la prestación principal.

21. NIVEL DE RIESGO

En mérito del numeral 6.1.27 de la Resolución Ministerial N° 1275-2021-MINSA, la ejecución de las prestaciones a cargo del Contratista en mérito del bien contratado configura:

- ☒ (x) Riesgo bajo de exposición o de precaución
- ☐ () Riesgo Mediano de Exposición
- ☐ () Riesgo Alto de Exposición
- ☐ () Riesgo Muy Alto de Exposición

22. PROTOCOLO SANITARIO

El contratista deberá cumplir con los Protocolos Sanitarios establecidos por el Ministerio de Salud en prevención del COVID-19 que sean necesarios para el ingreso a la institución durante la entrega de los bienes.

Medidas de prevención:

1. El ingreso del contratista a las oficinas del Instituto Nacional de Estadística se realizará con los equipos de protección personal esenciales, tales como mascarillas, protector facial y guantes.
2. El contratista respetará todas las medidas que el personal de seguridad o encargado de control de ingreso le impartan como medidas de prevención de seguridad y salubridad.

3. En caso se detecte que el contratista presenta algún síntoma de enfermedad (fiebre, tos seca, dificultad para respirar, entre otros), éste procederá a su retiro de la Entidad, con el fin de evitar cualquier tipo de riesgo de contagio.
4. Durante la permanencia dentro de la Entidad, el Contratista mantendrá en todo momento el distanciamiento mínimo de (1) metro con relación a cualquier persona.
5. Para el ingreso del Contratista con equipos, máquinas o herramientas, éste estará supeditado a su revisión y desinfección, esto estará a cargo del propio Contratista, antes de su ingreso y en presencia del personal de seguridad o encargado del control de ingreso a la Entidad.

23. 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 pueda constituir un incumplimiento de 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, los artículos 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 tuviera conocimiento; así también en adoptar medidas técnicas, prácticas, a través de los canales dispuestos por la entidad.

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 la entidad pueda accionar.

24. REQUISITOS DE CALIFICACIÓN

A. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

El postor debe acreditar un monto facturado acumulado equivalente a S/ 2'000,000 soles (dos millones y 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.

Se consideran bienes similares a los siguientes:

Venta y/o implementación y/o soporte de equipos Firewall, Firewall de Próxima Generación, Firewall Perimetral, Firewall UTM, Firewall de Aplicaciones Web (WAF), Balanceadores de Carga (ADC) y equipamiento de seguridad firewall.

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 voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 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 otra persona jurídica 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 N° 8 referido a la Experiencia del Postor en la Especialidad.

B. EXPERIENCIA DEL PERSONAL CLAVE

B.1 Un (01) Jefe de Proyecto

Requisitos:

Experiencia mínima de dos (02) años en gestión de proyectos, en labores de supervisión o dirección de proyectos de implementación en soluciones de data center o soluciones de servidores, balanceadores de carga, firewall de aplicaciones web o similares.

Acreditación:

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

B.2 Dos (02) Especialistas Técnicos de la solución ofertada

Requisitos:

Con una experiencia mínima de dos (02) años en implementación y/o seguimiento de proyectos similares al objetivo de la contratación. Serán considerados como proyectos similares, todas las implementaciones de proyectos en instalación, configuración y administración en solución de Balanceadores de Carga y Firewall de Aplicaciones Web (WAF), servicio de redes y/o seguridad.

Acreditación:

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

ANEXO 1

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

El postor deberá presentar en su propuesta la declaración jurada donde da cumplimiento a todo lo requerido en las especificaciones técnicas.

ADQUISICIÓN DE BALANCEADOR DE CARGA						
ÍTEM	SERVICIO	CUMPLE		FOLIO	FUENTE	OBSERVACIONES
		Si	No			
5.1.1	Características de la Solución					
5.1.1.1	Throughput mínimo de Capa 4 de 8 Gbps.					
5.1.1.2	Throughput mínimo de Capa 7 de 4 Gbps.					
5.1.1.3	Debe tener al menos 120 GB de disco					
5.1.1.4	Tener al menos 02 interfaces gigabit ethernet RJ-45 habilitados					
5.1.1.5	Tener al menos 4 interfaces SFP 1 Gb, incluir 2 transceivers multimodo más patch cord de fibra ó 2 cables DAC/AOC de 5m por equipo.					
5.1.1.6	Tener al menos 2 interfaces SFP+ 10 GE, incluir 2 transceivers multimodo más patch cord de fibra ó 2 cables DAC/AOC de 5m por equipo.					
5.1.1.7	Debe contar con doble fuente de poder redundante activas					
5.1.2	Requisitos Mínimos de Funcionalidad					
5.1.2.1	Los dispositivos deben ser un equipo de propósito específico de balanceador.					
5.1.2.2	Hardware de tipo appliance diseñado exclusivamente para la función específica de balanceador.					

5.1.2.3	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-ofsale o end-ofsupport (Fin de Vida o Fin de Ventas o Fin de Soporte) y no deberán tener reemplazo tecnológico anunciado. Se deberá adjuntar la ficha técnica (datasheet). El postor deberá presentar una declaración jurada de que los equipos ofertados, no tienen más de un año de fabricación en el mercado internacional hasta la fecha que se otorgue la buena pro en su propuesta.					
5.1.2.4	Los equipos deben ser nuevos y de primer uso, evidenciándose con la carta del fabricante.					
5.1.2.5	Debe soportar configuración en alta disponibilidad (HA), trabajando en un esquema de alta redundancia, para no permitir la pérdida de conexiones (2 equipos).					
5.1.2.6	Debe soportar la creación de cuentas de administrador con diferentes perfiles y derechos de acceso basado en roles (RBAC);					
5.1.2.7	El perfil de los administradores debe definirse sobre la base de los derechos a las diferentes funcionalidades de balanceo de carga.					
5.1.2.8	Los derechos de acceso deben ser: Lectura, Escritura (y Lectura) y Sin acceso.					
5.1.2.9	La solución debe soportar como mínimo un entorno de administración en los idiomas inglés o español.					
5.1.3	Funcionalidades de Balanceo de Servidores					
5.1.3.1	Debe soportar balanceo de Capa 7 para los siguientes protocolos HTTP, HTTPS.					

5.1.3.2	Debe balancear el tráfico entre los servidores reales utilizando algoritmos propios y utilizando información de salud de los servidores.					
5.1.3.3	Debe permitir la configuración de los perfiles que determinan el cifrado del tráfico entre el equipo (ADC) y los servidores reales.					
5.1.3.4	Cuando existe comunicación cifrada, esta debe ser controlada por los protocolos SSL / TLS y la lista protocolos de cifrado.					
5.1.3.5	Debe ser compatible con el protocolo TLS (v1.0, v1.1, v1.2).					
5.1.3.6	Debe soportar por lo menos una suite de ciframiento.					
5.1.3.7	Opcionalmente, debe ser capaz de reutilizar las sesiones SSL					
5.1.3.8	Para cada uno de los servidores que participan en el algoritmo de balanceo de carga, debería ser posible configurar al menos dos de los siguientes: "Round Robin, Weighted Round, Robin, IP Hash, Least Connection".					
5.1.3.9	El equipo proporcionado debe ser capaz de balancear las nuevas sesiones, pero preservando las sesiones existentes en el mismo servidor, usando persistencia de sesión.					
5.1.3.10	Debe poderse configurar timeouts de conexión sobre las persistencias					
5.1.3.11	El sistema debe permitir la selección del servidor real basado en la información de cabecera de paquetes TCP / IP y HTTP.					
5.1.3.12	Debe permitir la selección del servidor real basado en el valor del campo de encabezado HTTP.					

5.1.3.13	El sistema debe permitir la reescritura de mensajes de HTTP request, HTTP response.					
5.1.3.14	El sistema debe permitir la compresión de datos incluyendo: aplicaciones CSS, HTML, JavaScript.					
5.1.3.15	El sistema debe permitir páginas de error enviadas a los clientes en caso de fallo en los servidores. Opcionalmente, estas páginas de error deben tener la opción para ser editadas.					
5.1.3.16	Debe poderse implementar NAT, NAT64 y NAT46 (los dos últimos para permitir NAT en IPv4 e IPv6 entre clientes y servidores);					
5.1.3.17	Debe soportar alta disponibilidad.					
5.1.4	Funcionalidades de Red					
5.1.4.1	Debe ser compatible con PPPoE					
5.1.4.2	Debe soportar VLAN					
5.1.4.3	Debe permitir el enrutamiento entre VLAN diferentes					
5.1.4.4	Debe soportar la configuración de rutas estáticas					
5.1.4.5	Debe ser posible configurar políticas de enrutamiento basado en direcciones IP de origen y / o destino					
5.1.4.6	Debe ser compatible con OSPF v2 - RFC 2328					
5.1.4.7	Debe poderse implementar NAT (Network Address Translation), de los siguientes tipos: Source NAT (cambiar la dirección IP de origen), mapeo 1-1 y traslado de puertos (TCP o UDP)					

5.1.4.8	Debe asignar políticas de ancho de banda, teniendo en cuenta la dirección de origen, destino y el servicio (puertos TCP y UDP)					
5.1.5	Funcionalidades de Global Server Load Balancing					
5.1.5.1	Debe ofrecer servicio DNS o SmartDNS					
5.1.5.2	Debe ofrecer servicios como un DNS Autoritativo					
5.1.5.3	Debe soportar DNS64 para permitir la comunicación entre clientes IPv4 con servidores IPv6 en el contexto de balanceo de carga global					
5.1.5.4	Debe permitir (opcional) establecer los sitios basados en la ubicación geográfica de configuración (países). La base de datos que asocia direcciones IP a los países debe ser desarrollado y gestionado por el fabricante					
5.1.5.5	Debe soportar la creación de políticas de DNS. Se entiende por políticas de DNS la forma en que el balanceador interpreta y responde a una petición DNS					
5.1.5.6	Para cada uno de los posibles sitios remotos debe ser posible asignar peso a estos, para que este parámetro se tenga en cuenta en la secuencia de distribución de la respuesta de DNS.					
5.1.5.7	Debe permitir el cambiar los puertos HTTP, HTTPS, Telnet y SSH para fines de acceso remoto del equipo por el administrador					
5.1.5.8	Debe ser compatible con la sincronización de hora a través de NTP					
5.1.5.9	Debe permitir la actualización programada de firmas y de Base de Datos a través de la línea de comandos o de la interfaz gráfica					

5.1.5.10	Debe permitir proceso de upgrade de firmware					
5.1.5.11	Debe ser compatible con la configuración de un servidor de correo para el envío de alertas o logs por correo electrónico (SMTP)					
5.1.5.12	Debe contar con servicio de agente SNMP v1, V2c y 3					
5.1.6	Funcionalidades de Reportes y Logs					
5.1.6.1	El sistema debe tener un panel, a través de la interfaz gráfica que permite al administrador ver la información sobre el sistema, incluyendo al menos: el estado del sistema (uso de CPU, uso de memoria, número de conexiones actuales, ancho de banda utilizado, últimos registros) y el balanceo de carga.					
5.1.6.2	Debe mostrar los registros de eventos y el tráfico de datos o log de red, incluidas las actividades de los administradores del sistema o log de configuraciones					
5.1.6.3	Permitir configurar un servidor syslog el cual será proporcionado por el INEI					
5.1.6.4	Debe permitir los siguientes estados de log: Emergencia, Alerta, crítico, error, advertencia, notificación, información y Debug.					
5.1.6.5	Debe permitir seleccionar el tipo de registro para ser enviados al servidor syslog					
5.1.6.6	La solución debe ser compatible con el envío de alertas o logs a través de mensajes de correo electrónico					

ADQUISICIÓN DE WAF (FIREWALL DE APLICACIONES WEB)						
ÍTEM	SERVICIO	CUMPLE		FOLIO	FUENTE	OBSERVACIONES
		Si	No			
5.2.1	Características de la solución:					
5.2.1.1	Throughput mínimo para HTTP de 1.2 Gbps					
5.2.1.2	Mínimo de 4 interfaces de 1Gbps RJ-45 habilitados					
5.2.1.3	Mínimo de 4 interfaces de 1Gbps SFP, incluir 2 transceivers multimodo más patch cord de fibra ó 2 cables DAC/AOC de 8m por equipo.					
5.2.1.4	Tener al menos 2 interfaces SFP+ 10 GE, incluir 2 transceivers multimodo más patch cord de fibra ó 2 cables DAC/AOC de 8m por equipo.					
5.2.1.5	Almacenamiento de 450 GB SSD					
5.2.1.6	Debe contar con doble fuente de poder redundante activas.					
5.2.1.7	Los dispositivos deben ser un equipo de propósito específico.					
5.2.1.8	Hardware de tipo appliance diseñado exclusivamente para la función específica de protección de aplicaciones web (WAF).					
5.2.1.9	Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.					

5.2.1.10	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-ofsupport (Fin de Vida o Fin de Ventas o Fin de Soporte) y no deberán tener reemplazo tecnológico anunciado. Se deberá adjuntar la ficha técnica (datasheet).					
5.2.1.11	Los equipos deben ser nuevos y de primer uso, evidenciándose con la carta del fabricante.					
5.2.1.12	Debe soportar configuración en alta disponibilidad (HA), trabajando en un esquema de alta redundancia, con todas las licencias de software habilitadas para no permitir la pérdida de conexiones (2 equipos).					
5.2.2	Funcionalidades de Red:					
5.2.2.1	La solución debe de ser capaz de ser implementada en modo Proxy (Transparente y Reverso).					
5.2.2.2	Sistema operacional / firmware debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadores disponibles gratuitamente y protocolo HTTPS, y también por CLI (interface de línea de comando), accediendo localmente por puerto de consola, o remotamente vía SSH					
5.2.2.3	Debe de proveer, en la interfaz de gestión, las siguientes informaciones del sistema para cada equipo: consumo de CPU y estadísticas de conexión					

5.2.2.4	Debe de ser posible visualizar en la interfaz de gestión la información de consumo de memoria y los discos de log					
5.2.2.5	Debe de incluir herramienta dentro de la interfaz gráfica de gestión (dashboard) que permita visualizar los últimos logs de ataques detectados/bloqueados					
5.2.2.6	Debe proveer las siguientes informaciones en la interfaz gráfica de gestión: estadísticas de throughput HTTP en tiempo real, estadísticas de eventos de ataques etectados/bloqueados, y los últimos logs de eventos del sistema o de configuración					
5.2.2.7	Debe soportar los protocolos de monitoreo SNMP v1, SNMP v2c e SNMP v3					
5.2.2.8	Debe ser capaz de realizar notificación de eventos de seguridad a través de e-mail, traps SNMP y Syslog					
5.2.2.9	La solución deberá de soportar almacenar logs localmente en disco y en servidor externo vía protocolo SYSLOG					
5.2.2.10	La solución debe tener la capacidad de enviar alertas o logs por email					
5.2.2.11	La solución debe tener datos conteniendo la localización geográfica de los clientes web.					
5.2.2.12	Debe tener la capacidad de generar reportes					
5.2.3	Funcionalidades de Web Application Firewall					

5.2.3.1	Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de virus y reputación IP, actualizado de forma automática.					
5.2.3.2	La solución debe permitir utilizar la base de datos completa de protección del fabricante contra virus.					
5.2.3.3	Tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs.					
5.2.3.4	Tener la capacidad de protección contra ataques del tipo SQL Injection, Botnet, acceso por fuerza bruta, Data leakage, Cross Site Request Forgery (CSRF), cross site scripting (XSS), Remote File Inclusion (RFI), DoS Protection, cambios de cookie o cookie tampering, Directory Traversal.					
5.2.3.5	Debe tener protección contra ataques de Denial of Service (DoS);					
5.2.3.6	Tener la capacidad de protección contra ataques del tipo SYN flood					
5.2.3.7	Contar con algún mecanismo de protección contra ataques de días cero.					
5.2.3.8	Tener la capacidad de configurar protección del tipo TCP SYN flood-style para prevención de DoS.					

5.2.3.9	Debe soportar crear políticas de geolocalización, permitiendo que el tráfico de determinado país sea bloqueado					
5.2.3.10	Permitir configurar listas negras de bloqueo y listas blancas de confianza, basadas en dirección IP de origen					
5.2.3.11	Tener la funcionalidad de proteger el website contra acciones de defacement, con recuperación automática y rápida del website en caso de fallo					
5.2.3.12	Debe ser capaz de hacer aceleración de SSL					
5.2.3.13	La solución debe tener la capacidad de almacenar certificados digitales o cadenas de confianza					
5.2.3.14	La solución debe de tener un sistema de reputación de direcciones IP públicas conocidas como origen de ataques de DDoS y botnets.					
5.2.3.15	La solución debe permitir crear reglas definiendo el orden con que las páginas deben de ser accedidas para prevenir ataques como cross-site request forgery (CSRF).					
5.2.3.16	La solución debe de tener la capacidad de definir restricción a determinados métodos HTTP					
5.2.3.17	Debe de ser capaz de hacer compresión, para reducir la cantidad de información enviada al cliente					

5.2.3.18	Permitir redirección de requisiciones HTTP para HTTPS					
5.2.3.19	Permitir añadir el campo X-Forwarded-For para identificación de la dirección IP real del cliente.					
5.2.3.20	La solución debe de soportar reglas para definir si las requisiciones HTTP serán aceptadas en función de la URL o URI y origen de la petición.					
5.2.3.21	La solución debe de soportar políticas de control de acceso.					
5.2.3.22	Tener capacidad de web cache.					
5.2.3.23	La solución deberá actualizar la base de datos de firmas					
5.2.3.24	La solución debe incluir la funcionalidad de balanceo de carga entre servidores web					
5.2.3.25	Soportar algoritmos para balanceo de carga entre servidores tales como Round Robin, Weighted Round Robin, Least Connection o Weighted Least Connection.					
5.2.3.26	Permitir prueba de disponibilidad del servidor web.					
5.2.3.27	La solución o alguno de sus métodos de balanceo debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor.					

Nota: En caso de indicarse que **NO CUMPLE** con alguna ESPECIFICACIÓN TÉCNICA, deberá indicarse en la columna **OBSERVACIONES**.

Firma y Sello del Representante Legal Sello del
postor/ Razón Social de la empresa