

**REQUERIMIENTO DE BIENES - ESPECIFICACIONES TÉCNICAS****1. Datos Generales de la Contratación:**

1.1. Denominación de la Contratación	ADQUISICION DE SOFTWARE (INC. LICENCIA) PARA SISTEMA DE PROTECCION Y SEGURIDAD PARA RED - FIREWALL
1.2. Área Usuaría (Unidad Orgánica)	Oficina de Tecnologías de la Información
1.3. Meta Presupuestaria	0026
1.4. Actividad del POI	AOI00163000015 - EVALUACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)
1.5. Persona responsable del requerimiento su supervisión y seguimiento	Jefe de la Oficina de Tecnologías de la Información
1.6. Persona(s) a las que se le(s) hará la entrega del (los) Bien(es)	Jefe de la Oficina de Tecnologías de la Información
1.7. Persona que otorgará la Conformidad	Jefe de la Oficina de Tecnologías de la Información

2. Finalidad Pública

Proteger la red del INAIGEM, optimizar los procesos y servicios que son responsabilidad de la Oficina de tecnologías de la información, promoviendo una atención eficiente y eficaz, garantizando que la red institucional cuente con equipos de seguridad informática que detecten, bloqueen y eliminen códigos maliciosos para el correcto intercambio de información y compatibilidad con los equipos, por lo que se hace de finalidad pública contar con la activación de licencias, mantenimiento y soporte de los equipos firewall, así como considerar su disponibilidad en caso de un desperfecto.

3. Antecedentes:

Al contar con Infraestructura Pre Existente, se tiene la necesidad de realizar la renovación de Licencias que permitan continuar protegiendo la red institucional, a su vez es necesario contar con el mantenimiento de los mismos.

Cabe mencionar que las licencias tienen vigencia hasta el 10 de Octubre del 2024, se está solicitando con anticipación la certificación presupuestal del requerimiento

4. Objetivos Generales y/o específicos**4.1. Objetivo General:**

Contar con la adquisición de licencias, soporte y mantenimiento en los equipos de seguridad perimetral y de gestión de logs del INAIGEM.

4.2. Objetivo(s) Específico(s):

- Contar con un esquema de seguridad perimetral actualizado y con el mantenimiento y soporte para la sede principal y descentralizadas del INAIGEM.
- Proteger los equipos de ataques maliciosos
- Contar con el mínimo de disponibilidad de Equipos Firewall
- Contar con una solución que muestre información inmediata de los equipos de seguridad perimetral

5. Características y condiciones de los bienes a contratar**5.1 Descripción y cantidad de los bienes**

Descripción	Cantidad	Unidad de Medida
ADQUISICION DE SOFTWARE(INC. LICENCIA) PARA SISTEMA DE PROTECCION Y SEGURIDAD PARA RED - FIREWALL	04	Licencias



A- Características Generales

Detalle:

- 01 Licencia para el equipo de Seguridad de Cusco por 01 año.
- 01 Licencia para el equipo de Seguridad de Huaraz por 01 año.
- 01 Licencia para el equipo de Seguridad de Lima por 01 año.
- 01 Licencia para equipo de gestion de Logs de Huaraz por 01 año.
- Servicio de Soporte y Mantenimiento.

El INAIGEM cuenta con equipos de la marca FORTINET, tres (03) equipos de seguridad perimetral los cuales sirven para gestionar, administrar y controlar la seguridad perimetral y (01) equipo de gestión de logs, el cual sirve para el monitoreo y gestión de reportes de los equipos de seguridad perimetral

N° de Serial de FortiGate 30E	FGT30E5620023879
N° de Serial de FortiGate 100E	FG100ETK20003301
N° de Serial de FortiGate 60E	FGT60ETK18038940
N° de Serial de FortiAnalyzer 150G	FAZ15GT221000455

Tabla 1: Infraestructura Pre existente

Se ejecutará para los equipos descritos en la tabla 1 - INFRAESTRUCTURA PRE EXISTENTE, considerando la activación de las licencias que corresponden al módulo de IPS, Protección contra Malware Avanzado (Advanced Malware Protection), Web Filtering, Application Control, Security Rating, IoT Detection, Industrial Security, FortiConverter Svc solo para los 3 equipos Fortigate. Se debe incluir el soporte, y mantenimiento para la totalidad los equipos descritos en las Tabla 1, por el periodo de 1 año.

Se debe considerar la activación de las licencias de soporte para la totalidad los equipos descritos en las Tabla 1, por el periodo de 1 año.

Los equipos de seguridad perimetral FortiGate deberán estar licenciados para todas sus funcionalidades actualmente activas (Enterprise Proteccion + FortiCare)

El equipo de gestión de logs debe estar licenciado para la siguiente funcionalidad (FortiCare)

B- Servicio de Soporte del Proveedor

Se debe contar con el Servicio de Soporte del proveedor, el cual es el primer nivel de atención y deberá tenerse en cuenta lo siguiente:

- b.1 La cobertura de atención del soporte técnico del fabricante deberá ser del tipo 24x7 de lunes a domingo (24 horas, los 7 días de la semana y los 365 días del año) y del proveedor de 24x7 de lunes a domingo.
- b.2 El proveedor deberá brindar un número telefónico de contacto (teléfono fijo ó 0800), así como un correo electrónico de contacto, para la atención sobre cualquier avería, incidencia o requerimiento de la solución. Las llamadas de soporte serán realizadas por personal de la Oficina



de Tecnologías de la Información del INSTITUTO NACIONAL DE INVESTIGACION EN GLACIARES Y ECOSISTEMAS DE MONTAÑA (INAIGEM). Asimismo, el proveedor deberá indicar los canales de Atención del fabricante (**Correos, teléfonos**)- **Esta información debe ser parte del Informe de Mantenimiento Preventivo.**

- b.3 El proveedor debe contar con un sistema de mesa de ayuda en la modalidad de 24x7x365 por el tiempo de garantía de la solución que propone y describir las características del mismo.
- b.4 El proveedor deberá coordinar con el cliente la gestión del RMA ante el fabricante de la marca y deberá apoyar a la entidad con alguna solución que permita que se puedan mantener los servicios mientras se espera el reemplazo de los equipos de acuerdo con la tabla 1.

Se detalla a continuación las características de la atención requerida.

- La cantidad de atenciones de incidentes, requerimientos es ilimitada durante el periodo de ejecución del servicio.
- La atención de incidentes, requerimientos será solicitada a través de los medios de comunicación oficiales (canales de atención descritos en el punto b.2) y en cumplimiento de los SLA, descritos en la Tabla 2, definido por el INAIGEM.
- Levantamiento y acompañamiento para levantamiento de hallazgos de seguridad encontrados.
- Atención para nuevas configuraciones del software del equipamiento.
- Registro o actualización de la cuenta (soporte@inaigem.gob.pe) y acceso a la página web del fabricante para la gestión y monitoreo de los incidentes y acceso a la base de datos de conocimiento.
- Las atenciones a los incidentes/ requerimientos pueden ser presenciales o no presenciales.

Categoría	Tiempo Máximo de Atención	Tiempo Máximo de Solución
Incidencia Crítica	1h	2h
Incidencia Media	2h	4h
Incidencia Baja	4h	8h
Informativo	24h	48h
Solicitud de Reportes	8h	48h

Tabla 2 Categorías de atención y SLA

- Se debe considerar los siguientes parámetros para catalogar cada categoría de atención:

Categoría	Descripción
Incidencia Crítica	Indisponibilidad total de la plataforma o de los servicios
Incidencia Media	Afectación parcial de la plataforma o de los servicios
Incidencia Baja	Afectación mínima de la plataforma o de los servicios
Informativo	Consulta sobre funcionalidades del equipamiento o sobre las configuraciones
Solicitud de Reportes	Solicitud de un reporte



- En el caso de un requerimiento: el tiempo máximo de atención una vez solicitado será de 24 horas
- Se empieza a contabilizar el tiempo atención a partir del registro realizado por los medios indicados en ítem b.2

C- Mantenimiento Preventivo

El mantenimiento preventivo tiene como finalidad, prevenir la indisponibilidad del equipamiento del INAIGEM, por lo que se ha considerado un (01) mantenimiento preventivo para los equipos descritos en la Tabla 1, y debe de consistir en lo siguiente:

Para los equipos Fortigate

- c.1 Análisis y depuración de log del sistema.
- c.2 Revisión de parámetros de estado de salud.
- c.3 Validación y Optimización de Políticas Implementadas. (Las políticas deben estar activas)
- c.4 Validación y Revisión de funcionalidad de VPN, Seguridad.

Para el equipo FortiAnalyzer

- c.5 Revisión de parámetros de estado de salud.
- c.6 Revisión y análisis de plantillas actuales.(las plantillas deben ser optimizadas y de ser necesarias mejoradas)
- c.7 Validación y Optimización de almacenamiento actual de Log y reportes.

Para equipos Fortigate y FortiAnalyzer

- c.8 Informe del estado del equipo antes y después del mantenimiento preventivo.
- c.9 Recomendaciones en general

Dicha información debe estar descrita en el informe de mantenimiento preventivo y debe informarse las fechas de dicho mantenimiento, mediante correo a soporte@inaigem.gob.pe, la misma que será monitoreada.

Servicios de configuración

El proveedor deberá otorgar sin costo alguno para la INAIGEM los siguientes servicios:

- Servicio de configuración remota para configuración en la VPN Huaraz – Sedes Desconcentrada (a solitud)
- Actualización de los equipos a las nuevas versiones de firmware (sistema operativo), críticas (estabilidad y funcionamiento) y de seguridad del equipo. (Actualización del firmware, deben realizarse de ser el caso , los viernes a partir de las 19:00 hrs, previa coordinación con soporte)

5.2 Garantía comercial

Período de garantía: Los bienes deberán de tener una garantía mínima de 12 meses, a partir de la activación de las licencias.

El Servicio de Soporte del proveedor: tendrá una duración de 12 meses, a partir de la activación de las licencias

5.3 Capacitación

Se solicita que como parte del proyecto se incluya una capacitación basada en el temario oficial del curso dictada por un ingeniero certificado en la marca a ofertar por 08 horas en NSE6 (Forticlient) bajo las siguientes condiciones:



- La capacitación será de forma PRESENCIAL o VIRTUAL por parte de los especialistas propuestos por el proveedor.
- La capacitación tendrá un número máximo de 03 participantes, está dirigido al personal de la Oficina de Tecnologías de la Información.
- Al concluir la capacitación se debe entregar el voucher del examen de certificación para 03 participantes NSE6(Forticlient).

5.4 Documentos entregables (Físico / Digital).

- Certificado de licencias por suscripción.
- Carta de Garantía Comercial
- En digital Acta de Capacitación
- En digital Informe de mantenimiento Preventivo
- En digital activación de Licencias

5.5 Lugar y plazo de la ejecución de la presentación

5.5.1 Lugar

Los equipos se encuentran físicamente, en cada sede:

- Sede Principal ubicada en Av, Centenario 2656- Sector Palmira, Independencia Huaraz Ancash - Piso 2. Equipo 100E y equipo FortiAnalyzer 150G
- Sede Descentralizada Cusco: Av, Industrial Nro 1 Mz N Lt. 1 Urb Residencial Huancaro Santiago Cusco Equipo 30E
- Sede Descentralizada Lima: Av. Antonio Miroquesada 457 - Oficina 401 Edificio Corporativo ABC Lima - Magdalena del Mar – Perú -Equipo 60E
- Las licencia de software serán activadas via online.

5.5.2 Plazo

- Plazo de ejecución: Las licencias deben ser activadas el 10/10/2024
- Plazo de vigencia : 12 meses, contabilizados a partir del día de activación de la licencia
- Mantenimiento Preventivo: Hasta 20 días después de la activación
- Capacitación: Hasta 20 días después de la de la activación

6. Requisitos del proveedor, perfil del proveedor y/o su personal

6.1 Requisitos del Proveedor

- Ser partner autorizado de la tecnología a proponer, sustentar con carta de fabricante.
- Registro Único de Contribuyentes (RUC) habilitado.
- Código de Cuenta Interbancario registrado y vinculado a su N° de RUC.
- Registro Nacional de Proveedores (RNP) vigente, en el capitulo de Servicios.
- Debera presentar la autorizacion del fabricante a la firma del contrato u orden de compra.

6.2 Recursos y/o personal del Proveedor

- Para realizar la capacitacion, activacion de las licencias, mantenimiento y soporte debe contar como minimo con : Un (01) Ingeniero de Seguridad y Un (01) Técnico de Seguridad
Cualquier gasto adicional, no previsto para que se cumpla la orden de compra, sera cubierto por el proveedor.

6.2.1 Formación Académica

Requisitos:

**Un (01) Ingeniero de Seguridad**

Bachiller ó Titulado en ingeniería electrónica, ingeniería de las Telecomunicaciones o Ingeniería de Sistemas o afines.

Un (01) Técnico de Seguridad

Bachiller ó Titulado en Ingeniería de las telecomunicaciones o Ingeniería de Sistemas o Ingeniería Informática o Ingeniería Electrónica o afines.

Acreditación:

El grado de bachiller ó título, será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, 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 de que, el grado de Bachiller ó Título requerido no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

6.2.2 Experiencia del Personal**Requisitos:****Un (01) Ingeniero de Seguridad**

Experiencia no menor a cuatro (04) años liderando proyectos bajo el cargo de proyect mánager ó coordinador de proyectos en TI, redes ó afines.

Se acreditará con:

- Constancia ó Certificado en Gestión de Proyectos (45 horas)
- Constancia ó Certificado de experiencia laboral mínima de cinco (05) años en Gestión de Proyectos.
- Conocimientos en Soluciones de Seguridad
- Grado Bachiller ó Título según lo solicitado.

Un (01) Técnico de Seguridad

Experiencia laboral mínima de cuatro (04) años en proyectos referidos a ciberseguridad.

Se acreditará con:

- Certificado en Arquitecto de Soluciones de Seguridad de la Marca Ofertada (Vigente)
- Constancia ó Certificado de experiencia laboral mínima de cuatro (04) años en implementaciones referidos a ciberseguridad.
- Grado Bachiller ó Título según lo solicitado.

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.

Importante

- Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.



- En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.
- Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.
- Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.

7. Adelantos

El INAIGEM, no otorga adelantos o parte de pago por la adquisición de los bienes.

8. Conformidad

La conformidad la otorgará el Jefe de la Oficina de Tecnologías de la Información del INAIGEM, quien presentará un informe de conformidad, de acuerdo al cumplimiento de los entregables

9. Forma de pago.

El pago se realizará en una (01) armada según la ejecución y con la conformidad del Jefe de la Oficina de Tecnologías de la Información del INAIGEM.

10. Penalidad.

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

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

*Donde: F tiene los siguientes valores:

- Para plazos menores o iguales a sesenta (60) días, para bienes y servicios en general: F = 0.40.
- Para plazos mayores a sesenta (60) días, para bienes y servicios en general: F = 0.25.

11. Confidencialidad.

Al ser el INAIGEM, una entidad dedicada a la Investigación, el proveedor se obliga a guardar la confidencialidad y reserva absoluta en el manejo de información y documentación a la que se tenga acceso y que se encuentre relacionada con la prestación, quedando expresamente prohibido revelar dicha información a terceros.

12. Responsabilidad por vicios ocultos

El plazo máximo de responsabilidad del proveedor por la calidad ofrecida y por los vicios ocultos de los bienes entregados es de un (1) año contado a partir de la conformidad otorgada

13. Clausula única: Anticorrupción:

Con la elaboración y notificación de la Orden de Compra se formaliza el vínculo contractual, para lo cual se incluirá el siguiente texto:



“Con la notificación de la presente, El Proveedor, declara y garantiza no haber, directa o indirectamente, haber negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

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.

EL Proveedor, se Compromete a: (i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y (ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas. El incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, da el derecho al INAIGEM a resolver automáticamente y de pleno derecho el contrato, bastando para tal efecto que se remita una comunicación informando que se ha producido dicha resolución, sin perjuicio de las acciones civiles, penales y administrativas a que hubiera lugar”.