ADQUISICIÓN DE SISTEMA DE PROTECCION Y SEGURIDAD PARA RED – FIREWALL – EG 2026

1. ÁREA SOLICITANTE

Gerencia de Informática y Tecnología Electoral (GITE).

2. ANTECEDENTES

Resolución Jefatural N° 000051-2025-JN/ONPE (07ABR2025), se aprobó el "Plan Operativo Electoral – Elección del Presidente de la República, Vicepresidentes, Senadores y Diputados del Congreso de la República y Representantes Peruanos ante el Parlamento Andino 2026, Versión 00".

Resolución Jefatural N° 000143-2025-JN/ONPE (09/09/2025) que aprueba la modificación de la Resolución Jefatural N° 000131-2025-JN/ONPE, con la finalidad de incorporar precisiones procedimentales relativas a la invitación de proveedores, las condiciones aplicables a contrataciones con proveedores, los requisitos de documentación obligatoria y las garantías exigibles; así como adecuar la normativa interna a lo dispuesto en la Ley N° 32416 y en la Ley N° 32069, en lo que corresponda. Se precisa que los demás extremos de la Resolución Jefatural N° 000131-2025-JN/ONPE y sus anexos, que no han sido objeto de modificación mediante la presente resolución, conservan plena vigencia.

La ADQUISICIÓN DE SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED – FIREWALL permitirá cumplir con la Actividad AOI00047901054: GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA Y BASE DE DATOS

3. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

El presente requerimiento consiste en la ADQUISICIÓN DE SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED – FIREWALL – EG 2026, que permitirá fortalecer la infraestructura tecnológica de la Entidad, con el objetivo de atender de manera eficiente la seguridad en las bases de datos, protegiéndola de accesos no autorizados, modificaciones no controladas y robo de información. Para ello, se busca dotar a la Entidad de un sistema de seguridad que proteja las bases de datos críticas y gestionar la información generada por el sistema para proteger oportunamente los activos de actividades no autorizadas.

4. FINALIDAD PÚBLICA

El presente requerimiento busca contar con tecnología que permita agregar una capa de protección adicional a las Bases de Datos de las aplicaciones certificadas en la entidad, que permita disponer de recursos de capacidad de cómputo para procesar la información generada por actividades administrativas y que se brinda a la ciudadanía mediante servicios informáticos.

5. OBJETIVOS DE LA CONTRATACIÓN

- Aumentar significativamente la seguridad en las bases de datos de las aplicaciones informáticas de la entidad, respondiendo a las crecientes demandas operativas y de datos de la Entidad.

6. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios (R.O).

7. CARACTERÍSTICAS TÉCNICAS

ÍTEM	CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN DEL BIEN
1	1	UNIDAD	**SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED – FIREWALL**

Las características técnicas mínimas del sistema de protección y seguridad para red – Firewall se presentan a continuación:

Tabla N° 1

CARACTERÍSTICAS DEL SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED – FIREWALL	
CARACTERÍSTICAS	**DETALLE**
Compatibilidad de BD	Por lo menos con: • Oracle • Oracle Exadata • MySQL • PostgreSQL • Maria DB
Fuente de poder – equipo de seguridad	Redundancia en fuente de poder del tipo hot-swap
Funcionamiento Modo de trabajo	Debe funcionar en las instalaciones locales (centro de datos).
Factor de forma – equipo de seguridad	1 o 2 RU
Navegadores requeridos para la gestión	Firefox v13 y posteriores Chrome v130 y posteriores Microsoft v130 y posteriores
Cantidad de instancias de bases de datos cubiertas por la licencia	La licencia debe ser habilitada al menos para 20 agentes los que deben ser instalados por el contratista en al menos 6 servidores de la entidad que pueden tener distintos sistemas operativos con motores de bases de datos en MySQL, Postgree y Oracle.
Componentes del sistema	El sistema debe componerse de: - Software de gestión o consola de administración o consola centralizada. - Equipo de seguridad y de auditoria (hardware especializado) se deben incluir todas las licencias para subsistemas dependientes como Base de datos u otros componentes necesarios para el funcionamiento del sistema) - Agentes Todas las licencias necesarias para hacer funcionar el sistema deben incluirse de manera integral de parte del contratista e instalarse en la infraestructura existente de la ONPE y en sus gabinetes dentro del centro de datos en la sede central en Lima. **Nota**: Es importante señalar que el software de gestión o consola de administración, es y forma parte del sistema de protección y seguridad para red Firewall.
Compatibilidad del Sistema operativo con los Agentes	Los agentes deben ser compatibles con: Linux (RHEL, CentOS, Ubuntu) o Windows Server 2019/2022 estos sistemas operativos contienen los motores de bases de datos. En los Sistemas operativos se instalarán los agentes que son parte del sistema.
Funciones y capacidades requeridas al sistema de protección y seguridad	- El sistema ofertado y sus componentes deben ser de la misma marca incluyendo sus consolas de administración y equipo de seguridad y auditoría de base de datos. - El sistema deberá soportar mínimo 6.000 transacciones por segundo (TPS) en un modelo de seguridad y monitoreo de bases de datos con agentes. Los agentes deben ser del mismo fabricante que la consola de administración y el equipo de seguridad y de auditoría de base de datos. - El equipo de seguridad y de auditoría de base de datos debe ser nuevo y de propósito especializado. - El licenciamiento de la plataforma debe considerar como mínimo 20 agentes de seguridad y auditoría de bases de datos.

CARACTERÍSTICAS DEL SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED – FIREWALL	
CARACTERÍSTICAS	**DETALLE**

	- Los diferentes componentes deberán de administrarse a través de una consola centralizada.
	- La consola centralizada deberá de ser el único punto de contacto, administración, control, análisis y reporteo para las diferentes soluciones e infraestructura de seguridad en bases de datos.
	- El sistema deberá realizar monitoreo, auditoria y protección de bases de datos basados en agentes a instalar en los servidores de bases de datos.
	- El sistema deberá funcionar independiente a la activación de la auditoría nativa de la base de datos.
	- El sistema deberá ser transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
	- El sistema deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
	- El sistema deberá monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, links, stored procedures.
	- El sistema deberá hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.
	- El sistema deberá proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
	- El sistema deberá proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.
	- El sistema deberá manejar reglas y políticas tan amplias o granulares como se requieran y deberán poder ser construidas automática o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.
	- El sistema deberá soportar y aplicar simultáneamente un modelo de seguridad positivo y negativo.
	- El sistema deberá ser capaz de monitorear al menos las siguientes plataformas de bases de datos:
	  - Oracle
	  - MySQL
	  - PostgreSQL
	  - Maria DB
	- El sistema debe tener la capacidad de descubrir bases de datos en la red de la entidad basado en puertos, servicios y presentarlos dentro de un inventario.
	- El sistema debe tener el modo monitoreo en donde el administrador podrá visualizar alertas, ataques, errores de servidor y otra actividad no autorizada.
	- El sistema debe presentar dentro del inventario de bases de datos, los servidores, sistemas operativos, motores de bases de datos, versiones y direccionamiento IP.
	- El sistema deberá ser capaz de realizar un análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación y configuración de seguridad, sin

CARACTERÍSTICAS DEL SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED – FIREWALL	
CARACTERÍSTICAS	**DETALLE**
	importar el sistema operativo sobre el que se encuentren instaladas. - El sistema deberá contar con un módulo de gestión de riesgo que presente todas las vulnerabilidades descubiertas y permita su gestión incluyendo la aceptación, identificación de falsos positivos o eliminación de la vulnerabilidad. - Los escaneos de vulnerabilidades deberán ser personalizables y configurables por el administrador. - El sistema deberá contar con un módulo de monitoreo donde sea posible ver todas las violaciones y alertas generadas por las reglas con el detalle de la acción ejecutada, su periodicidad y usuario que lo ejecutó. - El sistema deberá generar reportes y tendencias en tiempo real, así como permitir la modificación de estas. - El sistema deberá contar con facilidades o herramientas analíticas para la conducción de análisis forense cuando sea reportado algún incidente. - El sistema deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema, información de seguridad/administración, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog. - Debe proporcionar un proceso de instalación, actualización y gestión de cambios centralizada, segura y ágil para los agentes; la cual debe proporcionar una visión completa de todas las actualizaciones disponibles para los componentes del sistema de protección de bases de datos. - El sistema deberá notificar cuando se encuentre disponible una nueva versión del agente de monitoreo. - El despliegue y la instalación centralizada de parches y actualizaciones a componentes solo deberá ser realizada por usuarios con los privilegios necesarios y administradores de la herramienta. - El sistema debe manejar una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas. - El sistema debe tener facilidades de archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP)
Garantía de software	El tiempo de soporte, actualizaciones y licenciamiento del sistema ofertado será de mínimo doce (12) meses. Debe ser brindado por el fabricante.

Tabla N°2

CONFIGURACION DEL SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED – FIREWALL	
Configuración	**DETALLE**
Instalación y configuración	El contratista debe instalar el equipo de seguridad y auditoria de base de datos en el centro de datos y gabinete de la ONPE, la consola de administración debe quedar instalada y configurada como máquina virtual en la infraestructura virtual de la ONPE. El contratista debe instalar el todo el sistema y debe incluir todo el software y soluciones de los que dependa para funcionar. El sistema debe quedar configurado y operando con sus agentes bajo

CONFIGURACION DEL SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED – FIREWALL	
Configuración	**DETALLE**
	las funciones y capacidades anteriormente descritas. Se deben realizar pruebas de monitoreo de las bases de datos en al menos 6 servidores bases de datos como mínimo, las cuales serán MySQL, ORACLE, PostgreeSQL. El contratista debe configurar las licencias y/o suscripciones necesarias para el funcionamiento del sistema y deben quedar registradas en el correo indicado en las CONDICIONES GENERALES. Toda la instalación del sistema debe ser integrada correctamente con las bases de datos. Todas las credenciales utilizadas con sus respectivas contraseñas deberán ser también entregadas en un documento físico al momento de la entrega del bien, además en duplicado digital en el correo detallado en las CONDICIONES GENERALES.

7.1 ADMINISTRACIÓN Y GESTIÓN

El contratista debe proveer el licenciamiento necesario para el funcionamiento del sistema con todos sus componentes, software dependiente y subsistemas. La consola de administración se deberá instalar en una máquina virtual dentro de los Hipervisores ubicados en el centro de datos de la Entidad, en esta máquina virtual se deberá instalar todo el software necesario para administrar el equipo de seguridad y agentes que conforman el sistema (Sistema de protección y seguridad para red). La consola de administración deberá interactuar y gestionar todos los componentes del sistema para cumplir con brindar protección a las bases de datos, la consola de administración debe tener las siguientes características:

- Controlar, administrar y gestionar las reglas que gobiernan a los agentes.
- Descubrir todas las instancias de bases de datos en los servidores donde son instalados los agentes.
- Realizar un inventario para todas las bases de datos.
- Monitorear el conjunto de todos los agentes desde su consola.
- Actualizaciones de software
- Visualización gráfica y distribuida de comportamiento anómalo o riesgos en las instancias de bases de datos protegidas.
- Generación de reportes con información detallada de los hallazgos.

La consola de administración deberá soportar la administración remota gráfica y mostrar los eventos, anomalías, hallazgos recogidos de cada agente instalado en los servidores donde se encuentran las bases de datos independientemente del sistema operativo donde este instalado el agente. Debe tener la capacidad de actualización de los componentes del sistema. Debe tener la funcionalidad para la creación y modificación de reglas desde nuevas plantillas o reutilizando plantillas prexistentes.

Los agentes instalados en las bases de datos en cada servidor deben poder actualizarse bajo demanda y ser controlados por la consola de administración.

7.2 CONDICIONES GENERALES

a) Los bienes entregados por el contratista deben ser nuevos y deben estar en perfectas condiciones para su uso, en donde los rótulos permitan identificar las características y la marca respectiva y si fuera el caso deberá estar impreso en el mismo bien.
b) No se aceptará bienes reciclados, reensamblados o reacondicionados, tampoco se aceptará aquel que tenga la denominación “refurbished”, “remarketing” o su equivalente comercial.
c) En caso se requiera licencias para el funcionamiento del bien ofertado, el contratista deberá registrar las licencias de software y/o suscripciones a nombre de la ONPE al correo electrónico: “Licenciasonpe@onpe.gob.pe”.
d) El contratista deberá brindar una instrucción del uso y despliegue del sistema de protección y los componentes que son solicitados en el presente documento. La

instrucción será por un mínimo de dieciséis (16) horas para cuatro (04) personas y debe iniciar dentro de los diez (10) días calendario siguientes de notificada la orden de compra o suscrito el contrato, lo que ocurra primero y deberá concluirlo dentro del plazo de ejecución de la prestación. La instrucción se realizará en forma remota (síncrona) de acuerdo a lo requerido por la ONPE. Asimismo, deberá entregar el "Acta de instrucción" con la firma del representante de la ONPE y representante del Contratista (Especialista), debiendo detallar el nombre de los participantes y los temas tratados.

8. DOCUMENTOS PARA LA SUSCRIPCIÓN DE CONTRATO

El contratista deberá presentar para el perfeccionamiento del contrato copia simple de los siguientes documentos:

8.1. Documento o referencia de web oficial del fabricante que indique que los bienes están vigentes en el mercado y se posicionan dentro de la familia de equipos de última generación en tecnología publicadas por el fabricante, asimismo, no deberán estar descontinuados (end-of-life), no deberán estar en el fin de soporte (end of support) y no deben estar en el fin de venta (end of sale). En caso el idioma original del documento, no sea el español, deberá ser traducido.

8.2. Carta en la que indique los datos siguientes de al menos un Centro de Soporte Regional o Canal Autorizado en la ciudad de Lima, firmada por el contratista:
- Nombre de la compañía.
- Dirección.
- Números de teléfonos.

8.3. Carta emitida por el fabricante que acredite y autorice al postor ganador para la venta de los equipos ofertados.

9. MODALIDAD DE PAGO

El presente procedimiento se rige por la modalidad de pago de A SUMA ALZADA.

10. SISTEMA DE ENTREGA

El sistema de entrega será de Llave en mano, el contratista se encargará de la provisión de los bienes, su instalación y puesta en funcionamiento.

11. REQUISITOS QUE DEBERÁ CUMPLIR EL POSTOR

La prestación será efectuada por una persona natural o persona jurídica, la cual debe cumplir con lo siguiente:

11.1. Perfil del personal clave

a) Especialista: Personal encargado de la instalación y configuración (Tabla N°2).

11.2. El postor en su propuesta deberá adjuntar la hoja de datos y/o ficha técnica y/o brochure, emitida por el fabricante, en idioma español o idioma original del fabricante, que permita verificar el cumplimiento de las características técnicas solicitadas en la Tabla N° 1 del numeral 7.

Los requisitos del personal clave se indican en el numeral denominado: "REQUISITOS DE CALIFICACIÓN".

12. OBLIGACIONES DEL CONTRATISTA

El contratista es el único responsable ante la ONPE de cumplir con la contratación, no pudiendo transferir esa responsabilidad a otras entidades ni terceros en general.

13. PLAZO DE EJECUCIÓN DE LA PRESTACIÓN

Se prestará por el periodo de treinta (30) días calendario (el cual incluye el plazo de entrega de los bienes y plazo de Instalación y puesta en funcionamiento), el mismo que se computa de acuerdo al siguiente detalle:

CONDICIONES Y PLAZO DE ENTREGA

	Descripción del Bien	Plazo de Entrega de los bienes	Plazo de la Instalación y Configuración
1	**SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED – FIREWALL**	Dentro de los veintiocho (28) días calendario siguientes de notificada la orden de compra o suscrito el contrato, lo que ocurra primero	Dentro de los dos (02) días calendario, contados a partir del día siguiente de la recepción del bien. (Descrito en la Tabla N°2).

La siguiente documentación deberá presentarse a la entrega del bien:

a. Guía de Remisión y entrega de un (01) equipo de seguridad y auditoría, montable para instalar en gabinete, con sus respectivos accesorios de instalación (manuales, cables de red, y cable de alimentación), sellado por el área de Almacén de la ONPE.
b. Documento (Informe o carta) del contratista indicando las fechas del inicio y fin de la garantía, contados a partir de la entrega de los bienes.
c. Carta del fabricante o impresión de página web, donde indique la marca, modelo y serie del equipo ofertado.
d. Carta del fabricante o impresión de página web, donde indique claramente la cuenta de acceso y dirección web del portal de soporte, descargas de información y actualizaciones de software.
e. Carta del contratista donde se detalle el enlace de las licencias y/o softwares que componen el sistema ofertado además del procedimiento de solicitud de garantía en caso de fallo en el equipo.
f. Documento del contratista donde se indique los medios de comunicación (mínimo el correo electrónico y número de teléfono, así como también el método para generar y reportar casos/ticket con el fabricante) para el registro de la atención de la garantía

14. ENTREGABLES

El contratista deberá cumplir con los siguientes entregables:

Dentro de los dos (02) días calendario siguientes de culminada la instalación y puesta en funcionamiento:

a) Informe detallado de la instalación en gabinete y configuración de los productos ofertados, que incluye lo siguiente:
   i. Se debe documentar el proceso de instalación, configuración y diagrama de la arquitectura que describa la forma en la que se realizó la instalación, del sistema ofertado.
   ii. Acta de puesta en operación del sistema, firmada por el Especialista y personal de la ONPE.

b) Acta de instrucción firmada por el representante de la ONPE y representante del contratista (Especialista).

El lugar de entrega de la documentación será en la oficina de trámite documentario de la Sede Central de la ONPE, situado en el Jr. Washington 1894, Cercado de Lima o mediante la mesa de partes virtual externa de la Institución a través de la página web de la ONPE (https://www.web.onpe.gob.pe/mpve), en el horario de lunes a viernes de 8:30 a 16:30 horas, con atención a la Subgerencia de Infraestructura y Seguridad Tecnológica de la Gerencia de Informática y Tecnología Electoral.

15. LUGAR DE ENTREGA

El bien será entregado en el área de Almacén sito en Jr. Washington 1894 – Cercado de Lima, de lunes a viernes en el horario de 09:00 a 16:00 horas.
El bien entregado será instalado en gabinete de la sede Washington (Jr. Washington 1894 Lima).

16. GARANTÍA

El contratista deberá otorgar una garantía mínima de un (01) año, contados a partir de la recepción del bien físico por parte de la entidad. Durante dicho periodo, el contratista será responsable de efectuar la reparación, reposición o sustitución de los bienes, según corresponda, sin costo alguno para la entidad contratante.

17. REPOSICIÓN DE BIEN DEFECTUOSO

El cambio del bien por defectos de fábrica, debe ser un plazo de veinticinco (25) días calendario, contados a partir de la notificación remitida al contratista mediante correo electrónico por personal de la Gerencia de Informática y Tecnología Electoral (GITE).

Cabe indicar, que el contratista debe realizar el cambio de la totalidad de las piezas o partes que requieran ser reemplazadas para restaurar la operatividad del bien, asumiendo la totalidad del costo de dichas piezas o partes.

18. CONFORMIDAD

Será otorgada por la Gerencia de informática y Tecnología Electoral (GITE), previo informe elaborado por la Subgerencia de Infraestructura y Seguridad Tecnológica (SGIST), a través de la verificación del cumplimiento de las condiciones establecidas en las especificaciones técnicas en el plazo máximo de siete (7) días calendario de producida la recepción total efectuada. En caso de observaciones, se procederá de acuerdo con lo indicado en el artículo 144 del Reglamento de la Ley 32069, Ley General de Contrataciones Públicas.

19. FORMA DE PAGO

El pago se realizará en un único pago, previa conformidad emitida por la Gerencia de Informática y Tecnología Electoral (GITE), en moneda nacional y a la presentación del comprobante de pago por parte del contratista, de acuerdo con lo siguiente:

El pago se efectuará mediante el respectivo abono en la cuenta bancaria individual del postor ganador, dentro de los diez (10) días hábiles luego de otorgada la conformidad, sea a través del Banco de la Nación o de cualquier otra institución bancaria del Sistema Financiero Nacional, para cuyo efecto EL CONTRATISTA comunicará su CÓDIGO DE CUENTA INTERBANCARIO (CCI), y se debe de contar además con:

- Recepción del bien por parte del área de Almacén
- Conformidad por parte de la GITE.
- Comprobante de pago

Dicha documentación debe ser presentada en la oficina de trámite documentario de la Sede Central de la ONPE, situado en el Jr. Washington 1894, Cercado de Lima, en el horario de lunes a viernes de 8:30 a 16:30 horas.

20. RESPONSABILIDAD DEL PROVEEDOR

El proveedor es responsable por la calidad ofrecida y por los vicios ocultos de los bienes ofertados por un plazo de un (01) año contado a partir de la conformidad otorgada por la Entidad.

21. PENALIDADES APLICABLES

21.1 Penalidades por mora

En caso de retraso injustificado del proveedor en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, de conformidad con el artículo 120 del Reglamento de la Ley 32069 Ley General de Contrataciones Públicas.

22. ANTICORRUPCIÓN Y ANTISOBORNO

EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

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

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

23. INTEGRIDAD

En caso de falsedad de cualquiera de las declaraciones efectuadas por el contratista, la ONPE podrá declarar la nulidad del presente contrato por infracción del principio de presunción de veracidad, de conformidad a lo establecido en la Ley 32069 Ley General de Contrataciones Públicas.

24. CONFIDENCIALIDAD DE LA INFORMACIÓN

El CONTRATISTA deberá mantener estricta confidencialidad sobre la información a que tendrá acceso durante la ejecución de la prestación, no podrá disponer de la misma para fines distintos al desarrollo de la prestación. El proveedor y su personal deben comprometerse a mantener las reservas del caso y no transmitir los datos e información de ONPE a ninguna persona (natural o jurídica) que no sea debidamente autorizada por la ONPE.

25. REQUISITOS DE CALIFICACIÓN

25.1 REQUISITOS DE CALIFICACIÓN OBLIGATORIOS

A. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 250,000.00 (doscientos cincuenta mil con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los diez años anteriores a la fecha de la presentación de ofertas que se computaran 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/ 50,000.00 (Cincuenta mil con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los diez años anteriores a la fecha de la presentación de ofertas que se computaran 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:

i. Venta de Solución de Protección y Auditoría de Bases de Datos.
ii. Venta de Software de monitoreo integral de Base de Datos.

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 constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o la cancelación del mismo con comprobante de pago[1], o comprobante de retención electrónico emitido por SUNAT por la retención del IGV, correspondientes a un máximo de veinte contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados[2], para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

25.2 REQUISITOS DE CALIFICACIÓN FACULTATIVOS

A. CAPACIDAD TÉCNICA Y PROFESIONAL

A.1. EXPERIENCIA DEL PERSONAL CLAVE

Especialista:

Requisitos:
Dos (02) años como mínimo de experiencia laboral en la implementación y/o instalación y/o configuración y/o soporte de sistema de protección y seguridad tipo firewall y/o Sistemas de protección de bases de datos y/o Firewall de base de datos.

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.

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 años anteriores a la fecha de la presentación de ofertas.

[1] 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. Es válido el sello colocado por el cliente del postor (sea utilizando el término "cancelado" o "pagado").
[2] Entendiéndose por estas a aquellos que no son entidades contratantes.

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

Visado digitalmente por
JESUS ALBERTO FELIX ATUNCAR
Subgerente de Infraestructura y Seguridad Tecnológica
SUBGERENCIA DE INFRAESTRUCTURA Y SEGURIDAD TECNOLÓGICA

Visado digitalmente por
ROBERTO CARLOS MONTENEGRO VEGA
Gerente de Informática y Tecnología Electoral
GERENCIA DE INFORMÁTICA Y TECNOLOGÍA ELECTORAL

(V02)