

BASES ESTÁNDAR DE LICITACIÓN PÚBLICA PARA LA CONTRATACIÓN DE BIENES

Aprobado mediante Directiva N° 001-2019-OSCE/CD



*SUB DIRECCIÓN DE NORMATIVIDAD – DIRECCIÓN TÉCNICO NORMATIVA
ORGANISMO SUPERVISOR DE LAS CONTRATACIONES DEL ESTADO - OSCE*

SIMBOLOGÍA UTILIZADA:

Nº	Símbolo	Descripción
1	[ABC] / [.....]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / [.....]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	Importante • Abc	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	Advertencia • Abc	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	Importante para la Entidad • Xyz	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

Las bases estándar deben ser elaboradas en formato WORD, y deben tener las siguientes características:

Nº	Características	Parámetros
1	Márgenes	Superior : 2.5 cm Inferior: 2.5 cm Izquierda: 2.5 cm Derecha: 2.5 cm
2	Fuente	Arial
3	Estilo de Fuente	Normal: Para el contenido en general Cursiva: Para el encabezado y pie de página Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
4	Color de Fuente	Automático: Para el contenido en general Azul : Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
5	Tamaño de Letra	16 : Para las dos primeras hojas de las Secciones General y Específica 11 : Para el nombre de los Capítulos. 10 : Para el cuerpo del documento en general 9 : Para el encabezado y pie de página Para el contenido de los cuadros, pudiendo variar, según la necesidad 8 : Para las Notas al pie
6	Alineación	Justificada: Para el contenido en general y notas al pie. Centrada : Para la primera página, los títulos de las Secciones y nombres de los Capítulos)
7	Interlineado	Sencillo
8	Espaciado	Anterior : 0 Posterior : 0
9	Subrayado	Para los nombres de las Secciones y para resaltar o hacer hincapié en algún concepto

INSTRUCCIONES DE USO:

- Una vez registrada la información solicitada dentro de los corchetes sombreados en gris, el texto deberá quedar en letra tamaño 10, con estilo normal, sin formato de negrita y sin sombrear.
- La nota **IMPORTANTE** no puede ser modificada ni eliminada en la Sección General. En el caso de la Sección Específica debe seguirse la instrucción que se indica en dicha nota.

Elaboradas en enero de 2019

Modificadas en junio 2019, diciembre 2019, julio 2020, julio y diciembre 2021, junio y octubre de 2022

**BASES ESTÁNDAR DE LICITACIÓN PÚBLICA PARA LA
CONTRATACIÓN DE BIENES**

BASES INTEGRADAS

LICITACIÓN PÚBLICA N° 003-2024-DINI

CONTRATACIÓN DE BIENES

**ADQUISICIÓN DE UN SISTEMA DE PROTECCIÓN Y
SEGURIDAD FIREWALL PERIMETRAL – RED EXTERNA**

DEBER DE COLABORACIÓN

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista, deben conducir su actuación conforme a los principios previstos en la Ley de Contrataciones del Estado.

En este contexto, se encuentran obligados a prestar su colaboración al OSCE y a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI, en todo momento según corresponda a sus competencias, a fin de comunicar presuntos casos de fraude, colusión y corrupción por parte de los funcionarios y servidores de la Entidad, así como los proveedores y demás actores que participan en el proceso de contratación.

De igual forma, deben poner en conocimiento del OSCE y a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI los indicios de conductas anticompetitivas que se presenten durante el proceso de contratación, en los términos del Decreto Legislativo N° 1034, "Ley de Represión de Conductas Anticompetitivas", o norma que la sustituya, así como las demás normas de la materia.

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista del proceso de contratación deben permitir al OSCE o a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI el acceso a la información referida a las contrataciones del Estado que sea requerida, prestar testimonio o absolución de posiciones que se requieran, entre otras formas de colaboración.

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

(ESTA SECCIÓN NO DEBE SER MODIFICADA EN NINGÚN EXTREMO, BAJO SANCIÓN DE NULIDAD)



CAPÍTULO I ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

Cuando en el presente documento se mencione la palabra Ley, se entiende que se está haciendo referencia a la Ley N° 30225, Ley de Contrataciones del Estado, y cuando se mencione la palabra Reglamento, se entiende que se está haciendo referencia al Reglamento de la Ley de Contrataciones del Estado aprobado por Decreto Supremo N° 344-2018-EF.

Las referidas normas incluyen sus respectivas modificaciones, de ser el caso.

1.2. CONVOCATORIA

Se realiza a través de su publicación en el SEACE de conformidad con lo señalado en el artículo 54 del Reglamento, en la fecha señalada en el calendario del procedimiento de selección, debiendo adjuntar las bases y resumen ejecutivo.

1.3. REGISTRO DE PARTICIPANTES

El registro de participantes se realiza conforme al artículo 55 del Reglamento. En el caso de un consorcio, basta que se registre uno (1) de sus integrantes.

Importante

- *Para registrarse como participante en un procedimiento de selección convocado por las Entidades del Estado Peruano, es necesario que los proveedores cuenten con inscripción vigente y estar habilitados ante el Registro Nacional de Proveedores (RNP) que administra el Organismo Supervisor de las Contrataciones del Estado (OSCE). Para obtener mayor información, se puede ingresar a la siguiente dirección electrónica: www.mp.gob.pe.*
- *Los proveedores que deseen registrar su participación deben ingresar al SEACE utilizando su Certificado SEACE (usuario y contraseña). Asimismo, deben observar las instrucciones señaladas en el documento de orientación "Guía para el registro de participantes electrónico" publicado en <https://www2.seace.gob.pe/>.*
- *En caso los proveedores no cuenten con inscripción vigente en el RNP y/o se encuentren inhabilitados o suspendidos para ser participantes, postores y/o contratistas, el SEACE restringirá su registro, quedando a potestad de estos intentar nuevamente registrar su participación en el procedimiento de selección en cualquier otro momento, dentro del plazo establecido para dicha etapa, siempre que haya obtenido la vigencia de su inscripción o quedado sin efecto la sanción que le impuso el Tribunal de Contrataciones del Estado.*

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

La formulación de consultas y observaciones a las bases se efectúa de conformidad con lo establecido en los numerales 72.1 y 72.2 del artículo 72 del Reglamento.

Importante

No pueden formularse consultas ni observaciones respecto del contenido de una ficha de homologación aprobada, aun cuando el requerimiento haya sido homologado parcialmente respecto a las características técnicas y/o requisitos de calificación y/o condiciones de ejecución. Las consultas y observaciones que se formulen sobre el particular, se tienen como no presentadas.

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

La absolución de consultas, observaciones e integración de las bases se realizan conforme a las disposiciones previstas en los numerales 72.4 y 72.5 del artículo 72 del Reglamento.

Importante

- No se absolverán consultas y observaciones a las bases que se presenten en forma física.
- Cuando exista divergencia entre lo indicado en el pliego de absolución de consultas y observaciones y la integración de bases, prevalece lo absuelto en el referido pliego; sin perjuicio, del deslinde de responsabilidades correspondiente.

1.6. ELEVACIÓN AL OSCE DEL PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y OBSERVACIONES E INTEGRACIÓN DE BASES

Los cuestionamientos al pliego de absolución de consultas y observaciones, así como a las bases integradas por supuestas vulneraciones a la normativa de contrataciones, a los principios que rigen la contratación pública u otra normativa que tenga relación con el objeto de la contratación, pueden ser elevados al OSCE de acuerdo a lo indicado en los numerales del 72.8 al 72.11 del artículo 72 del Reglamento.

La solicitud de elevación para emisión de Pronunciamiento se presenta ante la Entidad, la cual debe remitir al OSCE el expediente completo, de acuerdo a lo señalado en el artículo 124 del TUO de la Ley 27444, aprobado por Decreto Supremo N° 004-2019-JUS, al día hábil siguiente de recibida dicha solicitud.

Advertencia

La solicitud de elevación al OSCE de los cuestionamientos al pliego de absolución de consultas y observaciones, así como a las Bases integradas, se realiza de manera electrónica a través del SEACE, a partir de la oportunidad en que establezca el OSCE mediante comunicado.

Importante

Constituye infracción pasible de sanción según lo previsto en el literal n) del numeral 50.1 del artículo 50 de la Ley, presentar cuestionamientos maliciosos o manifiestamente infundados al pliego de absolución de consultas y/u observaciones.

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

Las ofertas se presentan conforme lo establecido en el artículo 59 del Reglamento.

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

Importante

¹ Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>

- *Los formularios electrónicos que se encuentran en el SEACE y que los proveedores deben llenar para presentar sus ofertas, tienen carácter de declaración jurada.*
- *En caso la información contenida en los documentos escaneados que conforman la oferta no coincida con lo declarado a través del SEACE, prevalece la información declarada en los documentos escaneados.*
- *No se tomarán en cuenta las ofertas que se presenten en físico a la Entidad.*

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

El participante presentará su oferta de manera electrónica a través del SEACE, desde las 00:01 horas hasta las 23:59 horas del día establecido para el efecto en el cronograma del procedimiento; adjuntando el archivo digitalizado que contenga los documentos que conforman la oferta de acuerdo a lo requerido en las bases.

El participante debe verificar antes de su envío, bajo su responsabilidad, que el archivo pueda ser descargado y su contenido sea legible.

Importante

Los integrantes de un consorcio no pueden presentar ofertas individuales ni conformar más de un consorcio en un procedimiento de selección, o en un determinado ítem cuando se trate de procedimientos de selección según relación de ítems.

En la apertura electrónica de la oferta, el comité de selección, verifica la presentación de lo exigido en la sección específica de las bases, de conformidad con el numeral 73.2 del artículo 73 del Reglamento y determina si las ofertas responden a las características y/o requisitos funcionales y condiciones de las Especificaciones Técnicas, detalladas en la sección específica de las bases. De no cumplir con lo requerido, la oferta se considera no admitida.

1.9. EVALUACIÓN DE LAS OFERTAS

La evaluación de las ofertas se realiza conforme a lo establecido en el artículo 74 del Reglamento.

El desempate mediante sorteo se realiza de manera electrónica a través del SEACE.

1.10. CALIFICACIÓN DE OFERTAS

La calificación de las ofertas se realiza conforme a lo establecido en los numerales 75.1 y 75.2 del artículo 75 del Reglamento.

1.11. SUBSANACIÓN DE LAS OFERTAS

La subsanación de las ofertas se sujeta a lo establecido en el artículo 60 del Reglamento. El plazo que se otorgue para la subsanación no puede ser inferior a un (1) día hábil.

La solicitud de subsanación se realiza de manera electrónica a través del SEACE y será remitida al correo electrónico consignado por el postor al momento de realizar su inscripción en el RNP, siendo su responsabilidad el permanente seguimiento de las notificaciones a dicho correo. La notificación de la solicitud se entiende efectuada el día de su envío al correo electrónico.

La presentación de las subsanaciones se realiza a través del SEACE. No se tomará en cuenta la subsanación que se presente en físico a la Entidad.

1.12. RECHAZO DE LAS OFERTAS

Previo al otorgamiento de la buena pro, el comité de selección revisa las ofertas económicas que cumplen los requisitos de calificación, de conformidad con lo establecido para el rechazo de ofertas, previsto en el artículo 68 del Reglamento, de ser el caso.

De rechazarse alguna de las ofertas calificadas, el comité de selección revisa el cumplimiento de los requisitos de calificación de los postores que siguen en el orden de prelación, en caso las hubiere.

1.13. OTORGAMIENTO DE LA BUENA PRO

Definida la oferta ganadora, el comité de selección otorga la buena pro, mediante su publicación en el SEACE, incluyendo el cuadro comparativo y las actas debidamente motivadas de los resultados de la admisión, no admisión, evaluación, calificación, descalificación, rechazo y el otorgamiento de la buena pro.

1.14. CONSENTIMIENTO DE LA BUENA PRO

Cuando se hayan presentado dos (2) o más ofertas, el consentimiento de la buena pro se produce a los ocho (8) días hábiles siguientes de la notificación de su otorgamiento, sin que los postores hayan ejercido el derecho de interponer el recurso de apelación.

En caso que se haya presentado una sola oferta, el consentimiento de la buena pro se produce el mismo día de la notificación de su otorgamiento.

El consentimiento del otorgamiento de la buena pro se publica en el SEACE al día hábil siguiente de producido.

Importante

Una vez consentido el otorgamiento de la buena pro, el órgano encargado de las contrataciones o el órgano de la Entidad al que se haya asignado tal función realiza la verificación de la oferta presentada por el postor ganador de la buena pro conforme lo establecido en el numeral 64.6 del artículo 64 del Reglamento.

CAPÍTULO II SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

A través del recurso de apelación se pueden impugnar los actos dictados durante el desarrollo del procedimiento de selección hasta antes del perfeccionamiento del contrato.

El recurso de apelación se presenta ante y es resuelto por el Tribunal de Contrataciones del Estado.

Los actos que declaren la nulidad de oficio, la cancelación del procedimiento de selección y otros actos emitidos por el Titular de la Entidad que afecten la continuidad de este, se impugnan ante el Tribunal de Contrataciones del Estado.

Importante

- *Una vez otorgada la buena pro, el comité de selección, está en la obligación de permitir el acceso de los participantes y postores al expediente de contratación, salvo la información calificada como secreta, confidencial o reservada por la normativa de la materia, a más tardar dentro del día siguiente de haberse solicitado por escrito.*

Luego de otorgada la buena pro no se da a conocer las ofertas cuyos requisitos de calificación no fueron analizados y revisados por el comité de selección.

- *A efectos de recoger la información de su interés, los postores pueden valerse de distintos medios, tales como: (i) la lectura y/o toma de apuntes, (ii) la captura y almacenamiento de imágenes, e incluso (iii) pueden solicitar copia de la documentación obrante en el expediente, siendo que, en este último caso, la Entidad deberá entregar dicha documentación en el menor tiempo posible, previo pago por tal concepto.*
- *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

La apelación contra el otorgamiento de la buena pro o contra los actos dictados con anterioridad a ella se interpone dentro de los ocho (8) días hábiles siguientes de haberse notificado el otorgamiento de la buena pro.

La apelación contra los actos dictados con posterioridad al otorgamiento de la buena pro, contra la declaración de nulidad, cancelación y declaratoria de desierto del procedimiento, se interpone dentro de los ocho (8) días hábiles siguientes de haberse tomado conocimiento del acto que se desea impugnar.

CAPÍTULO III DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

Los plazos y el procedimiento para perfeccionar el contrato se realiza conforme a lo indicado en el artículo 141 del Reglamento.

Para perfeccionar el contrato, el postor ganador de la buena pro debe presentar los documentos señalados en el artículo 139 del Reglamento y los previstos en la sección específica de las bases.

3.2. GARANTÍAS

Las garantías que deben otorgar los postores y/o contratistas, según corresponda, son las de fiel cumplimiento del contrato y por los adelantos.

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

Como requisito indispensable para perfeccionar el contrato, el postor ganador debe entregar a la Entidad la garantía de fiel cumplimiento del mismo por una suma equivalente al diez por ciento (10%) del monto del contrato original. Esta se mantiene vigente hasta la conformidad de la recepción de la prestación a cargo del contratista.

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

En las contrataciones que conllevan la ejecución de prestaciones accesorias, tales como mantenimiento, reparación o actividades afines, se otorga una garantía adicional por una suma equivalente al diez por ciento (10%) del monto del contrato de la prestación accesorio, la misma que debe ser renovada periódicamente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

3.2.3. GARANTÍA POR ADELANTO

En caso se haya previsto en la sección específica de las bases la entrega de adelantos, el contratista debe presentar una garantía emitida por idéntico monto conforme a lo estipulado en el artículo 153 del Reglamento.

3.3. REQUISITOS DE LAS GARANTÍAS

Las garantías que se presenten deben ser incondicionales, solidarias, irrevocables y de realización automática en el país, al solo requerimiento de la Entidad. Asimismo, deben ser emitidas por empresas que se encuentren bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, deben estar autorizadas para emitir garantías; o estar consideradas en la última lista de bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.

Importante

Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro y/o contratista cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.

Advertencia

Los funcionarios de las Entidades no deben aceptar garantías emitidas bajo condiciones distintas a las establecidas en el presente numeral, debiendo tener en cuenta lo siguiente:

- 1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (<http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo>).*
- 2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.*
- 3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.*
- 4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.*

En caso exista alguna duda sobre la clasificación de riesgo asignada a la empresa emisora de la garantía, se deberá consultar a la clasificadora de riesgos respectiva.

De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (<http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza>).

Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.

3.4. EJECUCIÓN DE GARANTÍAS

La Entidad puede solicitar la ejecución de las garantías conforme a los supuestos contemplados en el artículo 155 del Reglamento.

3.5. ADELANTOS

La Entidad puede entregar adelantos directos al contratista, los que en ningún caso exceden en conjunto del treinta por ciento (30%) del monto del contrato original, siempre que ello haya sido previsto en la sección específica de las bases.

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, de conformidad con el artículo 162 del Reglamento.

3.6.2. OTRAS PENALIDADES

La Entidad puede establecer penalidades distintas a la mencionada en el numeral precedente, según lo previsto en el artículo 163 del Reglamento y lo indicado en la sección específica de las bases.

Estos dos tipos de penalidades se calculan en forma independiente y pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

3.7. INCUMPLIMIENTO DEL CONTRATO

Las causales para la resolución del contrato, serán aplicadas de conformidad con el artículo 36 de la Ley y 164 del Reglamento.

3.8. PAGOS

El pago se realiza después de ejecutada la respectiva prestación, pudiendo contemplarse pagos a cuenta, según la forma establecida en la sección específica de las bases o en el contrato.

La Entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los bienes, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

La conformidad se emite en un plazo máximo de siete (7) días de producida la recepción salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad del funcionario que debe emitir la conformidad.

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.

Advertencia

En caso de retraso en los pagos a cuenta o pago final por parte de la Entidad, salvo que se deba a caso fortuito o fuerza mayor, esta reconoce al contratista los intereses legales correspondientes, de conformidad con el artículo 39 de la Ley y 171 del Reglamento, debiendo repetir contra los responsables de la demora injustificada.

3.9. DISPOSICIONES FINALES

Todos los demás aspectos del presente procedimiento no contemplados en las bases se regirán supletoriamente por la Ley y su Reglamento, así como por las disposiciones legales vigentes.

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

(EN ESTA SECCIÓN LA ENTIDAD DEBERÁ COMPLETAR LA INFORMACIÓN EXIGIDA, DE ACUERDO A LAS INSTRUCCIONES INDICADAS)



CAPÍTULO I GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre : **Dirección Nacional de Inteligencia**
RUC N° : 20502628128
Domicilio legal : Av. Edmundo Aguilar Pastor S/N – Chorrillos (ex. Av. Las Palmas)
Teléfono: : 6175400
Correo electrónico: : of127@dni.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación de la Adquisición de un Sistema de Protección y Seguridad Firewall Perimetral – Red Externa

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Hoja de Aprobación de Expediente N° 024-2024 el 18 de julio de 2024.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios

Importante

La fuente de financiamiento debe corresponder a aquella prevista en la Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal en el cual se convoca el procedimiento de selección.

1.5. SISTEMA DE CONTRATACIÓN

El presente procedimiento se rige por el sistema de SUMA ALZADA, de acuerdo con lo establecido en el expediente de contratación respectivo.

1.6. MODALIDAD DE EJECUCIÓN

LLAVE EN MANO

1.7. DISTRIBUCIÓN DE LA BUENA PRO

No aplica

1.8. ALCANCES DEL REQUERIMIENTO

El alcance de la prestación está definido en el Capítulo III de la presente sección de las bases.

1.9. PLAZO DE ENTREGA

Los bienes materia de la presente convocatoria se entregarán en el plazo de:

Prestación Principal

El proveedor debe realizar la entrega total de la solución ofertada implementada y operando a un 100% con todas sus funcionalidades habilitadas máximo el 21 de diciembre de 2024.

El periodo de vigencia de la solución ofertada debe ser de treinta y seis (36) meses, el cual empezará a partir del 22 de diciembre de 2024. Las licencias y soporte del fabricante deben estar homologados su inicio y termino de vigencia.

Prestación Accesorias

Del Soporte Técnico: La ejecución de la prestación del servicio será durante el periodo de treinta y seis (36) meses; el cual se contabilizará a partir del 22 de diciembre de 2024

En concordancia con lo establecido en el expediente de contratación.

CONSULTA 10 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Amablemente se informa a la entidad que en todas las plataformas de NGFW es estrictamente necesario y obligatorio contar con la licencia activada para poder iniciar con la implementación/configuración de los firewalls; motivo por el cual no es viable que la licencia sea activada desde el 22 de diciembre de 2024 como la entidad solicita.

Agradecemos por favor modificar este requerimiento de tal forma que la activación de la licencia sea desde el día de inicio de implementación (indicar fecha) hasta el 22 de diciembre 2027. O en su defecto, que la vigencia de la licencia sea de 3 años desde el día de inicio de implementación.

RESPUESTA A CONSULTA 10 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

No se acoge lo solicitado, debido a que las licencias vence el 21 de diciembre de 2024 de acuerdo a lo establecido en las bases.

CONSULTA 11 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Entendiendo que se tiene como fecha límite de implementación el 21 de diciembre de 2024, agradecemos a la entidad indicar con que personal por parte de la entidad se asignara a este proyecto para garantizar la completa fluidez de las tareas durante la configuración y pruebas de la solución.

RESPUESTA A CONSULTA 11 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que los datos del personal por parte de la entidad será otorgado al inicio del contrato.

CONSULTA 12 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Entendiendo que se tiene como fecha límite de implementación el 21 de diciembre de 2024, agradecemos a la entidad indicar que sucederá con los retrasos en la implementación que sean generados por retrasos por parte de la entidad.

RESPUESTA A CONSULTA 12 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que la entidad brindara las facilidades técnicas al contratistas a fin de no incurrir en retrasos.

1.10. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo

efecto deben cancelar el monto de S/ 5.00 (cinco con 00/100 soles) en Caja de la entidad, sito en Av. Edmundo Aguilar Pastor S/N (ex – Av. Las Palmas) – Chorrillos, en el horario de 08:30 a 17:30 horas.

Importante

El costo de entrega de un ejemplar de las bases no puede exceder el costo de su reproducción.

1.11. BASE LEGAL

- Ley N° N°31953 Ley de Presupuesto del Sector Público para el Año Fiscal 2024.
- Ley N°31954 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2024.
- Decreto Supremo N°082-2019-EF – Texto Único Ordenado de la Ley de Contrataciones del Estado, en adelante la ley.
- Decreto Supremo N°344-2018-EF, Reglamento de la Ley de contrataciones del Estado y sus modificatorias, en adelante el Reglamento.
- Ley N°27806 - Ley de Transparencia y Acceso a la Información Pública.
- Código Civil.
- Directivas del OSCE.
- Ley N° 29783, Ley de Seguridad y Salud en el Trabajo
- Ley N° 30222, Ley que modifica la Ley de Seguridad y Salud en el Trabajo
- D.S. N° 005-2012-TR, Reglamento de la Ley N° 29783.
- D.S. N° 016-2016-TR, Modifica el Reglamento de la Ley N° 29783.
- Norma SHA Seguridad, Higiene, Ambiente.
- Ley de Contrataciones del Estado N° 30225 y sus modificaciones.

Las referidas normas incluyen sus respectivas modificaciones, de ser el caso.

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

Según el cronograma de la ficha de selección de la convocatoria publicada en el SEACE.

Importante

De conformidad con la vigesimosegunda Disposición Complementaria Final del Reglamento, en caso la Entidad (Ministerios y sus organismos públicos, programas o proyectos adscritos) haya difundido el requerimiento a través del SEACE siguiendo el procedimiento establecido en dicha disposición, no procede formular consultas u observaciones al requerimiento.

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos², la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

- Declaración jurada de datos del postor. (**Anexo N° 1**)
- Documento que acredite la representación de quien suscribe la oferta.

En caso de persona jurídica, copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto.

En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda.

En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE³ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.

- Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. (**Anexo N° 2**)
- Declaración jurada de cumplimiento de las Especificaciones Técnicas contenidas en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo N° 3**)

Incorporar a las bases o eliminar, según corresponda

² La omisión del índice no determina la no admisión de la oferta.

³ Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

- e) Declaración jurada de plazo de entrega. **(Anexo N° 4)**⁴
- f) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)**
- g) El precio de la oferta en soles. Adjuntar obligatoriamente el **Anexo N° 6**.

El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales. Los precios unitarios pueden ser expresados con más de dos (2) decimales.
- h) Declaración Jurada que indique ser representante y/o distribuidor y/o partner para la distribución y soporte de la solución ofertada.
- i) Carta de compromiso del Personal Clave **(Anexo N° 07)**, debidamente acreditada con copias de los documentos indicados en la declaración jurada para cada personal clave requerido en las especificaciones técnicas.
- j) Declaración jurada para acreditar el sustento técnico de la solución propuesta **(Anexo N° 12)**. Indicar en la oferta, el cumplimiento de las especificaciones técnicas mínimas requeridas, lo cual evidenciará en la documentación técnica (indicar el folio específico) del sustento (folletos, instructivos, catálogos o similares de fuentes del fabricante) que demuestre el cumplimiento de las mismas (no direcciones de sitios ni links), así como su descripción detallada en forma resaltada. Pudiendo presentar los documentos en su idioma original junto con su traducción simple al castellano en caso de encontrarse en lengua extranjera. Las cartas del fabricante no podrán emplearse para el sustento técnico.
- k) Declaración Jurada por los servicios profesionales del fabricante para garantizar el cumplimiento de lo exigido en el numeral 5.1.12 del Capítulo III de las bases. **(Anexo N° 13)**

CONSULTA 14 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

h) Declaración Juada que indique ser representante y/o distribuidor y/o partner para la distribución y soporte de la solución ofertada.

En aras de garantizar información sustentatoria por parte del fabricante de la solución ofertada y considerando lo solicitado en el literal K de los requisitos para perfeccionar el contrato sírvase aceptar que para acreditar que el postor sea distribuidor autorizado sea tan solo con la carta del mismo fabricante.

RESPUESTA A CONSULTA 14 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que el postor podría presentar además de lo solicitado en las bases, la carta del fabricante que indique ser representante y/o distribuidor y/o partner para la distribución y soporte de la solución ofertada.

CONSULTA 20 DE PLATAFORMA TECNOLOGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Dado que resulta razonable requerir que el postor cuente con una relación comercial con el fabricante de la marca de la solución que oferta y en aras de que dicha solución pueda tener un tiempo previsible de duración -por mantenimientos y repuestos-; posibilidades de adecuación; integración o repotenciar si fuera necesario, en atención al Principio de ¿Vigencia tecnológica ¿(Ver el literal g) del artículo 2 de la Ley.) que es aplicable transversalmente a cualquier contratación estatal.

⁴ En caso de considerar como factor de evaluación la mejora del plazo de entrega, el plazo ofertado en dicho anexo servirá también para acreditar este factor.

Asimismo, dado que el Formato ¿Resumen Ejecutivo de las Actuaciones Preparatorias¿, la Entidad declaró la pluralidad de proveedores y/o marcas, en la capacidad de cumplir con el íntegro del requerimiento, lo cual incluye la condición de representante, distribuidor o concesionario de la marca ofertada en el país o de empresa autorizada a comercializar la marca en el Perú por el fabricante de esta. Se solicita al Comité Especial incluir adjunta a la ¿declaración Jurada que indique ser representante y/o distribuidor y/o partner para la distribución y soporte de la solución ofertada¿ la carta emitida por el fabricante de la solución ofertada, la cual sustente la condición del postor y que esta condición tenga una vigencia no exceda los últimos seis (06) meses.

RESPUESTA A CONSULTA 20 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que el postor podría presentar además de lo solicitado en las bases, la carta del fabricante que indique ser representante y/o distribuidor y/o partner para la distribución y soporte de la solución ofertada. Asimismo, dicho documento es un requisito para el perfeccionamiento del contrato el cual deberá estar vigente.

OBSERVACION 44 DE JAPAN COMPUTER SERVICE S.A.C.

"Dentro de la documentación para la admisión de la oferta se solicita: ""j) Declaración jurada para acreditar el sustento técnico de la solución propuesta (Anexo N° 12). Indicar en la oferta, el cumplimiento de las especificaciones técnicas mínimas requeridas, lo cual evidenciará en la documentación técnica

(indicar el folio específico) del sustento (folletos, instructivos, catálogos o similares de fuentes del fabricante) que demuestre el cumplimiento de las mismas (no direcciones de sitios ni links), así como su descripción detallada en forma resaltada. Pudiendo presentar los documentos en su idioma original junto con su traducción simple al castellano en caso de encontrarse en lengua extranjera. Las cartas del fabricante no podrán emplearse para el sustento técnico"".

En atención a ello, cabe señalar que, en las Bases Estándar aplicables al objeto de la convocatoria se ha establecido que, las especificaciones técnicas se acreditan con la ¿Declaración Jurada de cumplimiento de las Especificaciones Técnicas¿ (Anexo N° 3), siendo que, se podría afianzar la acreditación de algunas especificaciones técnicas del requerimiento a través de la presentación adicional folletos, instructivos, catálogos o similares, para lo cual la Entidad debe especificar con claridad qué aspectos de las características y/o requisitos funcionales serán acreditados con la documentación requerida.

OBSERVACIÓN:

En concordancia con lo establecido en la Resolución N° 2034-2018-TCE-S1, el Tribunal de Contrataciones del Estado ha establecido lo siguiente: ¿(...) no es posible acreditar la totalidad de especificaciones técnicas del bien ofertado con hojas técnicas, catálogos, brochures y manuales de fabricante, ello atendiendo a que la información requerida por las entidades no es homogénea y obedece a las particularidades de su necesidad¿.

Por lo tanto, debido a que NO es posible acreditar la totalidad de las especificaciones técnicas, sírvase indicar cuáles serán los puntos técnicos obligatorios a sustentar de forma detallada y documentada dentro de los ítems (5.1.1. al 5.1.97) de las Especificaciones Técnicas. Asimismo, sírvase a modificar el ANEXO N° 12 de acuerdo a esta respuesta.

RESPUESTA A OBSERVACION 44 DE JAPAN COMPUTER SERVICE S.A.C.

Se aclara que los puntos técnicos obligatorios a sustentar de forma detallada y documentada son todos los puntos solicitados en la 5.1 de las bases a excepción de los siguientes (5.1.1, 5.1.3, 5.1.5, 5.1.12, 5.1.13, 5.1.14, 5.1.45, 5.1.61, 5.1.70, 5.1.79, 5.1.81, 5.1.86, 5.1.87, 5.1.95, 5.1.96, 5.1.97), sin embargo, deberá indicar el cumplimiento de las mismas en el Anexo N° 12

CONSULTA 104 DE IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.

Dice: "Indicar en la oferta, el cumplimiento de las especificaciones técnicas mínimas requeridas, lo cual se evidenciará en la documentación técnica."

Consulta:

Considerando que no todos los puntos técnicos exigidos en bases se pueden encontrar en documentación pública de los fabricantes, se solicita a la Entidad confirmar que se aceptará como sustento de cumplimiento una carta de fabricante para aquellos puntos que no estén disponibles en folletos, instructivos, catálogos o similares de fuentes de la marca, toda vez que es el mismo fabricante la fuente autorizada para validar el cumplimiento de las características solicitadas

RESPUESTA A CONSULTA 104 DE IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.

Se aclara que los puntos técnicos obligatorios a sustentar de forma detallada y documentada son todos los puntos solicitados en la 5.1 de las bases a excepción de los siguientes (5.1.1, 5.1.3, 5.1.5, 5.1.12, 5.1.13, 5.1.14, 5.1.45, 5.1.61, 5.1.70, 5.1.79, 5.1.81, 5.1.86, 5.1.87, 5.1.95, 5.1.96, 5.1.97), sin embargo deberá indicar el cumplimiento de las mismas en el Anexo N° 12

Importante

El comité de selección verifica la presentación de los documentos requeridos. De no cumplir con lo requerido, la oferta se considera no admitida.

2.2.1.2. Documentos para acreditar los requisitos de calificación

Incorporar en la oferta los documentos que acreditan los **"Requisitos de Calificación"** que se detallan en el numeral 3.2 del Capítulo III de la presente sección de las bases.

Advertencia

El comité de selección no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápite "Documentos para la admisión de la oferta", "Requisitos de calificación" y "Factores de evaluación".

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

El postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:

- Garantía de fiel cumplimiento del contrato.
- Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso.
- Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.
- Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
- Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁵ y

⁵ Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) Declaración Jurada de Reserva y Confidencialidad. (**Anexo 10**)
- i) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación⁶ (**Anexo N° 11**).
- j) Detalle de los precios unitarios del precio ofertado⁷.
- k) Carta del fabricante que acredite ser representante y/o distribuidor y/o partner autorizado para la distribución y soporte de la solución ofertada.
- l) Carta del fabricante que acredite el cumplimiento de los servicios profesionales para garantizar lo exigido en el numeral 5.1.12 del Capítulo III de las bases.

Importante

- *En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y en el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*
- *En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

Importante

- *Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.*
- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya⁸.*
- *La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en Mesa de Partes de la entidad, sito en Av. Edmundo Aguilar Pastor S/N – Chorrillos, en el horario de 08:30 a 17:30 horas.

⁶ En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

⁷ Incluir solo en caso de la contratación bajo el sistema a suma alzada.

⁸ Según lo previsto en la Opinión N° 009-2016/DTN.

Importante

En el caso de procedimientos de selección por relación de ítems, se puede perfeccionar el contrato con la suscripción del documento o con la recepción de una orden de compra, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200,000.00).

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista de conformidad a lo señalado en el numeral 13 del Capítulo III – Requerimiento de las presentes bases, de acuerdo al siguiente detalle:

Prestación principal

La DINI realizará la cancelación de la prestación principal en un único pago y se hará efectiva dentro de los diez (10) días calendario de emitida la respectiva conformidad, siempre que se verifiquen las condiciones establecidas en el contrato.

Prestaciones accesorias

Soporte técnico

El pago se realizará de forma anual, dentro de los diez (10) días calendario de emitida la respectiva conformidad, siempre que se verifiquen las condiciones establecidas en el contrato.

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

- Recepción del área de Almacén de la entidad.
- Informe del funcionario responsable de la Oficina de Tecnologías de la Información y Comunicaciones emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Demás documentos solicitados en el Capítulo III- Requerimiento de las presentes bases.

Dicha documentación se debe presentar en Mesa de Partes de la entidad, sito en Av. Edmundo Aguilar Pastor S/N (ex. Av. Las Palmas) – Chorrillos en el horario de 08:30 a 17:30 horas y/o a través de la mesa de partes virtual de la entidad <https://facilita.gob.pe/t/1864>

CAPÍTULO III REQUERIMIENTO

Importante

De conformidad con el numeral 29.8 del artículo 29 del Reglamento, el área usuaria es responsable de la adecuada formulación del requerimiento, debiendo asegurar la calidad técnica y reducir la necesidad de su reformulación por errores o deficiencias técnicas que repercutan en el proceso de contratación.

3.1. ESPECIFICACIONES TÉCNICAS

1. Denominación de la contratación

"ADQUISICIÓN DE UN SISTEMA DE PROTECCIÓN Y SEGURIDAD FIREWALL PERIMETRAL - RED EXTERNA".

CONSULTA 1 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se solicita a la entidad confirmar por favor, si la instalación de los dos firewalls se debe realizar en el centro de datos Institucional O el Firewall de Alta Disponibilidad se debe desplegar en un data center diferente. Por favor confirmar ciudades y direcciones de el/los centros de datos.

RESPUESTA A CONSULTA 1 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que la instalación de los dos (2) firewall será en la Av. Edmundo Aguilar S/n Chorrillos, la cual esta indicada en las bases.

CONSULTA 2 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Sírvase confirmar que la entidad suministrara en el centro de datos recursos como cableado de red (Cobre y fibra), puntos de datos y eléctricos, espacio en rack.

RESPUESTA A CONSULTA 2 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que la entidad brindará los recursos como cableado de red (Cobre y fibra), puntos de datos y eléctricos, espacio en rack. Sin embargo, el contratista no elude la inclusión de todos los elementos necesarios para que los bienes/servicios ofertados funcionen correctamente de acuerdo a la modalidad llave en mano indicado en el punto 5.4

CONSULTA 3 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que la entidad brindara los puntos de datos y eléctricos, espacio en rack. Los cables patch Cord (Alcance corto de min 1.5 mts) de F.O/UTP deberán ser provistos por el contratista.

RESPUESTA A CONSULTA 3 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que la entidad brindará los recursos como cableado de red (Cobre y fibra). Sin embargo, el contratista no elude la inclusión de todos los elementos necesarios para que los bienes/servicios ofertados funcionen correctamente de acuerdo a la modalidad llave en mano indicado en el punto 5.4

2. Finalidad pública

El presente proceso de selección tiene como finalidad adquirir un sistema de protección y seguridad firewall perimetral para proteger los servicios internos de amenazas cibernéticas, a fin de mejorar el esquema de seguridad en la infraestructura tecnológica del Centro de Datos Institucional para que no afecte el cumplimiento de las funciones y actividades propias de la entidad.

3. Antecedentes

Como parte de su infraestructura tecnológica, la Dirección Nacional de Inteligencia cuenta con una solución de protección y seguridad firewall perimetral adquiridos en el año 2019 y que cada año se ha venido renovando la garantía y soporte de fábrica, los cuales actualmente cuentan con licenciamiento, garantía y soporte de fábrica hasta el 21DIC2024, fecha en la que ya no se podrá renovar por un año más y menos continuará protegiendo la infraestructura tecnológica de la entidad.

4. Objetivos de la contratación

La Dirección Nacional de Inteligencia, con el objetivo de mantener y mejorar los controles de seguridad y protección contra amenazas de tipo cibernéticos, se necesita la adquisición de un sistema de protección y seguridad firewall perimetral, el propósito es elevar el esquema de seguridad y la protección ante amenazas conocidas y desconocidas a la infraestructura tecnológica de la institución, en razón que se brindará acceso a internet en forma controlada a los usuarios de la DINI para actualizar las aplicaciones que soportan los procesos de producción y apoyo.

5. Características y condiciones de los bienes a contratar

5.1. Descripción y cantidad de los bienes

No.	Descripción	Cumple Sí o no	Observación de ser el caso
5.1.1	Cantidad: Dos (02) unidades de Firewall		
5.1.2	Los equipos deben ser hardware y software integrados de tipo appliance o chassis y provistos por el mismo fabricante. No se aceptarán servidores o máquinas virtuales.		
5.1.3	El hardware ofertado deberá ser totalmente nuevo.		
5.1.4	Altura máxima de 01 RU, con sus respectivos rieles telescópicos para montaje en gabinete 19"		
5.1.5	El sistema operativo deberá ser del fabricante de la solución ofertada, el mismo deberá venir de fábrica con el "hardening" necesario, el fabricante deberá desarrollar las actualizaciones de sistema operativo, parches del software o módulos utilizados por la solución ofertada.		
5.1.6	El fabricante de la solución propuesta debe recibir actualizaciones de inteligencia de amenazas provenientes de otros fabricantes a través del Cyber Threat Alliance, con el propósito de contar con un óptimo nivel de prevención de amenazas cibernéticas. El fabricante debe aparecer como miembro en la web oficial del Cyber Threat Alliance para lo cual debe presentar la versión impresa del sitio web de Cyber Threat Alliance, acompañado del link de la página impresa.		
5.1.7	El fabricante de la solución de seguridad debe estar presente en los últimos 08 reportes de Gartner (Magic Cuadrant), en el cuadrante de Líderes para Network Enterprise Firewalls.		
5.1.8	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciados 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 el link público de los equipos propuestos donde se verifique que los modelos propuestos no están en ese listado o sustentado mediante carta del fabricante dirigido al proceso.		
5.1.9	Los sistemas operativos que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas. Esto se aplicará únicamente al Sistema Operativo o firmware que se instalará en la entidad sobre los equipos propuestos por el postor.		
5.1.10	El sistema debe estar habilitado y configurado con las políticas de todas las funcionalidades: <ul style="list-style-type: none"> • Firewall. • Control de aplicaciones. • Sistema de Prevención de Intrusos (IPS). • Antivirus o Antimalware. • Emulación de amenazas (Sandbox). • Filtrado de comando y control, antibot o antispyware.- 		

	<p>• DNS Security.</p> <p>Que permita detectar y bloquear (prevenir) virus y malware que se propaguen, al menos, en los siguientes protocolos: HTTP, FTP, SMB, SMTP, IMAP, POP3 y SSL o TLS, que cubran finalmente el objetivo requerido.</p>		
5.1.11	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basado en usuarios y grupos de usuarios.		
5.1.12	<p>La implementación debe ser validada por los servicios profesionales del fabricante y al finalizar la validación deberá emitir un informe de aplicación de mejores prácticas en la habilitación de todas las funcionalidades y aplicando las políticas de seguridad por cada funcionalidad. Se debe contemplar un mínimo de 4 días de los servicios profesionales del fabricante.</p> <p>Para garantizar el cumplimiento de los servicios profesionales del fabricante se deberá sustentar una declaración jurada en la presentación de la propuesta y una carta del fabricante a la firma del contrato. Al finalizar la implementación se requiere un informe de los servicios profesionales del fabricante.</p> <p>Por otro lado, se aceptará que las actividades que realice este personal sean de manera remota siempre y cuando se cumpla con algunos requisitos, por motivos de seguridad nacional, que se especificarán una vez se haya realizado la firma y perfeccionamiento del contrato. Este personal debe ser de habla hispana.</p>		
5.1.13	El proveedor deberá considerar en la implementación los servicios de Networking necesario para la implementación (configuración del core, Switches, reglas en firewall perimetral e interno y aplicación de buenas prácticas para la convivencia de la red externa con la interna).		
5.1.14	El nivel de soporte del fabricante debe ser 24 x 7 durante el periodo del contrato. Debiendo ser asistido por el propio personal del fabricante a través de su propio centro de atención, y en coordinación directa con el contratista para el seguimiento y escalamiento de los requerimientos.		
Características Técnicas de cada Firewall			
5.1.15	El throughput como mínimo debe ser 5.8 Gbps para "Threat Prevention o Threat Protection" con las funcionalidades habilitadas: Application Control, IPS, Antivirus, Anti-Bot o Antispyware y Protección contra Dia Cero con logging activo; medido en condiciones de prueba empresariales o en transacciones de aplicaciones mixtas. Asimismo, el throughput mínimo de 9 Gbps de Next Generation Firewall o Firewall con todas las funcionalidades definidas por cada fabricante medido en condiciones de prueba empresariales o en transacciones de aplicaciones mixtas. No se aceptarán otras mediciones a las indicadas		
5.1.16	Debe soportar al menos cien mil (100 000) conexiones o sesiones por segundo.		
5.1.17	Debe soportar al menos 1'000,000 de conexiones o sesiones concurrentes.		
5.1.18	Cada equipo deberá contar con dos fuentes de poder de 100-240 VAC 50-60 Hz.		
5.1.19	Las fuentes de poder podrían ser de tipo hot-swap (cambio en caliente).		
5.1.20	Cada equipo deberá tener como mínimo 8 interfaces de cobre GE RJ45.		
5.1.21	Debe incluir un (01) puerto de administración dedicado y un (01) para HA dedicado.		
5.1.22	Debe soportar alta disponibilidad en modo activo/pasivo y modo activo/activo.		
5.1.23	Administración a través de SSH y de interfaz Web segura (HTTPS).		
Prevención de amenazas			
5.1.24	Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en tiempo real en el repositorio la clasificación y/o reputación de		

	direcciones IP y/o Dominios y/o URL y/o redes de C2 o Comando y Control y/o ataques DoS.		
5.1.25	La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.		
5.1.26	Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web, Mail (SMTP o POP3), SMB, FTP y SSL o TLS.		
5.1.27	Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real.		
5.1.28	La identificación de amenazas avanzadas camufladas en tráfico DNS deberá contar con mecanismos avanzados de detección con el objetivo de identificar ataques imposibles de mitigar con firmas y/o reputación del dominio. Para ello se requiere que el tráfico DNS sea analizado con técnicas de inteligencia artificial y/o análisis predictivo y/o machine learning en tiempo real.		
5.1.29	Debe soportar Inspección de tráfico cifrado/encryptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).		
5.1.30	Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware.		
5.1.31	Debe soportar el manejo personalizado (añadir, borrar o modificar) para registrar IoC (Indicadores de Compromiso) o listas dinámicas externa, siempre y cuando se cumpla con el requerimiento solicitado.		
5.1.32	Debe tener capacidad de integración con fuente de IoC de terceros (External IoC) a través de direcciones web URL, con capacidades de detección y prevención o listas dinámicas externa, siempre y cuando se cumpla con el requerimiento solicitado. La aplicación y prevención de seguridad, en base a los IoC o listas dinámicas externa incluidos, debe ser de manera automática, sin interacción del usuario administrador una vez aplicada a una política de seguridad.		
Funcionalidades de red			
5.1.33	Para tráfico cifrado SSL debe ser capaz de inspeccionar tráfico cifrado en TLS 1.3 y debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.		
5.1.34	Debe soportar L2 y L3.		
5.1.35	Deben soportar inspección del tráfico cifrado (SSL/TLS).		
5.1.36	Deberá soportar descifrado del tráfico considerando al menos los siguientes algoritmos: RSA y/o DHE y/o ECDHE y/o 3DES y/o RC4 y/o AES128 y/o AES256 y/o CHACHA20-POLY1305 y/o MD5 y/o SHA1 y/o SHA256 y/o SHA384.		
5.1.37	Debe soportar IPv4 e IPv6.		
5.1.38	Debe poder realizar límites de ancho de banda (upload/download) para controlar tráfico por tipo de destino, servicio y/o aplicación.		
5.1.39	Los firewalls deben soportar como mínimo 1,024 VLANs Tags 802.3ad.		
Gestión de políticas			
5.1.40	Las reglas de firewall deben poder tener limitantes y/o vigencia en base a tiempo o determinado periodo.		
5.1.41	El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como direcciones IP, redes, usuarios, grupos de usuarios, servicios de red		
	, direcciones de URL y aplicaciones.		
Geolocalización			
5.1.42	Soportar la creación de políticas basadas en Geolocalización, configurando que el tráfico de determinado País y/o Países sean bloqueados o permitidos.		
5.1.43	Debe contar con la visualización de los países de origen y destino en los logs de acceso.		
5.1.44	Debe contar con la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.		

5.1.45	Las actualizaciones de las direcciones o rangos de IP publica por cada país, debe realizarse periódicamente y de manera automática.		
IPS			
5.1.46	El IPS debe contar con mecanismo de detección de amenazas de múltiples niveles o métodos: detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías, detección basada en comportamiento.		
5.1.47	A nivel de aplicación, debe incluir protecciones tipo Cross Site Scripting y/o SQL Injection y/o Command Injection e injection protección para DN (Distinguished Names) y/o C&C desconocidos.		
5.1.48	Las firmas de protección de IPS deben poder categorizarse según un nivel de severidad, nivel de efectividad (confianza) o explotación cloud en línea o exploit-kit y nivel consumo de recursos o fuerza bruta.		
5.1.49	Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP y/o SMTP y/o IMAP y/o DNS y/o FTP y/o SNMP y/o IMAP y/o SMB.		
5.1.50	Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos.		
5.1.51	Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound.		
5.1.52	Debe permitir adicionar excepciones a las protecciones de IPS.		
5.1.53	Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense.		
5.1.54	Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos o ataques conocidos.		
5.1.55	Detección y prevención del uso indebido de un protocolo o ataques no basados en protocolos IP, para actividad maliciosa o amenaza potencial.		
5.1.56	Detección y prevención de comunicaciones de malware tipo C&C salientes.		
5.1.57	Detección y prevención de intentos de tunelización, para intentos de fuga de datos o intentos de eludir otras medidas de seguridad, como el filtrado web.		
Protección de DNS			
5.1.58	La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de URL y recursos DNS no identificados y/o no clasificados al momento de ser registrado.		
5.1.59	La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA), empleando protección basada en Machine Learning, así como protección fuga o exfiltración de información mediante DNS Tunneling, en tiempo real		
5.1.60	La solución debe contar con análisis la reputación de direcciones URL y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).		
5.1.61	La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de URL y recursos DNS no identificados y/o no clasificados al momento de ser registrado,		
Protección de amenazas desconocidas			
5.1.62	La solución debe ser capaz de emular o ejecutar los archivos identificados en el firewall de forma automática, a través del envío y posterior análisis en la nube del propio fabricante de firewall, para la emulación o ejecución de malware de día cero (sandbox).		
5.1.63	La solución debe proteger a los usuarios internos de manera que prevenga el acceso o descarga a los archivos en tanto estos son analizados en el equipo de emulación, si el archivo es benigno se entrega el archivo original al usuario y si el archivo es maligno se deniega su acceso o descarga.		

5.1.64	Cada archivo emulado en el sandbox debe generar un reporte detallado que incluya información forense sobre la actividad maliciosa originada por el archivo.		
5.1.65	El motor de emulación debe admitir varios sistemas operativos, como Windows XP y/o Windows7 y/o Windows 10.		
5.1.66	Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (personalizado y hardenizado), inyección de código a procesos permitidos o análisis de memoria en run time.		
5.1.67	Se debe emular archivos desconocidos en el sandbox.		
Control de aplicaciones y filtro Web			
5.1.68	La funcionalidad de control de aplicaciones debe tener una detección y reconocimiento de al menos 3,600 aplicaciones distintas, entre ellas: Streaming o Video, P2P, Proxy, redes sociales, Juegos o similares.		
5.1.69	Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.		
5.1.70	Debido a que diariamente se crean decenas de miles de nuevas páginas web, la solución deberá ser capaz de analizar en tiempo real si la página web tiene contenido malicioso cuando un usuario intenta acceder.		
5.1.71	Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y soportar protección al protocolo HTTP/2, esta última deberá habilitarse desde la interfaz web.		
Inventario de dispositivos de red			
5.1.72	La solución deberá contar con un módulo de descubrimiento, identificación y clasificación de dispositivos como teléfonos IP y/o cámaras de vigilancia y/o consolas de videojuegos y/o impresoras y/o dispositivos médicos y/o equipos industriales y/o equipos de seguridad y/o servidores, entre otros. Este módulo debe contar con capacidades de protección de amenazas a través de las políticas de seguridad.		
5.1.73	El descubrimiento de los dispositivos debe mostrar la marca del fabricante y/o tipo de dispositivo y/o serial y/o sistema operativo y/o dirección IP y/o dirección MAC.		
5.1.74	Debe identificar dispositivos que posean software o hardware desactualizado y vulnerable, junto con su respectivo identificador CVE.		
5.1.75	Debe hacer uso del protocolo SNMP para integrarse a los switches.		
5.1.76	Debe descubrir dispositivos inclusive si el tráfico de los dispositivos de red no pasan por los NGFW.		
Revisión de salud de los Firewall			
5.1.77	Debe contar con un módulo integrado que monitoree continuamente los firewalls, en base a sus políticas y configuración de buenas prácticas y los compare con base de datos de estándares reconocidos de la industria como mínimo Cobit y/o ISO 27001 y/o NIST 800 53 o mejores prácticas de seguridad, con la finalidad de obtener reportes gráficos detallados informes que demuestren el cumplimiento de los estándares reconocidos de la industria aplicables o mejores prácticas recomendadas.		
5.1.78	Se deberá incluir una herramienta integrada y/o externa que genere alertas si existen problemas de salud del equipo en materia de hardware y software, como mínimo: consumo de memoria, problemas de la alta disponibilidad (HA), problemas de disco duro, , expiración de licencias.		
Inteligencia de amenazas			
5.1.79	Se debe proporcionar acceso a la base de datos de inteligencia de amenazas del fabricante, el cual debe permitir hacer consultas de Hashes, Dominios y Direcciones IP, para mostrar información sobre la amenaza, a nivel de clasificación, reputación, familia de malware, comportamiento.		
VPN			
5.1.80	Debe soportar túneles VPN punto a punto (Site-to-Site) y túneles de acceso remoto para usuario final (Client-to-Site).		

5.1.81	Debe estar licenciado para soportar 50 usuarios concurrentes o simultáneos de IPsec VPN Client-to-Site, con capacidad de VPN para dispositivos Windows, Linux y MAC, y también dispositivos móviles como Android y IOS.		
5.1.82	Debe poder integrarse con Directorio Activo Microsoft u Open LDAP para crear reglas de control de acceso a través de VPN, empleando: usuarios, grupos de usuarios, maquinas, dirección IP y redes.		
5.1.83	El cliente VPN, debe instalarse sobre sistemas operativos Windows y Linux.		
5.1.84	<p>Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado en sistema operativo Windows, que permita validar en base al nivel de cumplimiento (compliance) del host permitir, denegar o limitar el acceso a los recursos de la red interna. Por lo menos se deberá poder configurar los siguientes casos de uso siguientes:</p> <ul style="list-style-type: none"> ▪ Software antivirus instalado y habilitado ▪ Software antivirus con la base de datos de firmas actualizada ▪ Parche de seguridad instalado o dispositivos vulnerables, según su nivel de criticidad ▪ Software de DLP instalado, el cual debe ser identificado a través de las llaves de registro o procesos del sistema operativo 		
5.1.85	La solución debe soportar autenticación de doble factor.		
Transferencia de conocimiento			
5.1.86	<p>El proveedor deberá realizar la transferencia de conocimiento al personal de la DINI con respecto a la solución ofertada, incluyendo lo siguiente:</p> <ul style="list-style-type: none"> • Temáticas: administración, configuración, monitoreo y formulación de reportes personalizadas, funcionalidades avanzadas, diagnóstico/troubleshooting, backup/restore de las configuraciones. • Cantidad: cinco (05) participantes. • 16 horas como mínimo siempre y cuando se cumpla con los temas solicitados y deben ser desarrollados antes de culminar la implementación de la solución ofertada. 		
ADMINISTRACIÓN			
5.1.87	La administración deberá ser centralizada de todos los componentes de la solución ofertada incluyendo el licenciamiento para tal fin. Se requiere que se tenga un equipo de administración y recolección, análisis de logs y generación de reportes, pudiendo separar ambos roles según recomendación del fabricante.		
5.1.88	Debe ser provisto en Appliance físico, es decir software y hardware provistos por el mismo fabricante.		
5.1.89	Debe ser del mismo fabricante de los firewalls.		
5.1.90	Debe contar con un almacenamiento mínimo de 4TB en RAID 1 o superior.		
5.1.91	Debe soportar una ingesta de 12 000 log por segundo como mínimo.		
5.1.92	La gestión de la solución debe soportar acceso por SSH, cliente o WEB (HTTPS).		
5.1.93	Debe permitir accesos concurrentes de al menos dos administradores.		
5.1.94	Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita o similar, acceso de lectura, cambio de configuraciones o similar;		
5.1.95	Generar alertas automáticas por Email, SNMP y Syslog		

5.1.96	Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horario.		
	<p>La solución debe generar reportes personalizados, debiendo permitir al administrador determinar el contenido de los reportes con las siguientes funcionalidades:</p> <ul style="list-style-type: none"> • El contenido de los reportes deben incluir los datos en formato tabular (tablas) y/o gráficas (pie-chart, graph-chart) • Los reportes deben contar con la utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos. • Debe generar reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente o por destino. • Debe permitir generar la incidencia de virus detectados y a nivel red por fuente o por destino. • Debe permitir personalizar los criterios bajo los cuales será obtenido el reporte, tales como fuentes, destinos, servicios, fechas y/o día de la semana. • Debe permitir especificar el periodo de tiempo específico para el cual el reporte va a ser obtenido. • Debe permitir enviar el reporte via correo electrónico. 		
5.1.97	Los reportes serán parte del informe de implementación de la solución, no será parte de la fase de evaluación de las propuestas.		

CONSULTA 4 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Con la finalidad de poder hacer una estimación ajustada a las necesidades de la entidad, agradecemos por favor suministrar la siguiente información de la solución Checkpoint actual, para determinar el alcance de implementación:

Cantidad Total de Políticas a Configurar o Networking o Threat Prevention o URL Filtering o DNS o QoS o VPN Client to Site o Etc., Cantidad de Rutas, Cantidad VPN Site to Site, Cantidad de Redes, Cantidad de Reglas de Nat, Cantidad de Usuarios administradores.

RESPUESTA A CONSULTA 4 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se precisa que se tiene un aproximado de 500 políticas configuradas entre Networking, application Control, Nat, vpn site to site entre otros.

CONSULTA 5 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

De acuerdo con este numeral, es nuestro entendimiento que la entidad solo requiere puertos en cobre RJ45 y no requiere puertos SPF; En caso de que requiera puertos SPF, por favor indicar: Cantidad interfaces SPF y Cantidad interfaces SPF+

RESPUESTA A CONSULTA 5 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que lo requerido son puertos en cobre RJ45, los postores pueden proponer características superiores.

CONSULTA 6 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Agradecemos a la entidad indicar si la transferencia de conocimiento debe ser dictada de forma presencial o remota.

RESPUESTA A CONSULTA 6 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que la transferencia de conocimiento podrá ser realizada de forma presencial o remota considerando los temas especificados en las bases.

CONSULTA 7 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Sírvase confirmar que solo se requiere un único appliance de Management.

RESPUESTA A CONSULTA 7 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que se está solicitando como mínimo un Appliance Management que hará las funciones de administración y recolección en condiciones óptimas.

CONSULTA 8 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Teniendo en cuenta que tradicionalmente los servicios de soporte se enfocan en la resolución de fallas y atención a consultas, por lo tanto, sírvase confirmar que la entidad requiere también de un servicio de administración para aplicación de configuración, casos de uso y mejora continua.

RESPUESTA A CONSULTA 8 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que el soporte técnico que se está solicitando es de configuración, casos de uso y mejora continua de acuerdo a las bases.

CONSULTA 13 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Sírvase confirmar que en la implementación no se debe configurar ningún reporte personalizado, sino que en el informe final de implementación se debe entregar un listado de los reportes por defecto de la solución.

RESPUESTA A CONSULTA 13 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

No se acoge lo solicitado, es necesario para la entidad contar con el reporte personalizado de acuerdo a lo establecido en las bases.

CONSULTA 23 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se solicita a la entidad confirmar si el proceso de SSL o TLS se refiere específicamente al proceso de descifrado.

RESPUESTA A CONSULTA 23 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se confirma que es para el proceso de descifrado al momento de detectar y bloquear virus y malware.

CONSULTA 24 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se solicita a la entidad confirmar, si el término 'prevención' hace referencia a 'bloqueo' de amenazas para el tráfico entrante y saliente.

RESPUESTA A CONSULTA 24 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que el término de "prevención" es equivalente al "bloqueo".

CONSULTA 25 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se solicita a la entidad confirmar si con el término 'Web' hace referencia a 'HTTP'

RESPUESTA A CONSULTA 25 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que el término "Web" hace referencia a los protocolos de http y/o https que utiliza.

CONSULTA 26 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

DICE: Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real.

Consulta: SE SOLICITA A LA ENTIDAD INDICAR SI LO SOLICITADO HACE REFERENCIA QUE SE REQUIERE QUE LOS NGFW BLOQUEEN ARCHIVOS MALICIOSOS.

RESPUESTA A CONSULTA 26 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que el término de "prevenir" es equivalente al "bloqueo"

CONSULTA 27 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se solicita a la entidad confirmar, si el término 'geolocalización' puede referirse también a 'fuente geográfica', debido a que diferentes fabricantes tienen variación en la terminología.

RESPUESTA A CONSULTA 27 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que los fabricantes manejan diferentes terminología, por lo tanto; el término de "geolocalización" es equivalente a "fuente geográfica".

CONSULTA 28 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se solicita a la entidad confirmar, si el término 'C&C' puede referirse también a 'C2', debido a que diferentes fabricantes tienen variación en la terminología.

RESPUESTA A CONSULTA 28 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que los fabricantes manejan diferentes terminología, por lo tanto; se aclara que el término de "C&C" es equivalente a "C2".

CONSULTA 29 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se solicita a la entidad confirmar si el término 'IPS' (Intrusion Prevention System) se refiere específicamente al bloqueo de vulnerabilidades.

RESPUESTA A CONSULTA 29 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se precisa que el IPS (sistema de prevención de intrusos) es bloqueo de vulnerabilidades o protección de vulnerabilidades.

CONSULTA 30 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se solicita a la entidad confirmas si con 'intentos de fuga de datos' pueden referirse hace referencia también como 'exfiltración de datos'.

RESPUESTA A CONSULTA 30 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que los fabricantes manejan diferentes terminologías; por lo tanto; el termino de "intentos de fuga de datos" es equivalente a "exfiltración de datos".

CONSULTA 31 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se solicita a la entidad confirmar si el término 'archivo emulado' hace referencia también como 'muestra analizada'.

RESPUESTA A CONSULTA 31 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que los fabricantes manejan diferentes terminología; por lo tanto; el termino de "archivo emulado" es equivalente a "muestra analizada".

CONSULTA 32 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se solicita a la entidad confirmar si la detección de hypervisor debe aplicarse específicamente al malware y no al sandboxing.

RESPUESTA A CONSULTA 32 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que el malware no debe detectar o evadir al hypervisor del sandboxing, conforme a lo solicitado en las bases.

CONSULTA 33 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se solicita a la entidad confirmar si los problemas de disco duro pueden estar relacionados con el consumo del mismo

RESPUESTA A CONSULTA 33 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que lo solicitado en el numeral 5.1.78 de las bases refiere a las alertas en caso existan problemas de salud en el equipo, la misma que contempla el consumo de disco duro.

CONSULTA 34 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se solicita a la entidad confirmar si se aceptarán soluciones que permitan guardar un backup automático de configuración de todos los cambios que se vayan realizando en los firewall.

RESPUESTA A CONSULTA 34 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que lo que se está solicitando en las bases son características mínimas, los postores pueden proponer características superiores.

CONSULTA 36 DE GRUPO ELECTRODATA S.A.C.

Dice: El proveedor deberá realzar la transferencia de conocimiento al personal de la DINI con respecto a la solución ofertada, incluyendo lo siguiente:

¿Temas: administración, configuración, monitoreo y formulación de reporterías personalizadas, funcionalidades avanzadas, diagnóstico/troubleshooting, backup/restore de las configuraciones.

¿Cantidad: cinco (05) participantes?

¿16 horas como mínimo siempre y cuando se cumpla con los temas solicitados y deben ser desarrollados antes de culminar la implementación de la solución ofertada.

Consulta: Sírvase a confirmar que la transferencia de conocimientos podrá ser brindada de manera remota, lo solicitado se basa en el Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones.

RESPUESTA A CONSULTA 36 DE GRUPO ELECTRODATA S.A.C

Se aclara que la transferencia de conocimiento podrá ser realizada de forma presencial o remota considerando los temas especificados en las bases.

CONSULTA 45 DE JAPAN COMPUTER SERVICE S.A.C.

Pag 24

Numeral 5.1.86

El proveedor deberá realizar la transferencia de conocimiento al personal de la DINI con respecto a la solución ofertada, incluyendo lo siguiente:

¿Temas: administración, configuración, monitoreo y formulación de reporterías personalizadas, funcionalidades avanzadas, diagnóstico/troubleshooting, backup/restore de las configuraciones.

¿Cantidad: cinco (05) participantes.

¿16 horas como mínimo siempre y cuando se cumpla con los temas solicitados y deben ser desarrollados antes de culminar la implementación de la solución ofertada.

Consulta:

En aras de brindar flexibilidad de horarios al personal de la entidad para la transferencia de conocimientos en mención, sírvase confirmar que el presente servicio podrá darse de forma remota."

RESPUESTA A CONSULTA 45 DE JAPAN COMPUTER SERVICE S.A.C.

Se aclara que la transferencia de conocimiento podrá ser realizada de forma presencial o remota considerando los temas especificados en las bases.

CONSULTA 48 DE THINK NETWORKS PERU S.A.C.

Dice:

El hardware ofertado deberá ser totalmente nuevo.

Consulta:

De acuerdo con lo solicitado, no es posible proporcionar sustento mediante documentación o información de dominio público.

Por lo tanto, se solicita a la entidad aceptar la sustentación de este a través de una declaración jurada del postor o carta del mayorista.

RESPUESTA A CONSULTA 48 DE THINK NETWORKS PERU S.A.C.

Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases.

CONSULTA 49 DE THINK NETWORKS PERU S.A.C.

Dice:

El sistema operativo deberá ser del fabricante de la solución ofertada, el mismo deberá venir de fábrica con el ¿hardening ¿necesario, el fabricante deberá desarrollar las actualizaciones de sistema operativo, parches del software o módulos utilizados por la solución ofertada.

Consulta:

De acuerdo con lo solicitado, no es posible proporcionar sustento mediante documentación o información de dominio público.

Por lo tanto, se solicita a la entidad aceptar la sustentación de este a través de una declaración jurada del postor o carta del fabricante.

RESPUESTA A CONSULTA 49 DE THINK NETWORKS PERU S.A.C.

Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases.

CONSULTA 50 DE THINK NETWORKS PERU S.A.C.

Dice:

El fabricante de la solución de seguridad debe estar presente en los últimos 8 reportes de Gartner (Magic Quadrant), en el cuadrante de Líderes para Network Enterprise Firewalls.

Consulta/Observación:

Entendemos que los reportes de analistas como Gartner, no suele ser documentación o información de dominio público. Para lograr tener acceso a esta información, se necesita llenar un formulario y realizar un pago.

Dicho lo anterior, se solicita a la entidad confirmar que se aceptarán link o enlaces de páginas web en la cual se valide que el fabricante cumple con lo solicitado, o en su defecto considerarlo como opcional.

RESPUESTA A CONSULTA 50 DE THINK NETWORKS PERU S.A.C.

No se acoge lo solicitado por el postor, ceñirse a lo requerido en las bases.

CONSULTA 51 DE THINK NETWORKS PERU S.A.C.

Dice:

Los sistemas operativos que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas. Esto se aplicará únicamente al Sistema Operativo o firmware que se instalará en la entidad sobre los equipos propuestos por el postor.

Consulta:

Los fabricantes publican regularmente las vulnerabilidades detectadas en las distintas versiones de sus sistemas operativos. Con el objetivo de mantener a los usuarios informados y al día, esta información se actualiza continuamente en una página web pública.

Dicho lo anterior, se solicita confirmar que se podrá presentar el link de la página web donde el fabricante publica las vulnerabilidades sobre las versiones de sus sistemas operativos, con una impresión de esta, caso contrario se podrá sustentar mediante carta de fabricante o declaración jurada.

RESPUESTA A CONSULTA 51 DE THINK NETWORKS PERU S.A.C.

Se aclara que bastaría con presentar en el Anexo N° 12 un sustento con un documento impreso de la pagina web considerando que las vulnerabilidades(CVE) son de información publica .

CONSULTA 52 DE THINK NETWORKS PERU S.A.C.

Dice:

El sistema debe estar habilitado y configurado con las políticas de todas las funcionalidades:

- ¿ Firewall.
- ¿ Control de aplicaciones.
- ¿ Sistema de Prevención de Intrusos (IPS).
- ¿ Antivirus o Antimalware.
- ¿ Emulación de amenazas (Sandbox).
- ¿ Filtrado de comando y control, antibot o antispymware.-
- ¿ DNS Security.

Que permita detectar y bloquear (prevenir) virus y malware que se propaguen, al menos, en los siguientes protocolos: HTTP, FTP, SMB, SMTP, IMAP, POP3 y SSL o TLS, que cubran finalmente el objetivo requerido.

Consulta:

Se solicita a la entidad confirmar si al referirse a SSL o TLS hace referencia al proceso de descifrado que realiza el firewall para tener visibilidad del tráfico cifrado.

RESPUESTA A CONSULTA 52 DE THINK NETWORKS PERU S.A.C.

Se confirma que es para el proceso de descifrado al momento de detectar y bloquear virus y malware.

CONSULTA 53 DE THINK NETWORKS PERU S.A.C.

Dice:

El proveedor deberá considerar en la implementación los servicios de Networking necesario para la implementación (configuración del core, Switches, reglas en firewall perimetral e interno y aplicación de buenas prácticas para la convivencia de la red externa con la interna).

Consulta:

Debido que el requerimiento no hace referencia a ninguna tecnología de parte del fabricante, no se podría sustentar con documentación pública el requerimiento.

Dicho lo anterior, se solicita a la entidad que se pueda sustentar el requerimiento con una declaración jurada del postor.

RESPUESTA A CONSULTA 53 DE THINK NETWORKS PERU S.A.C.

Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases.

CONSULTA 55 DE THINK NETWORKS PERU S.A.C.

Dice:

Cada equipo deberá contar con dos fuentes de poder de 100-240 VAC 50-60 Hz.

Consulta:

Se solicita a la entidad que se pueda acompañar al documento de sustento la lista de materiales para referenciar que se cuenta con dos fuentes poder, con la finalidad de reforzar el sustento de lo requerido.

RESPUESTA A CONSULTA 55 DE THINK NETWORKS PERU S.A.C.

Se aclara que el postor en caso considere conveniente podría adicionalmente indicar el numero de parte o similar con la ficha técnica o documentación que la sustenta.

CONSULTA 56 DE THINK NETWORKS PERU S.A.C.

Dice:

Las fuentes de poder podrían ser de tipo hot-swap (cambio en caliente)

Consulta:

Se solicita a la entidad aclarar que al referirse a hot-swap (cambio en caliente) hace referencia a que se realizará el remplazo de una fuente poder sin generar una interrupción de servicio.

RESPUESTA A CONSULTA 56 DE THINK NETWORKS PERU S.A.C.

Se aclara que las fuentes de poder de tipo hot-swap (cambio en caliente) son opcionales.

CONSULTA 57 DE THINK NETWORKS PERU S.A.C.

Dice:

Cada equipo deberá tener como mínimo 8 interfaces de cobre GE RJ45.

Consulta:

Se solicita a la entidad confirmar que se aceptarán los términos interfaces de cobre GE o puertos RJ45.

RESPUESTA A CONSULTA 57 DE THINK NETWORKS PERU S.A.C.

Se aclara que lo que los términos de "cobre GE o puertos RJ45" es equivalente al "GE RJ45"

CONSULTA 58 DE THINK NETWORKS PERU S.A.C.

Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en tiempo real en el repositorio la clasificación y/o reputación de direcciones IP y/o Dominios y/o URL y/o redes de C2 o Comando y Control, y/o ataques DoS.

Consulta:

Con la finalidad de brindar el mejor sustento técnico para el entendimiento de la entidad, se solicita a la entidad confirmar si se aceptarán términos similares como:

Repositorio de inteligencia de amenazas en nube del propio fabricante o servicio en nube de prevención avanzada de amenazas.

RESPUESTA A CONSULTA 58 DE THINK NETWORKS PERU S.A.C.

Se aclara que lo solicitado es equivalente al repositorio de inteligencia de amenazas en nube, tener en cuenta que debe ser del propio fabricante.

CONSULTA 59 DE THINK NETWORKS PERU S.A.C.

Dice:

La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.

Consulta:

Se solicita a la entidad confirmar, que se aceptarán los términos de entrante y saliente o carga y descarga.

RESPUESTA A CONSULTA 59 DE THINK NETWORKS PERU S.A.C.

Se aclara que el termino de "entrante y saliente" es equivalente al "carga y descarga"

CONSULTA 60 DE THINK NETWORKS PERU S.A.C.

Dice:

Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web, Mail (SMTP o POP3), SMB, FTP y SSL o TLS

Consulta:

Debido que web no es un protocolo, la entidad estaría generando una confusión con lo requerido, con la finalidad de brindar el mejor sustento posible, se solicita a la entidad aclarar que, al indicar Web, hace referencia a los protocolos HTTP y/o HTTPS.

RESPUESTA A CONSULTA 60 DE THINK NETWORKS PERU S.A.C.

Se aclara que el termino "Web" hace referencia a los protocolos de http y/o https que utiliza.

CONSULTA 61 DE THINK NETWORKS PERU S.A.C.

Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real.

Consulta:

Las soluciones de Next Generation Firewall o Firewall, no realizan la prevención de la infección de archivos, lo que hace esta es bloquear el tráfico de archivos maliciosos.

Dicho lo anterior, se solicita a la entidad aclarar si se requiere que la solución brinde bloqueo de archivos maliciosos como (Word, Excel, PowerPoint, PDF) en tiempo real.

RESPUESTA A CONSULTA 61 DE THINK NETWORKS PERU S.A.C.

Se aclara que el termino de "prevenir" es equivalente al "bloqueo"

CONSULTA 62 DE THINK NETWORKS PERU S.A.C.

Dice:

La identificación de amenazas avanzadas camufladas en tráfico DNS deberá contar con mecanismos avanzados de detección con el objetivo de identificar ataques imposibles de mitigar con firmas y/o reputación del dominio. Para ello se requiere que el tráfico DNS sea analizado con técnicas de inteligencia artificial y/o análisis predictivo y/o machine learning en tiempo real.

Consulta:

Se solicita a la entidad confirmar que se aceptarán fabricantes que cuenten con identificación de amenazas avanzadas camufladas en tráfico DNS que deberá contar con mecanismos avanzados y/o múltiples fuentes de detección con el objetivo de identificar ataques imposibles de mitigar con firmas y/o reputación del dominio. Para ello se requiere que el tráfico DNS sea analizado con técnicas de inteligencia artificial y/o análisis predictivo y/o machine learning en tiempo real.

RESPUESTA A CONSULTA 62 DE THINK NETWORKS PERU S.A.C.

Se aclara que lo que se está solicitando en las bases son características mínimas, los postores pueden proponer características superiores.

CONSULTA 63 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe soportar Inspección de tráfico cifrado/encryptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).

Consulta:

Debido que se comprende que HTTPS es el protocolo utilizado para la navegación web, se solicita a la entidad confirmar que se aceptarán soluciones que soporten inspección de tráfico cifrado/encryptado sobre protocolo HTTPS o web o servidor web, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).

RESPUESTA A CONSULTA 63 DE THINK NETWORKS PERU S.A.C.

Se aclara que lo que se está solicitando en las bases son características mínimas, los postores pueden proponer características superiores.

CONSULTA 64 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware.

Consulta:

Entendemos que lo solicitado, se refiere a el bloqueo de sitios web categorizado y/o identificados como malware.

Dicho lo anterior, se solicita a la entidad confirmar que el punto hace referencia al bloqueo de sitios web categorizados como malware permitiendo mitigar el riesgo asociado a estos sitios.

RESPUESTA A CONSULTA 64 DE THINK NETWORKS PERU S.A.C.

Se aclara que el termino de "bloqueo de sitios web categorizados" es equivalente al punto 5.1.30

CONSULTA 65 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe tener capacidad de integración con fuente de IoC de terceros (External IoC) a través de direcciones web URL, con capacidades de detección y prevención o listas dinámicas externa, siempre y cuando se cumpla con el requerimiento solicitado. La aplicación y prevención de seguridad, en base a los IoC o listas dinámicas externa incluidos, debe ser de manera automática, sin interacción del usuario administrador una vez aplicada a una política de seguridad.

Consulta:

De acuerdo con lo solicitado, no es posible proporcionar sustento mediante documentación o información de dominio público.

Por lo tanto, se solicita a la entidad aceptar la sustentación de este a través de una declaración jurada del postor o carta del mayorista.

RESPUESTA A CONSULTA 65 DE THINK NETWORKS PERU S.A.C.

No se acoge, deberá ceñirse a lo indicado en las bases, esta característica de seguridad debe tener el sustento técnico.

CONSULTA 66 DE THINK NETWORKS PERU S.A.C.

Dice:

Los firewalls deben soportar como mínimo 1,024 VLANs tags 802.3ad

Consulta:

Se solicita a la entidad aclarar que el requerimiento consta de que la solución debe soportar mínimo 1,024 VLANs tags y 802.3ad, debido que son dos temas diferentes.

RESPUESTA A CONSULTA 66 DE THINK NETWORKS PERU S.A.C.

Se aclara que lo referido en el numeral 5.1.39 son dos temas diferentes.

CONSULTA 67 DE THINK NETWORKS PERU S.A.C.

Dice:

Soportar la creación de políticas basadas en Geolocalización, configurando que el tráfico de determinado País y/o Países sean bloqueados o permitidos.

Consulta:

Con la finalidad de brindar el mejor sustento posible, se solicita a la entidad confirmar que se aceptarán los términos de geolocalización o fuente geográfica.

RESPUESTA A CONSULTA 67 DE THINK NETWORKS PERU S.A.C.

Se entiende que los fabricantes manejan diferentes terminología. Por lo tanto; se aclara que el termino de "geolocalización" es equivalente a "fuente geográfica".

CONSULTA 68 DE THINK NETWORKS PERU S.A.C.

Dice:

Las actualizaciones de las direcciones o rangos de IP publica por cada país, debe realizarse periódicamente y de manera automática.

Consulta:

Debido que no se cuenta con documentación pública la cual indique lo requerido, se solicita a la entidad confirmar que se aceptará como sustento una carta de fabricante o declaración jurada del postor para este requerimiento.

RESPUESTA A CONSULTA 68 DE THINK NETWORKS PERU S.A.C.

Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases.

CONSULTA 69 DE THINK NETWORKS PERU S.A.C.

Dice:

A nivel de aplicación, debe incluir protecciones tipo Cross Site Scripting y/o SQL Injection y/o Command Injection e injection protecction para DN (Distinguished Names) y/o C&C desconocidos.

Consulta:

Con la finalidad de no generar confusiones a la entidad con la terminología propuesta por cada fabricante, se solicita a la entidad confirmar que se aceptarán los términos C&C o C2 desconocidos.

RESPUESTA A CONSULTA 69 DE THINK NETWORKS PERU S.A.C.

Se entiende que los fabricantes manejan diferentes terminologías. Por lo tanto; se aclara que el termino de "C&C" es equivalente a "C2 desconocidos".

CONSULTA 70 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos.

Consulta:

Se solicita a la entidad confirmar que se aceptarán soluciones que detecten y bloqueen tráfico o url relacionadas a peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos o elude puerto.

RESPUESTA A CONSULTA 70 DE THINK NETWORKS PERU S.A.C.

Se aclara que lo que se está solicitando en las bases son características mínimas, los postores pueden proponer características superiores.

CONSULTA 71 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe permitir adicionar excepciones a las protecciones de IPS

Consulta:

Debido que una excepción de protección de IPS se realizaría básicamente realizando excepciones a ciertas firmas para omitir la protección de estas.

Dicho lo anterior, se solicita a la entidad confirmar que se aceptarán soluciones que permitan adicionar excepciones a las protecciones de IPS o firmas de amenazas.

RESPUESTA A CONSULTA 71 DE THINK NETWORKS PERU S.A.C.

Se aclara que lo señalado por el postor refiere a terminologías equivalentes.

CONSULTA 72 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense.

Consulta:

Con la finalidad de brindar un mejor sustento técnico, no todos los fabricantes cuentan la denominación de IPS para la funcionalidad requerida, en algunos casos se utiliza la denominación protección de vulnerabilidades.

Dicho lo anterior, se solicita a la entidad confirmar que se aceptará soluciones que deban capturar paquetes automáticamente de eventos de IPS o protección de vulnerabilidades para proveer un mejor análisis forense.

RESPUESTA A CONSULTA 72 DE THINK NETWORKS PERU S.A.C.

se aclara que esta característica de seguridad debe tener el sustento técnico, muy independientemente de las terminologías de cada fabricante.

CONSULTA 73 DE THINK NETWORKS PERU S.A.C.

Dice:

Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos o ataques conocidos.

Consulta:

Debido que, para realizar una prevención de una vulnerabilidad, se debe primero detectar esta, caso contrario, no se sabría que prevenir.

Dicho lo anterior, se solicita a la entidad confirmar que se aceptarán soluciones que realicen la prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos o ataques conocidos.

RESPUESTA A CONSULTA 73 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico.

CONSULTA 74 DE THINK NETWORKS PERU S.A.C.

Dice:

Detección y prevención del uso indebido de un protocolo o ataques no basados en protocolos IP, para actividad maliciosa o amenaza potencial.

Consulta:

Se comprende que el término prevención difiere de acciones, las cuales se pueden realizar para cumplir el término de prevención, la acción de bloqueo es una manera de prevenir.

Dicho lo anterior, se solicita a la entidad confirmar si se aceptarán soluciones que cuenten con la capacidad de Detección y prevención o bloqueo del uso indebido de un protocolo o ataques no basados en protocolos IP, para actividad maliciosa o amenaza potencial.

RESPUESTA A CONSULTA 74 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico, teniendo en cuenta que el término "prevención" es equivalente a "bloqueo".

CONSULTA 75 DE THINK NETWORKS PERU S.A.C.

Dice:

Detección y prevención de intentos de tunelización, para intentos de fuga de datos o intentos de eludir otras medidas de seguridad, como el filtrado web.

Consulta:

Se solicita a la entidad confirmar si se aceptarán los términos fuga de datos o exfiltración de datos o robo de datos.

RESPUESTA A CONSULTA 75 DE THINK NETWORKS PERU S.A.C.

Se aclara que los términos o "exfiltración de datos o robo de datos" es equivalente al término "fuga de datos".

CONSULTA 76 DE THINK NETWORKS PERU S.A.C.

Dice:

Cada archivo emulado en el sandbox debe generar un reporte detallado que incluya información forense sobre la actividad maliciosa originada por el archivo.

Consulta:

Se solicita a la entidad confirmar si se aceptarán los términos archivo emulado o muestra analizada siempre y cuando se encuentre en el mismo contexto.

RESPUESTA A CONSULTA 76 DE THINK NETWORKS PERU S.A.C.

Se aclara que los fabricantes manejan diferentes terminologías, por lo tanto, el término de "archivo emulado" es equivalente a "muestra analizada".

CONSULTA 77 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (personalizado y hardenizado), inyección de código a procesos permitidos o análisis de memoria en run time.

Consulta:

El requerimiento hace referencia que el sandboxing debe de detectar hypervisores, se comprende que la detección de hypervisores, no la realiza ninguna solución de sandboxing en el mundo. En su lugar, las soluciones de sandboxing utilizan hypervisores personalizados y hardenizados.

Dicho lo anterior, se solicita a la entidad aclarar si lo solicitado quiere decir que la solución de sandboxing no debe permitir la evasión de malware utilizando un hypervisor (personalizado y hardenizado), inyección de código a procesos permitidos o análisis de memoria en run time.

RESPUESTA A CONSULTA 77 DE THINK NETWORKS PERU S.A.C.

Se aclara que el malware no debe detectar o evadir al hypervisor del sandboxing, conforme a lo solicitado en las bases.

CONSULTA 78 DE THINK NETWORKS PERU S.A.C.

Dice:

La funcionalidad de control de aplicaciones debe tener una detección y reconocimiento de al menos 3,600 aplicaciones distintas, entre ellas: Streaming o Video, P2P, Proxy, redes sociales, Juegos o similares.

Consulta:

Debido que el fabricante constantemente se encuentra realizando actualizaciones a las aplicaciones detectadas, este no indica un número exacto de aplicaciones detectadas.

Con la finalidad de sustentar el requerimiento, se solicita a la entidad que opcionalmente se pueda sustentar lo requerido con una carta del fabricante o el enlace del portal de aplicaciones detectadas y reconocidas por el fabricante.

RESPUESTA A CONSULTA 78 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico.

CONSULTA 79 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.

Consulta:

Debido que no todos los fabricantes cuentan con las mismas categorías, se solicita a la entidad confirmar que se aceptarán soluciones que ofrezcan categorías similares como:

Proxy o Proxy-avoidance-and-anonymizers

Páginas de adultos o adultos.

RESPUESTA A CONSULTA 79 DE THINK NETWORKS PERU S.A.C.

Se precisa que lo consultado son términos equivalentes a lo solicitado, por lo que se aceptará lo indicado.

CONSULTA 80 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y soportar protección al protocolo HTTP/2, esta última deberá habilitarse desde la interfaz web.

Consulta:

Con la finalidad de brindar el mejor sustento técnico, se solicita a la entidad confirmar que se aceptarán el término implementación o uso.

RESPUESTA A CONSULTA 80 DE THINK NETWORKS PERU S.A.C.

Se precisa que lo consultado son términos equivalente a lo solicitado, por lo que se aceptará lo indicado.

CONSULTA 81 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y soportar protección al protocolo HTTP/2, esta última deberá habilitarse desde la interfaz web.

Consulta:

Con la finalidad de brindar el mejor sustento técnico, se solicita a la entidad confirmar que se aceptará que la habilitación desde la interfaz web sea opcional, debido que otros fabricantes lo traen habilitados por default.

RESPUESTA A CONSULTA 81 DE THINK NETWORKS PERU S.A.C.

No se acepta lo solicitado, dado que se requiere que la habilitación sea por una interfaz web para una gestión adecuada.

CONSULTA 82 DE THINK NETWORKS PERU S.A.C.

Dice:

La solución deberá contar con un módulo de descubrimiento, identificación y clasificación de dispositivos como teléfonos IP y/o cámaras de vigilancia y/o consolas de videojuegos y/o impresoras y/o dispositivos médicos y/o equipos industriales y/o equipos de seguridad y/o servidores, entre otros. Este módulo debe contar con capacidades de protección de amenazas a través de las políticas de seguridad.

Consulta:

Debido que no todos los fabricantes cuentan con las mismas formas de trabajo, sin embargo, se cumple con la finalidad requerida.

Se solicita a la entidad confirmar que se aceptarán soluciones que cuenten con capacidades de protección de amenazas a través de políticas de seguridad o recomendaciones de políticas según el comportamiento de la red.

RESPUESTA A CONSULTA 82 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de política de seguridad debe tener el sustento técnico.

CONSULTA 83 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe hacer uso del protocolo SNMP para integrarse a los switches

Consulta:

Debido que no todos los fabricantes cuentan con las mismas formas de trabajo, sin embargo, se cumple con la finalidad requerida.

Se solicita a la entidad confirmar que se aceptarán soluciones que hagan uso del protocolo SNMP para integrarse o consultar a los switches.

RESPUESTA A CONSULTA 83 DE THINK NETWORKS PERU S.A.C.

Se confirma que se aceptarán soluciones que hagan uso del protocolo SNMP para integrarse o consultar a los switches, dado que la función del SNMP es supervisar la infraestructura tecnológica dentro de ello a los switches.

CONSULTA 84 DE THINK NETWORKS PERU S.A.C.

Dice:

Se deberá incluir una herramienta integrada y/o externa que genere alertas si existen problemas de salud del equipo en materia de hardware y software, como mínimo: consumo de memoria, problemas de la alta disponibilidad (HA), problemas de disco duro, , expiración de licencias.

Consulta:

Con la finalidad de brindar un mejor sustento técnico, se solicita a la entidad confirmar que se aceptarán las siguientes alertas similares:

Consumo de memoria: uso de memoria alcanzo umbral crítico

Problema de disco duro: capacidad máxima de disco.

RESPUESTA A CONSULTA 84 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico.

CONSULTA 85 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe estar licenciado para soportar 50 usuarios concurrentes o simultáneos de IPsec o SSL VPN Client-to-Site, con capacidad de VPN para dispositivos Windows, Linux y MAC, y también dispositivos móviles como Android y IOS.

Consulta:

De acuerdo a lo indicado en este punto hace referencia a cantidad de usuarios para la funcionalidad de vpn ssl o vpn ipsec para soportar los diferentes sistemas operativos.

Tener en consideración que, a nivel de cantidades de usuarios concurrentes, no se dispone de información de dominio público, por ende, se solicita a la entidad que la cantidad de usuarios solicitados para esta funcionalidad se pueda sustentar a través de una declaración jurada por parte del postor o carta del fabricante.

RESPUESTA A CONSULTA 85 DE THINK NETWORKS PERU S.A.C.

Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases.

CONSULTA 86 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado en sistema operativo Windows, que permita validar en base al nivel de cumplimiento (compliance) del host permitir, denegar o limitar el acceso a los recursos de la red interna. Por lo menos se deberá poder configurar los siguientes casos de uso siguientes:

- ¿ Software antivirus instalado y habilitado
- ¿ Software antivirus con la base de datos de firmas actualizada
- ¿ Parche de seguridad instalado o dispositivos vulnerables, según su nivel de criticidad
- ¿ Software de DLP instalado, el cual debe ser identificado a través de las llaves de registro o procesos del sistema operativo

Consulta:

Se solicita a la entidad confirmar que se aceptarán los términos como antivirus o antimalware en el punto requerido.

RESPUESTA A CONSULTA 86 DE THINK NETWORKS PERU S.A.C.

Se precisa que lo consultado son términos equivalente a lo solicitado, por lo que se aceptará lo indicado.

CONSULTA 87 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado en sistema operativo Windows, que permita validar en base al nivel de cumplimiento (compliance) del host permitir, denegar o limitar el acceso a los recursos de la red interna. Por lo menos se deberá poder configurar los siguientes casos de uso siguientes:

- ¿ Software antivirus instalado y habilitado
- ¿ Software antivirus con la base de datos de firmas actualizada
- ¿ Parche de seguridad instalado o dispositivos vulnerables, según su nivel de criticidad
- ¿ Software de DLP instalado, el cual debe ser identificado a través de las llaves de registro o procesos del sistema operativo

Consulta:

De acuerdo a lo solicitado en este punto, respecto a la funcionalidad de software de dlp instalado, el cual debe ser identificado a través de las llaves de registro o procesos del sistema operativo. Debido que no se cuenta con información pública disponible que sustente lo requerido, se solicita la ampliación y/o apertura de la siguiente manera:

Sírvase confirmar que aceptarán soluciones que Deban permitir configurar una postura de seguridad del equipo con el cliente VPN instalado en sistema operativo Windows, que permita validar en base al nivel de cumplimiento (compliance) del host permitir, denegar o limitar el acceso a los recursos de la red interna. Por lo menos se deberá poder configurar los siguientes casos de uso siguientes:

- ¿ Software antivirus instalado y habilitado
- ¿ Software antivirus con la base de datos de firmas actualizada
- ¿ Parche de seguridad instalado o dispositivos vulnerables, según su nivel de criticidad
- ¿ Software de DLP instalado.

RESPUESTA A CONSULTA 87 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, no se acepta lo propuesto, este característica de seguridad debe tener el sustento técnico.

CONSULTA 88 DE THINK NETWORKS PERU S.A.C.

Dice:

El proveedor deberá realizar la transferencia de conocimiento al personal de la DINI con respecto a la solución ofertada, incluyendo lo siguiente:

- ¿ Temas: administración, configuración, monitoreo y formulación de reporterías personalizadas, funcionalidades avanzadas, diagnóstico/troubleshooting, backup/restore de las configuraciones.

¿ Cantidad: cinco (05) participantes.

¿ 16 horas como mínimo siempre y cuando se cumpla con los temas solicitados y deben ser desarrollados antes de culminar la implementación de la solución ofertada.

Consulta:

Debido que lo requerido es una transferencia de conocimientos, esta no podrá ser sustentada mediante documentación pública, por lo que se solicita a la entidad confirmar si lo requerido se podrá sustentar mediante una declaración jurada.

RESPUESTA A CONSULTA 88 DE THINK NETWORKS PERU S.A.C.

Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases.

CONSULTA 89 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe permitir accesos concurrentes de al menos dos administradores.

Consulta:

Se solicita a la entidad confirmar que se aceptará el término concurrentes o simultáneos.

RESPUESTA A CONSULTA 89 DE THINK NETWORKS PERU S.A.C.

Se precisa que lo consultado son términos equivalentes a lo solicitado, por lo que se aceptará lo indicado.

CONSULTA 90 DE THINK NETWORKS PERU S.A.C.

Dice:

Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, acceso de lectura o similar, cambio de configuraciones o similar;

Consulta:

Con la finalidad de presentar el mejor sustento técnico para el entendimiento de la entidad, se solicita a la entidad confirmar que se aceptarán términos similares como los siguientes:

Perfiles: roles

Lectura: readonly

RESPUESTA A CONSULTA 90 DE THINK NETWORKS PERU S.A.C.

Se precisa que lo consultado son términos equivalentes a lo solicitado, por lo que se aceptará lo indicado.

CONSULTA 91 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horario.

Consulta:

Con la finalidad de tener claro el requerimiento, se solicita a la entidad confirmar si se aceptarán ofertas que soporten backup/restore o copia de seguridad de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar o programar backups de configuración o copia de seguridad en un determinado día y horario o utilizar un formato de 24horas para programar la exportación.

RESPUESTA A CONSULTA 91 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico.

CONSULTA 94 DE THINK NETWORKS PERU S.A.C.

Dice:

Generar alertas automáticas por Email, SNMP y Syslog

Consulta:

Con la finalidad de brindar una apertura de postores, enviar diferentes fuentes de correo, puede generar confusiones al recibir alertas de diferentes fuentes.

Dicho lo anterior, se solicita a la entidad confirmar que se aceptarán alertas automáticas por Email (SMTP) y/o SNMP y/o Syslog

RESPUESTA A CONSULTA 94 DE THINK NETWORKS PERU S.A.C.

Se aclara que se aceptara Generar alertas automáticas por: Email, Email (SMTP) o SNMP o Syslog.

CONSULTA 95 DE THINK NETWORKS PERU S.A.C.

Dice:

Debe contar con un módulo integrado que monitoree continuamente los firewalls, en base a sus políticas y configuración de buenas prácticas y los compare con base de datos de estándares reconocidos de la industria como mínimo Cobit y/o ISO 27001 y/o NIST 800 53 o mejores prácticas de seguridad, con la finalidad de obtener reportes gráficos detallados informes que demuestren el cumplimiento de los estándares reconocidos de la industria aplicables o mejores prácticas recomendadas.

Consulta:

Entendemos que lo solicitado en este punto va orientado a mejorar la postura de seguridad de los equipos firewalls en la infraestructura de la entidad.

Dicho lo anterior, se solicita a la entidad confirmar que se aceptarán soluciones que cuenten un módulo integrado que monitoree continuamente los firewalls o evaluación continua de la postura de seguridad en base a las buenas prácticas.

RESPUESTA A CONSULTA 95 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico.

CONSULTA 96 DE THINK NETWORKS PERU S.A.C.

Dice:

Debido a que diariamente se crean decenas de miles de nuevas páginas web, la solución deberá ser capaz de analizar en tiempo real si la página web tiene contenido malicioso cuando un usuario intenta acceder.

Consulta:

Tal como se solicita el requerimiento de forma literal, no es posible sustentar con información de dominio público.

Dicho lo anterior, se solicita a la entidad confirmar que se aceptarán declaración jurada o carta de fabricante para la sustentación de dicho punto.

RESPUESTA A CONSULTA 96 DE THINK NETWORKS PERU S.A.C.

Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases.

CONSULTA 97 DE THINK NETWORKS PERU S.A.C.

Dice:

Para tráfico cifrado SSL debe ser capaz de inspeccionar tráfico cifrado en TLS 1.3 y debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.

Consulta:

Se comprende que al referirse a inspeccionar tráfico cifrado en TLS 1.3 y debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante, hace referencia que se debe obtener visibilidad completa y prevenir amenazas conocidas y desconocidas en el tráfico TLSv 1.3

RESPUESTA A CONSULTA 97 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, se está solicitando funcionalidades básicas y el postor puede proponer adicionalmente funcionalidades superiores

CONSULTA 98 DE THINK NETWORKS PERU S.A.C.

Dice:

Se debe proporcionar acceso a la base de datos de inteligencia de amenazas del fabricante, el cual debe permitir hacer consultas de Hashes, Dominios y Direcciones IP, para mostrar información sobre la amenaza, a nivel de clasificación, reputación, familia de malware, comportamiento.

Consulta:

Debido que se requiere que la solución tenga acceso a una base de datos de inteligencia y se detalle las consultas que se logra obtener de este, no es posible sustentar este requerimiento con documentación de dominio público.

Dicho lo anterior, se solicita a la entidad confirmar que sea aceptará que el sustento sea mediante una declaración jurada del postor o una carta del fabricante.

RESPUESTA A CONSULTA 98 DE THINK NETWORKS PERU S.A.C.

Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases.

CONSULTA 99 DE THINK NETWORKS PERU S.A.C.

Dice:

El IPS debe contar con mecanismo de detección de amenazas de múltiples niveles o métodos: detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías, detección basada en comportamiento.

Consulta:

Se solicita a la entidad confirmar que al menos se aceptarán soluciones que cuenten con el módulo de IPS o protección de vulnerabilidades el cual cuente con mecanismos de detección de amenazas de múltiples niveles o métodos o capas: detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías o características anómalas en la red, detección basada en comportamiento o comportamiento malicioso.

RESPUESTA A CONSULTA 99 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, esta característica de seguridad debe tener el sustento técnico.

CONSULTA 100 DE THINK NETWORKS PERU S.A.C.

Dice:

Las firmas de protección de IPS deben poder categorizarse según un nivel de severidad, nivel de efectividad (confianza) o explotación cloud en línea o exploit-kit y nivel consumo de recursos o fuerza bruta.

Consulta:

Debido que el texto literal indica que las firmas se deban de categorizar de más de 4 formas, impide la participación y sustento técnico del requerimiento.

Dicho lo anterior, se solicita a la entidad confirmar que al menos se aceptarán soluciones que los módulos de IPS o protección de vulnerabilidades categoricen las firmas de protección según el nivel de severidad y/o nivel de efectividad (confianza) y/o explotación cloud en línea y/o exploit-kit y/o nivel consumo de recursos o fuerza bruta.

RESPUESTA A CONSULTA 100 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, esta característica de seguridad debe tener el sustento técnico.

CONSULTA 101 DE THINK NETWORKS PERU S.A.C.

Dice:

La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de URL y recursos DNS no identificados y/o no clasificados al momento de ser registrado.

Consulta:

La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de URL o sitio web y recursos DNS o dominos no identificados y/o no clasificados al momento de ser registrado.

RESPUESTA A CONSULTA 101 DE THINK NETWORKS PERU S.A.C.

Se precisa que lo consultado son términos equivalentes a lo solicitado, por lo que se aceptará lo indicado.

CONSULTA 102 DE THINK NETWORKS PERU S.A.C.

Dice:

La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA), empleando protección basada en Machine Learning, así como protección fuga o exfiltración de información mediante DNS Tunneling, en tiempo real

Consulta:

Debido lo requerido en este punto, no es posible sustentar con documentación de dominio público, se solicita a la entidad que al menos se considere lo siguiente con la finalidad de ampliar la participación de psotores:

La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA) o identificación y bloqueo de amenazas basadas en DGA, empleando protección o técnicas basada en Machine Learning o ML, así como protección fuga o exfiltración de información o datos mediante DNS Tunneling, en tiempo real

RESPUESTA A CONSULTA 102 DE THINK NETWORKS PERU S.A.C.

Se precisa que lo consultado son términos equivalentes a lo solicitado, por lo que se aceptará lo indicado.

CONSULTA 103 DE THINK NETWORKS PERU S.A.C.

Dice:

La solución debe contar con análisis la reputación de direcciones URL y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).

Consulta:

Debido lo requerido en este punto, no es posible sustentar con documentación de dominio público, se solicita a la entidad que al menos se considere lo siguiente con la finalidad de ampliar la participación de postores:

Dicho lo anterior, sirvase confirmar, que aceptarán soluciones que al menos cuenten con análisis la reputación y/o contenido de direcciones URL o web y los dominios externos (DNS) o categorías DNS a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).

RESPUESTA A CONSULTA 103 DE THINK NETWORKS PERU S.A.C.

Se precisa que lo consultado son términos equivalentes a lo solicitado, por lo que se aceptará.

CONSULTA 105 DE IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.

Dice: "Altura maxima 01 RU, con sus respectivos rieles telescopicos para montaje en gabinete 19".

Consulta:

Considerando que los fabricantes proporcionan los accesorios adecuados para el montaje de sus equipos, se solicita a la Entidad que se considerará que los equipos ofertados cuenten con sus respectivos rieles telescopicos y/o sus soportes de montaje para su instalación en gabinete 19"

RESPUESTA A CONSULTA 105 DE IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.

Se aclara que el postor debe de considerar los accesorios necesarios para el montaje de los equipos Firewall de acuerdo a los solicitado en el punto 5.1.4

CONSULTA 106 DE IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.

Dice: "El proveedor deberá considerar en la implementación los servicios de Networking necesario para la implementación (configuración del core, Switches, reglas en firewall perimetral e interno y aplicación de buenas prácticas para la convivencia de la red externa con la interna)."

Consulta:

Considerando que se requiere que los servicios de implementación incluyan la configuración de equipos terceros a los ofertados por el postor, se solicita a la Entidad confirmar la cantidad de equipos a intervenir, las marcas, la vigencia del soporte del fabricante de los equipos a intervenir, los accesos y permisos de configuración a los equipos. Así mismo, confirmar que las configuraciones estarán limitadas a los alcances de capacidad y licenciamiento de los equipos de la Entidad.

RESPUESTA A CONSULTA 106 DE IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.

Se aclara que el servicio de Networking es la misma solución y no en otro equipamiento, para que fluya el trafico en los diferentes equipos de la red (Core, Switches, firewall interno) para la convivencia de la red externa con la interna.

5.2. Impacto ambiental

El proveedor deberá cumplir con la implementación de las medidas de ecoeficiencia institucionales, en cumplimiento con el Decreto Supremo N° 016-2021-MINAM.

5.3. Condiciones de operación

El bien ofertado debe operar los 24x7x365 por el periodo del contrato.

5.4. Modalidad de ejecución

Los bienes/servicios ofertados deberán ser entregados bajo la modalidad "A TODO COSTO" en la modalidad "LLAVE EN MANO", garantizándose compatibilidad, integración, interoperabilidad y funcionalidad entre los mismos, es decir, que todos los elementos necesarios para que los bienes/servicios ofertados funcionen correctamente y para que provean los servicios requeridos, deberán incluirse, aunque no hayan sido especificados.

5.5. Garantía comercial

La garantía de la solución debe tener vigencia desde el día siguiente de la entrega total de la solución ofertada, implementada y operando a un 100% con todas sus funcionalidades habilitadas por un periodo mínimo de 36 meses.

5.6. Prestaciones accesorias a la prestación principal

5.6.1. Soporte Técnico

Ítem	Descripción
5.6.1.1	Soporte Vía Web y Telefónico 24x7x365 por el periodo del contrato por parte del contratista.
5.6.1.2	Soporte remoto para casos especializados y específicos que el área técnica lo amerite.
5.6.1.3	Soporte Local (en sitio) para la atención de los problemas de mal funcionamiento de la solución será de 24x7x365 por el personal capacitado en la solución durante el periodo del contrato.
5.6.1.4	En caso el personal propuesto indicado para realizar el servicio de soporte técnico no se encuentre disponible, el contratista debe comunicar a la Oficina de Administración – Logística, con la debida anticipación, la nueva asignación del personal. Quien debe tener el mismo perfil que el propuesto inicialmente.
5.6.1.5	El soporte técnico debe incluir la actualización y configuración de nuevas versiones liberadas por el fabricante, así como configuraciones, casos de uso, y mejora continua del sistema en base a buenas prácticas del fabricante, durante la vigencia del contrato. En caso se cuente con incidentes como consecuencia de realizar actualizaciones, upgrades o averías de software al momento del soporte técnico de la solución ofertada, el contratista tendrá un plazo máximo de dos (2) horas para la restauración de la información del servicio relacionado solo a la solución propuesta y no a la plataforma de correo o la información contenida en esta, la misma que se registrará en la hoja de visita técnica del contratista o correo electrónico.
5.6.1.6	Cada vez que ocurra una avería y finaliza la atención de la misma, a satisfacción de la DINI, el contratista debe entregar un reporte detallado en documento físico o electrónico indicando las causas de la avería, diagnósticos, solución y tiempos empleados, el cual debe ser remitido en un plazo no mayor de tres días (03 días) calendario.
5.6.1.7	El tiempo máximo para la atención de incidentes será de 3 horas y para resolver la avería será de 3 horas posteriores como máximo, será contabilizado desde que el contratista tome conocimiento del incidente reportado (Interrupción del servicio y demora en la restauración de la información del servicio). Este tiempo no aplicará para los casos que sea necesario cambio de partes que impliquen mayor tiempo de reposición física de la pieza o repuesto afectado.
5.6.1.8	En los meses que no se cuente con atención por solicitudes de soporte técnico, el contratista debe brindar una charla de temas asociados a la plataforma acerca del uso y buenas prácticas de la solución de al menos dos (02) horas, la misma que debe figurar en el informe de soporte técnico anual. La coordinación para la realización de la charla técnica se realizará luego de finalizado cada mes de servicio. La charla podrá realizarse de forma remota previa coordinación y aprobación del área técnica de la institución.

Ítem	Descripción
5.6.1.9	El contratista debe entregar un informe de soporte técnico al término del servicio de soporte anual en el cual se indiquen los tickets de atención generados, el detalle de cada solicitud, soporte y detalle de charlas de ser el caso.

CONSULTA 21 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Dice:

¿Soporte remoto para casos especializados y específicos que el área técnica lo amerite

Dado que el Principio de Transparencia, contempla el derecho a la información en la compra pública, el cual tiene esencialmente por objeto garantizar que no exista riesgo de favoritismo y arbitrariedad por parte de la Entidad convocante; para lo cual, 8 se exige que todas las condiciones del procedimiento estén formuladas de forma clara, precisa e inequívoca en las Bases o en las respuestas brindadas en el pliego absolutorio, con el fin de que todos los postores razonablemente informados y normalmente diligentes puedan comprender su alcance exacto e interpretarlas de la misma forma. Dicho esto; se solicita al Comité Especial, que con motivo de la integración de bases se especifique y acote las actividades que se deberán considerar dentro del soporte remoto para los denominados ¿casos especializados y específicos.

RESPUESTA A CONSULTA 21 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que los casos especializados son los que el fabricante atienda; por lo tanto, se dará el acceso remoto.

CONSULTA 22 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Dice:

¿En los meses que no se cuente con atención por solicitudes de soporte técnico, el contratista debe brindar una charla de temas asociados a la plataforma acerca del uso y buenas prácticas de la solución de al menos dos (02) horas ¿

Dado que, el Principio de Transparencia consignado en el literal c) del artículo 2 de la Ley establece que la Entidad debe proporcionar información clara y coherente con el fin que esta sea comprendida por todos los potenciales proveedores; se solicita al Comité Especial, que con motivo de la integración de bases se el número de personas que participaran en la charla de temas asociados a la plataforma acerca del usos y buenas prácticas e la solución y que esta charla solo se brindará dentro del horario laboral de la entidad.

RESPUESTA A CONSULTA 22 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que la charla de 2 horas debe ser dentro del horario laboral en coordinación y aprobación del área técnica. Con respecto al numero de personas que participaran en la charla, será como mínimo un (1) personal del área técnica.

CONSULTA 37 DE GRUPO ELECTRODATA S.A.C.

Dice: El soporte técnico debe incluir la actualización y configuración de nuevas versiones liberadas por el fabricante, así como configuraciones, casos de uso, y mejora continua del sistema en base a buenas prácticas del fabricante, durante la vigencia del contrato.

En caso se cuente con incidentes como consecuencia de realizar actualizaciones, upgrades o averías de software al momento del soporte técnico de la solución ofertada, el contratista tendrá un plazo máximo de dos (2) horas para la restauración de la información del servicio relacionado solo a la solución propuesta y no a la plataforma de correo o la información contenida en esta, la misma que se registrará en la hoja de visita técnica del contratista o correo electrónico.

Consulta: Sírvase a confirmar, que el plazo no aplicará en caso el incidente requiera ser escalado con el fabricante, ya que su Centro de atención técnica cuenta con un SLA de atención mas no de resolución, lo solicitado se basa en el Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones.

RESPUESTA A CONSULTA 37 DE GRUPO ELECTRODATA S.A.C

Se aclara que el incidente debe ser atendido en los tiempos solicitados; sin embargo, en caso el incidente sea escalado con el fabricante y no cuenten con una resolución el contratista deberá proporcionar el ticket de escalamiento para realizar el seguimiento respectivo.

CONSULTA 38 DE GRUPO ELECTRODATA S.A.C.

Dice: El tiempo máximo para la atención de incidentes será de 3 horas y para resolver la avería será de 3 horas posteriores como máximo, será contabilizado desde que el contratista tome conocimiento del incidente reportado (Interrupción del servicio y demora en la restauración de la información del servicio). Este tiempo no aplicará para los casos que sea necesario cambio de partes que impliquen mayor tiempo de reposición física de la pieza o repuesto afectado.

Consulta: Sírvase a confirmar, que el plazo no aplicará en caso el incidente requiera ser escalado con el fabricante, ya que su Centro de atención técnica cuenta con un SLA de atención mas no de resolución, lo solicitado se basa en el Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones.

RESPUESTA A CONSULTA 38 DE GRUPO ELECTRODATA S.A.C

Se aclara que el incidente debe ser atendido en los tiempos solicitados; sin embargo, en caso el incidente sea escalado con el fabricante y no cuenten con una resolución el contratista deberá proporcionar el ticket de escalamiento para realizar el seguimiento respectivo.

CONSULTA 42 DE GRUPO ELECTRODATA S.A.C.

Dice: Por interrupción del servicio por averías en la solución mayor a tres (03) horas
Se considera como consecuencia de un incidente que afecta la operatividad de la solución afectando a los usuarios que lo utilizan. Se considera desde la notificación al Contratista por parte del área usuaria posteriores a las solicitudes de soporte técnico mayor a 3 horas para la atención
Procedimiento:

¿El área usuaria detecta interrupción del servicio y solicita atención al contratista a través de llamada telefónica o correo electrónico a su centro de atención u otros correos que proporcione el Contratista
¿En caso de pasado tres (03) horas continuas con la interrupción del servicio, se informará al área de Logística para la aplicación de la penalidad correspondiente.

Consulta: Sírvase a confirmar que el plazo no aplicará en caso el incidente requiera ser escalado con el fabricante, ya que su Centro de atención técnica cuenta con un SLA de atención mas no de resolución, lo solicitado se basa en el Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones.

RESPUESTA A CONSULTA 42 DE GRUPO ELECTRODATA S.A.C

Se aclara que las averías debe ser atendido en los tiempos solicitados; sin embargo, en caso la avería sea escalado con el fabricante y no cuenten con una resolución el contratista deberá proporcionar el ticket de escalamiento para realizar el seguimiento respectivo.

CONSULTA 43 DE GRUPO ELECTRODATA S.A.C.

Dice: Por problemas en la restauración de la información del servicio mayor a dos (02) horas
Se aplicará como consecuencia de realizar actualizaciones, upgrades o averías de software al momento del soporte técnico de la solución ofertada.
Procedimiento:
¿ El área usuaria determina que la solución no cuenta con la configuración que permita el correcto funcionamiento del mismo.

¿ El área usuaria comunica el incidente al contratista, quien se encuentra realizando actividades sobre la solución, a partir de este momento se contabiliza el tiempo.

En caso de que el contratista no pueda resolver el incidente dentro del plazo de dos (02) horas, se registrará la observación en la hoja de visita técnica del contratista o correo electrónico y se informará al área de Logística para la aplicación de la penalidad correspondiente

Consulta: Sirvase a confirmar, que el plazo no aplicará en caso el incidente requiera ser escalado con el fabricante, ya que su Centro de atención técnica cuenta con un SLA de atención mas no de resolución, lo solicitado se basa en el Art. 2 de la Ley de Contrataciones del Estado, de conformidad con el literal a) Principio de Libre Concurrencia, literal b) Principio de Igualdad de Trato.; como también Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones.

RESPUESTA A CONSULTA 43 DE GRUPO ELECTRODATA S.A.C

Se aclara que los problemas en la restauración de la información debe ser atendido en los tiempos solicitados; sin embargo, en caso el incidente sea escalado con el fabricante y no cuenten con una resolución el contratista deberá proporcionar el ticket de escalamiento para realizar el seguimiento respectivo.

OBSERVACION 46 DE JAPAN COMPUTER SERVICE S.A.C.

Numeral 5.6.1.7.

Dice:

El tiempo máximo para la solución de incidentes será de 3 horas y para resolver la avería será de 3 horas posteriores como máximo, será contabilizado desde que el contratista tome conocimiento del incidente reportado (Interrupción del servicio y demora en la restauración de la información del servicio). Este tiempo no aplicará para los casos que sea necesario cambio de partes que impliquen mayor tiempo de reposición física de la pieza o repuesto afectado.

Observación:

Si bien el contratista se compromete a ir escalando el incidente en nivel de severidad y especialización de personal si la solución del mismo no es favorable, y dado que la solución de un incidente depende mucho de la naturaleza del problema, no existe un tiempo mínimo de resolución que pueda establecerse en el caso que la causa del problema sea por un sistema del cliente independiente a la seguridad perimetral, ello tomando en cuenta que el soporte del fabricante y del contratista sólo cubre la solución de Firewall ofertada".

RESPUESTA A OBSERVACION 46 DE JAPAN COMPUTER SERVICE S.A.C.

Se aclara que el incidente debe ser atendido en los tiempos solicitados; sin embargo, en caso el incidente sea escalado con el fabricante y no cuenten con una resolución el contratista deberá proporcionar el ticket de escalamiento para realizar el seguimiento respectivo.

CONSULTA 54 DE THINK NETWORKS PERU S.A.C.

Dice:

El nivel de soporte del fabricante debe ser 24 x 7 durante el periodo del contrato. Debiendo ser asistido por el propio personal del fabricante a través de su propio centro de atención, y en coordinación directa con el contratista para el seguimiento y escalamiento de los requerimientos.

Consulta:

Debido que no se encuentra sustento de documentación pública donde se indique que el postor debe de tenerse una coordinación con el contratista para el seguimiento y escalamientos de los requerimientos

Dicho lo anterior, se solicita a la entidad que se pueda sustentar con documentación del servicio de soporte del fabricante y una declaración jurada que sustente lo siguiente: ¿Debiendo ser asistido por el propio personal del fabricante a través de su propio centro de atención, y en coordinación directa con el contratista para el seguimiento y escalamiento de los requerimientos?

RESPUESTA A CONSULTA 54 DE THINK NETWORKS PERU S.A.C.

Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases.

5.7. Lugar y plazo de ejecución de la prestación

5.7.1. Prestación Principal

5.7.1.1. Lugar

En la sede de la Dirección Nacional de Inteligencia, sitio en la Av. Edmundo Aguilar Pastor S/N (Ex avenida Las Palmas), en el distrito de Chorrillos.

5.7.1.2. Plazo

El proveedor debe realizar la entrega total de la solución ofertada implementada y operando a un 100% con todas sus funcionalidades habilitadas máximo el 21 de diciembre de 2024.

El periodo de vigencia de la solución ofertada debe ser de treinta y seis (36) meses, el cual empezará a partir del 22 de diciembre de 2024. Las licencias y soporte del fabricante deben estar homologados su inicio y termino de vigencia.

5.7.2. Prestación Accesorias

5.7.2.1. Lugar

En la sede de la Dirección Nacional de Inteligencia, sitio en la Av. Edmundo Aguilar Pastor S/N (Ex avenida Las Palmas), en el distrito de Chorrillos.

5.7.2.2. Plazo

Del Soporte Técnico: La ejecución de la prestación del servicio será durante el periodo de treinta y seis (36) meses; el cual se contabilizará a partir del 22 de diciembre de 2024.

6. Requisitos y recursos del proveedor

6.1. Requisitos del proveedor

Ítem	Descripción
6.1.1.	El proveedor deberá ser distribuidor o representante autorizado de la marca, para la distribución y soporte de la solución ofertada, se sustentará con una Declaración Jurada.
	Jefe de Proyecto: El proveedor debe contar con uno (01) líder del proyecto para la implementación y este debe ser ingeniero titulado de Sistemas, electrónico, telecomunicaciones o afines con certificación PMP vigente u otro similar de reconocimiento internacional y con 03 años de experiencia como Jefe de Proyectos en implementaciones de sistemas de seguridad perimetral o de ciberseguridad.
	Personal Especialista implementador:
	i. Actividades
6.1.2.	Para la prestación Principal: Implementará la solución propuesta, migrará las políticas de todos los módulos del firewall actual (CheckPoint 5800 pudiendo afectar servicios en un horario controlado no mayor a 1 hora por caso de migración) a los nuevos equipos, formulará y firmará el informe respectivo.
	ii. Perfil
	El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas: Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines, quienes debe contar con la certificación en la solución ofertada a nivel profesional o experto o ingeniero o superior brinda por la marca ofertada. Además, deben contar con experiencia mínima de dos (02) años en implementación, migración y soporte de la solución propuesta.

	Personal de Soporte: i. Actividades Para la prestación Accesorio: Brindará el soporte técnico a la solución implementada, emitirá y firmará el informe respectivo. ii. Perfil El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas: Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines, quienes debe contar con la certificación en la solución ofertada a nivel profesional o experto o ingeniero o superior brindada por la marca ofertada. Además, deben contar con experiencia mínima de dos (02) años en soporte de la solución propuesta.
6.1.3.	El proveedor debe contar con un centro de atención de llamadas para la asistencia técnica las 24 horas con el siguiente alcance: <ul style="list-style-type: none">• Niveles de atención y Respuesta• Sistema de control y seguimiento de tickets• Sistema de atención 24 x 7
6.1.4.	El proveedor no debe estar inhabilitado para contratar con el Estado Peruano.
6.1.5.	El personal del contratista debe ser de nacionalidad peruana por nacimiento para cualquier actividad relacionada con el presente proyecto por razones de seguridad nacional.

CONSULTA 16 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Para fomentar una mayor pluralidad de postores, sírvase confirmar que para acreditar el grado académico del jefe de proyecto se aceptará Bachiller.

RESPUESTA A CONSULTA 16 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

No se acoge lo solicitado por el postor, se requiere que el personal clave requerido como Jefe de Proyecto cuente con título profesional.

CONSULTA 17 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

En aras de fomentar una mayor pluralidad de postores, sírvase confirmar que para los perfiles del personal especialista implementador y personal de soporte se pueden aceptar bachiller de electrónica y de ingeniería de software como carreras afines.

RESPUESTA A CONSULTA 17 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que lo solicitado se dentro de las carreras afines.

CONSULTA 18 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

En aras de fomentar una mayor pluralidad de postores, sírvase confirmar que para los perfiles del personal de especialista implementador y personal de soporte se podrá aceptar que un personal pueda desempeñar más de un rol.

RESPUESTA A CONSULTA 18 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se acoge lo indicado por el postor, el personal clave requerido como especialista implementador y soporte técnico podrán ser desempeñados por el mismo personal, siempre y cuando el personal propuesto cumpla con el perfil solicitado y presente la documentación que sustenta el cumplimiento de cada perfil por separado. Se aceptará lo descrito debido a que la implementación y el soporte técnico se dan en momentos diferentes.

CONSULTA 35 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se solicita al comité especial aclarar que las certificaciones del Personal Especialista implementador y Personal de Soporte deberán estar vigentes y no se aceptarán certificaciones con fecha de vencimiento anteriores al proceso y/o certificaciones caducadas.

RESPUESTA A CONSULTA 35 DE PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. – PLATECCS S.A.C.

Se aclara que la certificación de la solución ofertada debe de estar vigente.

CONSULTA 39 DE GRUPO ELECTRODATA S.A.C.

Dice:

Personal Especialista implementador:

i. Actividades

Para la prestación Principal: Implementará la solución propuesta, migrará las políticas de todos los módulos del firewall actual (CheckPoint 5800 pudiendo afectar servicios en un horario controlado no mayor a 1 hora por caso de migración) a los nuevos equipos, formulará y firmará el informe respectivo.

ii. Perfil

El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas: Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines, quienes debe contar con la certificación en la solución ofertada a nivel profesional o experto o ingeniero o superior brinda por la marca ofertada. Además, deben contar con experiencia mínima de dos (02) años en implementación, migración y soporte de la solución propuesta

Consulta: A fin de permitir mayor pluralidad de postores, sírvase a confirmar que se aceptarán como carreras afines las siguientes:

- Bachiller en Ingeniería de Sistemas e Informática
- Bachiller en Computación e Informática
- Bachiller en Ingeniería Electrónica
- Profesional Técnico en Ingeniería de Redes y Comunicaciones. Lo solicitado se basa en el Art. 2 de la Ley de Contrataciones del Estado, de conformidad con el literal a) Principio de Libre Concurrencia, literal b) Principio de Igualdad de Trato.; como también Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones.

RESPUESTA A CONSULTA 39 DE GRUPO ELECTRODATA S.A.C

Se confirma que lo solicitado por el postor se encuentra considerado como carreras afines.

CONSULTA 40 DE GRUPO ELECTRODATA S.A.C.

Dice:

Personal de Soporte:

1. Actividades

Para la prestación Accesorio: Brindará el soporte técnico a la solución implementada. emitirá y firmará el informe respectivo,

ii Perfil

El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas: Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines, quienes debe contar con la certificación en la solución ofertada a nivel profesional o experto o ingeniero o superior brindada por la marca ofertada. Además, deben contar con experiencia mínima de dos (02) años en soporte de la solución propuesta.

Consulta: A fin de permitir mayor pluralidad de postores, sírvase a confirmar que se aceptarán como carreras afines las siguientes:

- Bachiller en Ingeniería de Sistemas e Informática
- Bachiller en Computación e Informática
- Bachiller en Ingeniería Electrónica

- Profesional Técnico en Ingeniería de Redes y Comunicaciones. Lo solicitado se basa en el Art. 2 de la Ley de Contrataciones del Estado, de conformidad con el literal a) Principio de Libre Concurrencia, literal b) Principio de Igualdad de Trato.; como también Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones.

RESPUESTA A CONSULTA 40 DE GRUPO ELECTRODATA S.A.C

Se confirma que lo solicitado por el postor se encuentra considerado como carreras afines.

CONSULTA 41 DE GRUPO ELECTRODATA S.A.C.

Dice:

Personal Especialista implementador:

i. Actividades

Para la prestación Principal; Implementará la solución propuesta, migrará las políticas de todos los módulos del firewall actual (CheckPoint 5800 pudiendo afectar servicios en un horario controlado no mayor a 1 hora por caso de migración) a los nuevos equipos, formulará y firmará el informe respectivo.

ii. Perfil

El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas: Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines, quienes debe contar con la certificación en la solución ofertada a nivel profesional o experto o ingeniero o superior brinda por la marca ofertada. Además, deben contar con experiencia mínima de dos (02) años en implementación, migración y soporte de la solución propuesta

Personal de Soporte:

1. Actividades

Para la prestación Accesorio: Brindará el soporte técnico a la solución implementada. emitirá y firmará el informe respectivo,

ii Perfil

El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas: Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines, quienes debe contar con la certificación en la solución ofertada a nivel profesional o experto o ingeniero o superior brindará por la marca ofertada. Además, deben contar con experiencia mínima de dos (02) años en soporte de la solución propuesta.

Consulta: Sírvase confirmar que, a fin de permitir una mayor pluralidad de postores, se aceptará que el personal especialista implementador sea el mismo que el personal de Soporte, siempre y cuando cumpla con el perfil solicitado. Teniendo en cuenta que la etapa de Soporte Técnico (Prestación Accesorio) es posterior a la etapa de implementación (Prestación Principal), lo solicitado se basa en el Art. 2 de la Ley de Contrataciones del Estado, de conformidad con el literal a) Principio de Libre Concurrencia, literal b) Principio de Igualdad de Trato.; como también Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones.

RESPUESTA A CONSULTA 41 DE GRUPO ELECTRODATA S.A.C

Se acoge lo indicado por el postor, el personal clave requerido como especialista implementador y soporte técnico podrán ser desempeñados por el mismo personal, siempre y cuando el personal propuesto cumpla con el perfil solicitado y presente la documentación que sustenta el cumplimiento de cada perfil por separado. Se aceptará lo descrito debido a que la implementación y el soporte técnico se dan en momentos diferentes.

CONSULTA 47 DE JAPAN COMPUTER SERVICE S.A.C.

EN BASES INDICAN:

PERSONAL DE SOPORTE:

CONSULTA:

Considerando que la implementación y el soporte NO se brindarán en simultáneo, sírvase confirmar que el rol del PERSONAL DE SOPORTE podrá ser cubierto por el rol del ESPECIALISTA

IMPLEMENTADOR, siempre y cuando dicha persona cumpla con las certificaciones y experiencia requerida para ambos perfiles.""

Es decir, se podrá presentar 2 personas que cubran con el rol de Implementador y también el de Soporte, siempre y cuando cumplan con los requisitos de ambos perfiles."

RESPUESTA A CONSULTA 47 DE JAPAN COMPUTER SERVICE S.A.C.

Se acoge lo indicado por el postor, el personal clave requerido como especialista implementador y soporte técnico podrán ser desempeñados por el mismo personal, siempre y cuando el personal propuesto cumpla con el perfil solicitado y presente la documentación que sustenta el cumplimiento de cada perfil por separado. Se aceptará lo descrito debido a que la implementación y el soporte técnico se dan en momentos diferentes.

CONSULTA 92 DE THINK NETWORKS PERU S.A.C.

Dice:

Personal Especialista implementador:

Consulta:

Dado que los flujos de trabajo pueden variar significativamente entre empresas, estamos limitando la participación de postores a aquellos que cuenten con al menos dos implementadores y dos profesionales de soporte. Reconocemos que algunos postores pueden tener un esquema en el que el personal de soporte también se encargue de la implementación. Sin embargo, esta medida busca garantizar una sinergia efectiva entre la implementación y el servicio postventa ofrecido.

Dicho lo anterior, se solicita a la entidad confirmar, que únicamente se requiera 1 personal de soporte y 1 personal de implementación.

RESPUESTA A CONSULTA 92 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, ya que son las condiciones minimas requeridas para el personal propuesto.

CONSULTA 93 DE THINK NETWORKS PERU S.A.C.

Dice:

Personal de Soporte:

Consulta:

Dado que los flujos de trabajo pueden variar significativamente entre empresas, estamos limitando la participación de postores a aquellos que cuenten con al menos dos implementadores y dos profesionales de soporte. Reconocemos que algunos postores pueden tener un esquema en el que el personal de soporte también se encargue de la implementación. Sin embargo, esta medida busca garantizar una sinergia efectiva entre la implementación y el servicio postventa ofrecido.

Dicho lo anterior, se solicita a la entidad confirmar, que únicamente se requiera 1 personal de soporte y 1 personal de implementación.

RESPUESTA A CONSULTA 93 DE THINK NETWORKS PERU S.A.C.

Ceñirse a lo solicitado en las bases, ya que son las condiciones minimas requeridas para el personal propuesto.

CONSULTA 107 DE IMPERIA SOLUCIONES TECNOLOGICASS.A.C.

Personal Especialista implementador:

Dice: " El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas: Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines."

Consulta:

Sírvase a la Entidad confirmar que se considerará las carreras de Ingeniería Electrónica, y/o Ingeniería de Seguridad y Auditoría Informática, y/o Redes y Comunicaciones de Datos, y/o Ingeniería de Telecomunicaciones como afines para el perfil de especialista implementador.

RESPUESTA A CONSULTA 107 DE IMPERIA SOLUCIONES TECNOLOGICASS.A.C.

Se confirma que lo solicitado por el postor se encuentra considerado como carreras afines.

CONSULTA 108 DE IMPERIA SOLUCIONES TECNOLOGICASS.A.C.

Personal de Soporte:

Dice: " El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas: Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines."

Consulta:

Sírvase a la Entidad confirmar que se considerará las carreras de Ingeniería Electrónica, y/o Ingeniería de Seguridad y Auditoría Informática, y/o Redes y Comunicaciones de Datos, y/o Ingeniería de Telecomunicaciones como afines para el perfil de personal de soporte.

RESPUESTA A CONSULTA 108 DE IMPERIA SOLUCIONES TECNOLOGICASS.A.C.

Se confirma que lo solicitado por el postor se encuentra considerado como carreras afines.

7. Otras consideraciones para la ejecución de la prestación

7.1. Otras obligaciones

7.1.1. Otras obligaciones del contratista

Ítem	Descripción	Cumple Sí o No	Observaciones de ser el caso
7.1.1.1	Las ESPECIFICACIONES TECNICAS/TERMINOS DE REFERENCIA de los bienes/servicios ofertados deberán ser iguales o superiores al mínimo requerido, y en cuanto a los tipos de tecnologías, deberán ser equivalentes o superiores.		
7.1.1.2	En las ESPECIFICACIONES TECNICAS/TERMINOS DE REFERENCIA, las palabras "capacidad", "soporte", "contar" y/o similares, significan que el contratista deberá contemplar la provisión, inclusión y/o disponibilidad, de las características a las que se hace alusión, a efecto de cumplir con las ESPECIFICACIONES TÉCNICAS mínimas requeridas.		
7.1.1.3	Indicar en la oferta, el cumplimiento de las especificaciones técnicas mínimas requeridas, lo cual evidenciará en la documentación técnica (indicar el folio específico) del sustento (folletos, instructivos, catálogos o similares de fuentes del fabricante) que demuestre el cumplimiento de las mismas (no direcciones de sitios ni links), así como su descripción detallada en forma resaltada. Pudiendo presentar los documentos en su idioma original junto con su traducción simple al castellano en caso de encontrarse en lengua		

Ítem	Descripción	Cumple Sí o No	Observaciones de ser el caso
	extranjera. Las cartas del fabricante no podrán emplearse para el sustento técnico.		
7.1.1.4	Las garantías y soporte empezarán a partir del día siguiente de la entrega total de la solución ofertada, implementada y operando a un 100% con todas sus funcionalidades habilitadas.		
Documentación a ser provista por el contratista			
7.1.1.5	Plan de Implementación de la solución		
7.1.1.6	Relación de números de contacto y la lista de escalamiento.		
7.1.1.7	Las licencias serán entregadas al correo electrónico of412@ dini. gob. pe		
7.1.1.8	Deberá entrega la arquitectura lógica y arquitectura física debiendo detallar cada conexión, puerto, servicios, dirección IP, conexión, ubicación de rack, toma eléctrica debidamente rotulado cada componente.		
7.1.1.9	Deberá entregar un informe final de la solución en donde se incluya el diagrama de la arquitectura física y lógica de la solución, grafico de vigencia de licenciamiento, configuración final, así como también los manuales de instalación, actualización, despliegue y mantenimiento.		
7.1.1.10	Debe entregar el plan de disaster recovery probado por el área técnica, considerando los procedimientos de respaldos de información de la solución.		
7.1.1.11	Deberá entregar los niveles del servicio del fabricante y el proveedor.		
7.1.1.12	El plan de implementación debe ser entregado a los diez (10) días calendario de la firma del contrato, contabilizados a partir de suscrito el contrato. Los demás entregables deben ser entregados como máximo al día siguiente culminada la implementación.		

CONSULTA 9 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Agradecemos a la entidad indicar cuantas pruebas de disaster recovery y/o High vilability se deben realizar durante la fase de implementación.

RESPUESTA A CONSULTA 9 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se aclara que se debe realizar como mínimo una prueba válida de disaster recovery y/o High vilability una vez implementado la solución a fin de comprobar el funcionamiento.

7.2. Confidencialidad

El contratista, con motivo de la prestación, recibirá de la Dirección Nacional de Inteligencia información de carácter estrictamente confidencial que debe ser utilizada solo para los fines de ejecución, por ello, será obligación del contratista mantener la secrecia y confidencialidad respecto a los datos e información de cualquier clase, que la Dirección Nacional de Inteligencia le proporcione, o bien, a la que tenga acceso, con motivo de la prestación y desarrollo de su ejecución.

Adicionalmente, el contratista está obligado a instruir a sus funcionarios o personal que será parte conformante del recurso humano que ejecutará la prestación respecto a la obligación de mantener total secrecia y confidencialidad.

Como parte de la prestación y en relación a la CONFIDENCIALIDAD el contrato considerara la cláusula y acuerdo de confidencialidad.

7.3. Medidas de control durante la ejecución contractual

Las medidas de control las realizará el área técnica OTIC de acuerdo al plan de implementación de la solución ofertada.

7.4. Conformidad de los bienes

7.4.1. Área que recepcionará y brindará la conformidad

7.4.1.1. Para la prestación principal

La conformidad de la prestación principal será otorgada por la Oficina de Tecnologías de Información y Comunicaciones en su calidad de área usuaria, dentro de los 7 días calendario de la entrega total de la solución ofertada, implementada y operando a un 100% con todas sus funcionalidades habilitadas y de la entrega de la documentación solicitada en el punto 7.1.1.5 al 7.1.1.12.

7.4.1.2. Para las prestaciones accesorias

7.4.1.2.1. Soporte técnico

La conformidad será otorgada por la Oficina de Tecnologías de Información y Comunicaciones – OTIC en su calidad de área usuaria luego de cumplido el periodo anual de servicio de soporte técnico y de la entrega por el postor del informe del soporte solicitado en el numeral 5.6.1 y será emitida dentro de los siete (07) días calendario.

7.4.2. Pruebas de puesta en funcionamiento para la conformidad de los bienes

Una vez concluida la implementación, el área usuaria evaluará los distintos aspectos requeridos y si todo está conforme dentro de los 7 días posteriores a la implementación total de la solución, se procederá con la aceptación de las mismas. Cualquier incumplimiento debe ser asumido por el contratista, a costo cero para la Entidad.

7.5. Forma de pago

7.5.1. Para la prestación principal

La DINI realizará la cancelación de la prestación principal en un único pago y se hará efectiva dentro de los diez (10) días calendario de emitida la respectiva conformidad, siempre que se verifiquen las condiciones establecidas en el contrato.

7.5.2. Para las prestaciones accesorias

7.5.2.1. Soporte técnico

El pago se realizará de forma anual, dentro de los diez (10) días calendario de emitida la respectiva conformidad, siempre que se verifiquen las condiciones establecidas en el contrato.

7.6. Otras penalidades aplicables

7.6.1. Para la prestación principal

En caso de retraso injustificado en el plazo de entrega se aplicará lo establecido en el artículo 162 del Reglamento de la Ley de Contrataciones.

7.6.2. Para las prestaciones accesorias

7.6.2.1. Soporte Técnico

Concepto	Monto
<p>Por demora en la respuesta de solicitudes de soporte técnico mayor a 3 horas</p> <p>Se considera desde la notificación al Contratista por parte del área usuaria y la contestación de la misma.</p> <p>Procedimiento:</p> <ul style="list-style-type: none"> El área usuaria solicita atención al contratista a través de llamada telefónica o correo electrónico a su centro de atención u otros correos que proporcione el Contratista. En caso de pasado tres (03) horas y no tener respuesta del contratista, se informará a la unidad orgánica de Logística para la aplicación de la penalidad correspondiente. 	0.1 UIT por incidente
<p>Por interrupción del servicio por averías en la solución mayor a tres (03) horas</p> <p>Se considera como consecuencia de un incidente que afecta la operatividad de la solución afectando a los usuarios que lo utilizan. Se considera desde la notificación al Contratista por parte del área usuaria posteriores a las solicitudes de soporte técnico mayor a 3 horas para la atención.</p> <p>Procedimiento:</p> <ul style="list-style-type: none"> El área usuaria detecta interrupción del servicio y solicita atención al contratista a través de llamada telefónica o correo electrónico a su centro de atención u otros correos que proporcione el Contratista. En caso de pasado tres (03) horas continuas con la interrupción del servicio, se informará al área de Logística para la aplicación de la penalidad correspondiente. 	0.20 UIT por incidente
<p>Por problemas en la restauración de la información del servicio mayor a dos (02) horas</p> <p>Se aplicará como consecuencia de realizar actualizaciones, upgrades o averías de software al momento del soporte técnico de la solución ofertada.</p> <p>Procedimiento:</p> <ul style="list-style-type: none"> El área usuaria determina que la solución no cuenta con la configuración que permita el correcto funcionamiento del mismo. El área usuaria comunica el incidente al contratista, quien se encuentra realizando actividades sobre la solución, a partir de este momento se contabiliza el tiempo. <p>En caso de que el contratista no pueda resolver el incidente dentro del plazo de dos (02) horas, se registrará la observación en la hoja de visita técnica del contratista o correo electrónico y se informará al área de Logística para la aplicación de la penalidad correspondiente.</p>	0.20 UIT por incidente

7.7. Responsabilidad por vicios ocultos

La recepción conforme de la prestación por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento. El plazo máximo de responsabilidad del contratista es de, no menor de 36 meses contado a partir de la conformidad de la implementación otorgada por LA ENTIDAD.

7.8. La subcontratación para la ejecución de la prestación principal y accesorias

Durante la ejecución de la presente contratación está prohibida la sub contratación tanto para la implementación como para el soporte técnico.

Importante

Para determinar que los postores cuentan con las capacidades necesarias para ejecutar el contrato, el comité de selección incorpora los requisitos de calificación previstos por el área usuaria en el requerimiento, no pudiendo incluirse requisitos adicionales, ni distintos a los siguientes:

3.2. REQUISITOS DE CALIFICACIÓN

B	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 1,979,451.80 (Un Millón Novecientos Setenta y Nueve Mil Cuatrocientos Cincuenta y Uno con 80/100 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.</p> <p>Se consideran bienes similares a los siguientes:</p> <ul style="list-style-type: none"> • Ventas de Firewall en donde pueden incluir soporte, garantía y capacitación del bien. • Adquisición de Firewalls en general, en donde se pueden incluir implementación, soporte, garantía y/o capacitación del bien. • Ventas o adquisición del sistema de Seguridad Perimetral y/o Plataforma Seguridad Red Perimetral. • Equipamiento de Soluciones de Seguridad Perimetral. • Venta de licencias de firewall incluyendo mantenimiento y/o soporte técnico de firewall. • Venta de firewall que pueda estar dentro de un proceso de servicios • Venta de equipos y productos de software de seguridad perimetral • Venta de soluciones de seguridad perimetral (Firewall de Red) • Venta de soluciones de IPS • Venta de productos de seguridad NGFW • Adquisición de Firewall para Aplicaciones WEB (WAF) • Equipamiento de Soluciones de Seguridad Perimetral <p><u>Acreditación:</u></p> <p>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 pago⁹, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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</p>

⁹ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehacencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"

(...)

"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".

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.

Importante

En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".

CONSULTA 19 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

En aras de fomentar una mayor pluralidad de postores, sírvase confirmar que pare acreditar la experiencia en bienes similares se aceptará las siguientes experiencias:

- ¿Adquisición de Sistema de Protección y Seguridad para Red del Centro de Datos:
- ¿Sistema de protección y seguridad para red firewall NGFW
- ¿Implementación Mejoras de Seguridad Perimetral: Firewall de Nueva Generación
- ¿Solución Next Generation Firewall

RESPUESTA A CONSULTA 19 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.

Se acoge parcialmente lo solicitado, se aceptarán como bienes similares: Sistema de protección y seguridad para red firewall NGFW, Implementación Mejoras de Seguridad Perimetral: Firewall de Nueva Generación, Solución Next Generation Firewall, por considerarse equivalentes al objeto de contratación.

C	CAPACIDAD TÉCNICA Y PROFESIONAL
C.1	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>Experiencia mínima de tres (3) años en implementaciones de sistemas de seguridad perimetral o de ciberseguridad del personal clave requerido como JEFE DE PROYECTOS.</p> <p>CONSULTA 15 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.</p> <p>Respecto al perfil del jefe de proyecto sírvase confirmar que para acreditar la experiencia se aceptará constancia o certificado indicando el cargo de ¿Gerente de Proyecto y/o Project Manager.</p> <p>RESPUESTA A CONSULTA 15 DE NEOSECURE SOCIEDAD ANONIMA CERRADA – NEOSECURE S.A.C.</p> <p>Se acoge lo indicado por el postor, se considerará Gerencia de Proyecto y/o Project Manager para acreditar la experiencia del personal clave requerido como Jefe de Proyecto, debido a que existen diferentes nomenclaturas sobre el líder del proyecto.</p>

DICE:

Experiencia mínima de tres (3) años en implementaciones de sistemas de seguridad perimetral o de ciberseguridad del personal clave requerido como **JEFE DE PROYECTOS**.

DEBE DECIR:

Experiencia mínima de tres (3) años en implementaciones de sistemas de seguridad perimetral o de ciberseguridad o Gerente de Proyecto y/o Project Manager del personal clave requerido como **JEFE DE PROYECTOS**.

Experiencia mínima de dos (2) años en implementación, migración y soporte de la solución propuesta del personal clave requerido como **ESPECIALISTA IMPLEMENTADOR**.

Experiencia mínima de dos (2) años en soporte de la solución propuesta del personal clave requerido como **PERSONAL DE SOPORTE**.




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

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

Importante

- 
- 
- 
- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*
 - *El cumplimiento de las Especificaciones Técnicas se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de las características y/o requisitos funcionales. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*
 - *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*

CAPÍTULO IV FACTORES DE EVALUACIÓN

La evaluación se realiza sobre la base de cien (100) puntos.

Para determinar la oferta con el mejor puntaje y el orden de prelación de las ofertas, se considera lo siguiente:

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
<u>Evaluación:</u> Se evaluará considerando el precio ofertado por el postor. <u>Acreditación:</u> Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).	La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $P_i = \frac{O_m \times PMP}{O_i}$ i = Oferta P _i = Puntaje de la oferta a evaluar O _i = Precio i O _m = Precio de la oferta más baja PMP = Puntaje máximo del precio 100 puntos
PUNTAJE TOTAL	100 puntos¹⁰

Importante

Los factores de evaluación elaborados por el comité de selección son objetivos y guardan vinculación, razonabilidad y proporcionalidad con el objeto de la contratación. Asimismo, estos no pueden calificar con puntaje el cumplimiento de las Especificaciones Técnicas ni los requisitos de calificación.

¹⁰ Es la suma de los puntajes de todos los factores de evaluación.

CAPÍTULO V PROFORMA DEL CONTRATO

Importante

Dependiendo del objeto del contrato, de resultar indispensable, puede incluirse cláusulas adicionales o la adecuación de las propuestas en el presente documento, las que en ningún caso pueden contemplar disposiciones contrarias a la normativa vigente ni a lo señalado en este capítulo.

Conste por el presente documento, la contratación de **ADQUISICIÓN DE UN SISTEMA DE PROTECCIÓN Y SEGURIDAD FIREWALL PERIMETRAL – RED EXTERNA**, que celebra de una parte **DIRECCIÓN NACIONAL DE INTELIGENCIA**, en adelante LA ENTIDAD, con RUC N° 20502628128, con domicilio legal en Av. Edmundo Aguilar Pastor S/N° - Chorrillos, representada por [...], identificado con DNI N° [...], y de otra parte [...], con RUC N° [...], con domicilio legal en [...], inscrita en la Ficha N° [...], Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], debidamente representado por su Representante Legal, [...], con DNI N° [...], según poder inscrito en la Ficha N° [...], Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [...], el comité de selección adjudicó la buena pro de la **LICITACIÓN PÚBLICA N° 003-2024-DINI** para la contratación de la **ADQUISICIÓN DE UN SISTEMA DE PROTECCIÓN Y SEGURIDAD FIREWALL PERIMETRAL – RED EXTERNA** a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto **ADQUISICIÓN DE UN SISTEMA DE PROTECCIÓN Y SEGURIDAD FIREWALL PERIMETRAL – RED EXTERNA**.

CLÁUSULA TERCERA: MONTO CONTRACTUAL

El monto total del presente contrato asciende a [CONSIGNAR MONEDA Y MONTO], que incluye todos los impuestos de Ley.

PRESTACIÓN	DESCRIPCIÓN	PRECIO S/
Prestación Principal	SISTEMA DE PROTECCIÓN Y SEGURIDAD FIREWALL PERIMETRAL – RED EXTERNA	
Prestación Accesorio	SOPORTE TÉCNICO	
TOTAL		

Este monto comprende el costo del bien, todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre la ejecución de la prestación materia del presente contrato.

CLÁUSULA CUARTA: DEL PAGO¹¹

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en SOLES, en pago único la prestación principal y en pagos anuales la prestación accesorio, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

Prestación principal

¹¹ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

La DINI realizará la cancelación de la prestación principal en un único pago y se hará efectiva dentro de los diez (10) días calendario de emitida la respectiva conformidad, siempre que se verifiquen las condiciones establecidas en el contrato.

Prestaciones accesorias

Soporte técnico

El pago se realizará de forma anual, dentro de los diez (10) días calendario de emitida la respectiva conformidad, siempre que se verifiquen las condiciones establecidas en el contrato.

Para tal efecto, el responsable de otorgar la conformidad de la prestación deberá hacerlo en un plazo que no excederá de los siete (7) días de producida la recepción, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad de dicho funcionario.

LA ENTIDAD debe efectuar el pago dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los bienes, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

En caso de retraso en el pago por parte de LA ENTIDAD, salvo que se deba a caso fortuito o fuerza mayor, EL CONTRATISTA tendrá derecho al pago de intereses legales conforme a lo establecido en el artículo 39 de la Ley de Contrataciones del Estado y en el artículo 171 de su Reglamento, los que se computan desde la oportunidad en que el pago debió efectuarse.

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de acuerdo al siguiente detalle:

Prestación Principal

El proveedor debe realizar la entrega total de la solución ofertada implementada y operando a un 100% con todas sus funcionalidades habilitadas máximo el 21 de diciembre de 2024.

El periodo de vigencia de la solución ofertada debe ser de treinta y seis (36) meses, el cual empezará a partir del 22 de diciembre de 2024. Las licencias y soporte del fabricante deben estar homologados su inicio y termino de vigencia.

CLÁUSULA SEXTA: PRESTACIONES ACCESORIAS¹²

Las prestaciones accesorias tienen por objeto brindar el soporte vía Web y Telefónico 24x7x365 por el periodo del contrato por parte del contratista.

El monto de las prestaciones accesorias asciende a [CONSIGNAR MONEDA Y MONTO], que incluye todos los impuestos de Ley.

Soporte Técnico: La ejecución de la prestación del servicio será durante el periodo de treinta y seis (36) meses; el cual se contabilizará a partir del 22 de diciembre de 2024.

CLÁUSULA SÉTIMA: PARTES INTEGRANTES DEL CONTRATO

El presente contrato está conformado por las bases integradas, la oferta ganadora, así como los documentos derivados del procedimiento de selección que establezcan obligaciones para las partes.

CLÁUSULA OCTAVA: GARANTÍAS

EL CONTRATISTA entregó al perfeccionamiento del contrato la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de LA ENTIDAD, por los conceptos, montos y vigencias siguientes:

¹² De conformidad con la Directiva sobre prestaciones accesorias, los contratos relativos al cumplimiento de la(s) prestación(es) principal(es) y de la(s) prestación(es) accesoria(s), pueden estar contenidos en uno o dos documentos. En el supuesto que ambas prestaciones estén contenidas en un mismo documento, estas deben estar claramente diferenciadas, debiendo indicarse entre otros aspectos, el precio y plazo de cada prestación.

- De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la [INDICAR EL TIPO DE GARANTÍA PRESENTADA] N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE]. Monto que es equivalente al diez por ciento (10%) del monto del contrato original, la misma que debe mantenerse vigente hasta la conformidad de la recepción de la prestación.

En el caso que corresponda, consignar lo siguiente:

- Garantía fiel cumplimiento por prestaciones accesorias: [CONSIGNAR EL MONTO], a través de la [INDICAR EL TIPO DE GARANTÍA PRESENTADA] N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE], la misma que debe mantenerse vigente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

CLÁUSULA NOVENA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

LA ENTIDAD puede solicitar la ejecución de las garantías cuando EL CONTRATISTA no las hubiere renovado antes de la fecha de su vencimiento, conforme a lo dispuesto en el literal a) del numeral 155.1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA: RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La recepción será otorgada de acuerdo al siguiente detalle:

Prestación principal

La Oficina de Administración mediante su área de logística será la encargada de recepcionar los bienes ofertados.

La conformidad de la prestación principal será otorgada por la Oficina de Tecnologías de Información y Comunicaciones en su calidad de área usuaria, dentro de los 7 días calendario de la entrega total de la solución ofertada, implementada y operando a un 100% con todas sus funcionalidades habilitadas y de la entrega de la documentación solicitada en el punto 7.1.1.5 al 7.1.1.12.

Prestaciones accesorias

Soporte técnico

La conformidad será otorgada por la Oficina de Tecnologías de Información y Comunicaciones – OTIC en su calidad de área usuaria luego de cumplido el periodo anual de servicio de soporte técnico y de la entrega por el postor del informe del soporte solicitado en el numeral 5.6.1 y será emitida dentro de los siete (07) días calendario.

Pruebas de puesta en funcionamiento para la conformidad de los bienes

Una vez concluida la implementación, el área usuaria evaluará los distintos aspectos requeridos y si todo está conforme dentro de los 7 días posteriores a la implementación total de la solución, se procederá con la aceptación de las mismas. Cualquier incumplimiento debe ser asumido por el contratista, a costo cero para la Entidad.

De existir observaciones, LA ENTIDAD las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (8) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no cumpliera a cabalidad con la subsanación, LA ENTIDAD puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

Este procedimiento no resulta aplicable cuando los bienes manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

EL CONTRATISTA declara bajo juramento que se compromete a cumplir las obligaciones derivadas del presente contrato, bajo sanción de quedar inhabilitado para contratar con el Estado en caso de incumplimiento.

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

La recepción conforme de la prestación por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de, no menor de 3 años contados a partir de la conformidad de la implementación otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA ENTIDAD le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo a la siguiente fórmula:

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

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;

F = 0.40 para plazos menores o iguales a sesenta (60) días.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de LA ENTIDAD no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme el numeral 162.5 del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

Importante

De haberse previsto establecer penalidades distintas a la penalidad por mora, incluir dichas penalidades, los supuestos de aplicación de penalidad, la forma de cálculo de la penalidad para cada supuesto y el procedimiento mediante el cual se verifica el supuesto a penalizar, conforme el artículo 163 del Reglamento de la Ley de Contrataciones del Estado.

Otras penalidades aplicables

Concepto	Monto
Por demora en la respuesta de solicitudes de soporte técnico mayor a 3 horas Se considera desde la notificación al Contratista por parte del área usuaria y la contestación de la misma. Procedimiento: <ul style="list-style-type: none"> El área usuaria solicita atención al contratista a través de llamada telefónica o correo electrónico a su centro de atención u otros correos que proporcione el Contratista. En caso de pasado tres (03) horas y no tener respuesta del contratista, se informará a la unidad orgánica de Logística para la aplicación de la 	0.1 UIT por incidente

penalidad correspondiente.	
Por interrupción del servicio por averías en la solución mayor a tres (03) horas Se considera como consecuencia de un incidente que afecta la operatividad de la solución afectando a los usuarios que lo utilizan. Se considera desde la notificación al Contratista por parte del área usuaria posteriores a las solicitudes de soporte técnico mayor a 3 horas para la atención. Procedimiento: <ul style="list-style-type: none"> El área usuaria detecta interrupción del servicio y solicita atención al contratista a través de llamada telefónica o correo electrónico a su centro de atención u otros correos que proporcione el Contratista. En caso de pasado tres (03) horas continuas con la interrupción del servicio, se informará al área de Logística para la aplicación de la penalidad correspondiente. 	0.20 UIT por incidente
Por problemas en la restauración de la información del servicio mayor a dos (02) horas Se aplicará como consecuencia de realizar actualizaciones, upgrades o averías de software al momento del soporte técnico de la solución ofertada. Procedimiento: <ul style="list-style-type: none"> El área usuaria determina que la solución no cuenta con la configuración que permita el correcto funcionamiento del mismo. El área usuaria comunica el incidente al contratista, quien se encuentra realizando actividades sobre la solución, a partir de este momento se contabiliza el tiempo. En caso de que el contratista no pueda resolver el incidente dentro del plazo de dos (02) horas, se registrará la observación en la hoja de visita técnica del contratista o correo electrónico y se informará al área de Logística para la aplicación de la penalidad correspondiente.	0.20 UIT por incidente

Estas penalidades se deducen de los pagos a cuenta o del pago final, según corresponda; o si fuera necesario, se cobra del monto resultante de la ejecución de la garantía de fiel cumplimiento.

Estos dos (2) tipos de penalidades pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

Cuando se llegue a cubrir el monto máximo de la penalidad por mora o el monto máximo para otras penalidades, de ser el caso, LA ENTIDAD puede resolver el contrato por incumplimiento.

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 32.3 del artículo 32 y artículo 36 de la Ley de Contrataciones del Estado, y el artículo 164 de su Reglamento. De darse el caso, LA ENTIDAD procederá de acuerdo a lo establecido en el artículo 165 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

Cuando se resuelva el contrato por causas imputables a algunas de las partes, se debe resarcir los daños y perjuicios ocasionados, a través de la indemnización correspondiente. Ello no obsta la aplicación de las sanciones administrativas, penales y pecuniarias a que dicho incumplimiento diere lugar, en el caso que éstas correspondan.

Lo señalado precedentemente no exime a ninguna de las partes del cumplimiento de las demás obligaciones previstas en el presente contrato.

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

EL CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el CONTRATISTA 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, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL CONTRATISTA 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.

Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO

Sólo en lo no previsto en este contrato, en la Ley de Contrataciones del Estado y su Reglamento, en las directivas que emita el OSCE y demás normativa especial que resulte aplicable, serán de aplicación supletoria las disposiciones pertinentes del Código Civil vigente, cuando corresponda, y demás normas de derecho privado.

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS¹³

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación o arbitraje, según el acuerdo de las partes.

Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley de Contrataciones del Estado y su Reglamento.

Facultativamente, cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 224 del Reglamento de la Ley de Contrataciones del Estado, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 45.21 del artículo 45 de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

Cualquiera de las partes puede elevar el presente contrato a Escritura Pública corriendo con todos los gastos que demande esta formalidad.

CLÁUSULA VIGÉSIMA: CONFIDENCIALIDAD

EL CONTRATISTA se compromete a no hacer uso para su beneficio personal, ni proporcionar a terceros, por ningún motivo, la información relacionada con las actividades desarrolladas por LA ENTIDAD a la que tenga acceso como consecuencia de la prestación que brindará, lo cual debe ser respetado desde el inicio del presente contrato e inclusive hasta después de su culminación.

Todos los documentos generados por LA ENTIDAD constituyen bienes a su cuidado y protección, por lo que, EL CONTRATISTA se encuentra prohibido de reproducir, deteriorar o hacer mal uso de aquello que tengan en su poder en razón de la prestación que brindará.

EL CONTRATISTA se encuentra obligado a cumplir con las Políticas de Seguridad de la Información que le indique la ENTIDAD.

¹³ De acuerdo con el numeral 225.3 del artículo 225 del Reglamento, las partes pueden recurrir al arbitraje ad hoc cuando las controversias deriven de procedimientos de selección cuyo valor estimado sea menor o igual a cinco millones con 00/100 soles (S/ 5 000 000,00).

Cabe precisar, que el contratista, con motivo de la prestación, recibirá de la Dirección Nacional de Inteligencia información de carácter estrictamente confidencial que debe ser utilizada solo para los fines de ejecución, por ello, será obligación del contratista mantener la secrecía y confidencialidad respecto a los datos e información de cualquier clase, que la Dirección Nacional de Inteligencia le proporcione, o bien, a la que tenga acceso, con motivo de la prestación y desarrollo de su ejecución. Adicionalmente, el contratista está obligado a instruir a sus funcionarios o personal que será parte conformante del recurso humano que ejecutará la prestación respecto a la obligación de mantener total secrecía y confidencialidad.

Se deberá garantizar la confidencialidad de los datos transmitidos o recibidos.

Como parte de la prestación y en relación a la CONFIDENCIALIDAD el contrato considerará la cláusula y acuerdo de confidencialidad.

Toda documentación generada para cumplir con los entregables debe ser desarrollada en las instalaciones de la DINI de ser el caso.

CLÁUSULA VIGÉSIMA PRIMERA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución del presente contrato:

DOMICILIO DE LA ENTIDAD: [.....]

DOMICILIO DEL CONTRATISTA: [CONSIGNAR EL DOMICILIO SEÑALADO POR EL POSTOR GANADOR DE LA BUENA PRO AL PRESENTAR LOS REQUISITOS PARA EL PERFECCIONAMIENTO DEL CONTRATO]

La variación del domicilio aquí declarado de alguna de las partes debe ser comunicada a la otra parte, formalmente y por escrito, con una anticipación no menor de quince (15) días calendario.

De acuerdo con las bases integradas, la oferta y las disposiciones del presente contrato, las partes lo firman por duplicado en señal de conformidad en la ciudad de [.....] al [CONSIGNAR FECHA].

"LA ENTIDAD"

"EL CONTRATISTA"

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹⁴.

¹⁴ Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>

ANEXOS



ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 003-2024-DINI
Presente.-

El que se suscribe, [...], postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Autorización de notificación por correo electrónico:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de compra¹⁵

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o Representante legal, según corresponda

Importante

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

Importante

Cuando se trate de consorcios, la declaración jurada es la siguiente:

¹⁵ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de compra.

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 003-2024-DINI
Presente.-

El que se suscribe, [...], representante común del consorcio [CONSIGNAR EL NOMBRE DEL CONSORCIO], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Datos del consorciado 1			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Datos del consorciado 2			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Datos del consorciado ...			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de compra¹⁶

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del representante
común del consorcio**

Importante

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

¹⁶ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000 00), cuando se haya optado por perfeccionar el contrato con una orden de compra.

ANEXO N° 2

DECLARACIÓN JURADA (ART. 52 DEL REGLAMENTO DE LA LEY DE CONTRATACIONES DEL ESTADO)

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 003-2024-DINI

Presente. -

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento:

- i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.
- ii. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.
- iii. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- iv. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo N° 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.
- v. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.
- vi. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.
- vii. Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda**

Importante

En el caso de consorcios, cada integrante debe presentar esta declaración jurada, salvo que sea presentada por el representante común del consorcio.

ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 003-2024-DINI

Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el **[CONSIGNAR EL OBJETO DE LA CONVOCATORIA]**, de conformidad con las Especificaciones Técnicas que se indican en el numeral 3.1 del Capítulo III de la sección específica de las bases y los documentos del procedimiento.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda**

Importante

Adicionalmente, puede requerirse la presentación de documentación que acredite el cumplimiento de las especificaciones técnicas, conforme a lo indicado en el acápite relacionado al contenido de las ofertas de la presente sección de las bases.

ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE ENTREGA

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 003-2024-DINI
Presente. -

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a entregar los bienes objeto del presente procedimiento de selección en el plazo de

Prestación Principal

El proveedor debe realizar la entrega total de la solución ofertada implementada y operando a un 100% con todas sus funcionalidades habilitadas máximo el 21 de diciembre de 2024.

El periodo de vigencia de la solución ofertada debe ser de treinta y seis (36) meses, el cual empezará a partir del 22 de diciembre de 2024. Las licencias y soporte del fabricante deben estar homologados su inicio y termino de vigencia.

Prestación Accesorias

Del Soporte Técnico: La ejecución de la prestación del servicio será durante el periodo de treinta y seis (36) meses; el cual se contabilizará a partir del 22 de diciembre de 2024.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

ANEXO N° 5

PROMESA DE CONSORCIO

(Sólo para el caso en que un consorcio se presente como postor)

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 003-2024-DINI

Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta a la LICITACIÓN PÚBLICA N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO].

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, de conformidad con lo establecido por el artículo 140 del Reglamento de la Ley de Contrataciones del Estado, bajo las siguientes condiciones:

a) Integrantes del consorcio

1. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1].
2. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2].

b) Designamos a [CONSIGNAR NOMBRES Y APELLIDOS DEL REPRESENTANTE COMÚN], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], como representante común del consorcio para efectos de participar en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato correspondiente con [CONSIGNAR NOMBRE DE LA ENTIDAD].

Asimismo, declaramos que el representante común del consorcio no se encuentra impedido, inhabilitado ni suspendido para contratar con el Estado.

c) Fijamos nuestro domicilio legal común en [.....].

d) Las obligaciones que corresponden a cada uno de los integrantes del consorcio son las siguientes:

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [%]¹⁷

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]¹⁸

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%¹⁹

[CONSIGNAR CIUDAD Y FECHA]

Consortiado 1

Nombres, apellidos y firma del Consortiado 1 o de
su Representante Legal
Tipo y N° de Documento de Identidad

Consortiado 2

Nombres, apellidos y firma del Consortiado 2 o de
su Representante Legal
Tipo y N° de Documento de Identidad

Importante

De conformidad con el artículo 52 del Reglamento, las firmas de los integrantes del consorcio deben ser legalizadas.

¹⁷ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

¹⁸ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

¹⁹ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

ANEXO N° 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 003-2024-DINI
Presente. -

Es grato dirigirme a usted, para hacer de su conocimiento que, de acuerdo con las bases, mi oferta es la siguiente:

CONCEPTO	PRECIO TOTAL
PRESTACIÓN PRINCIPAL: SISTEMA DE PROTECCIÓN Y SEGURIDAD FIREWALL PERIMETRAL – RED EXTERNA	
PRESTACIÓN ACCESORIA: SOPORTE TÉCNICO	
TOTAL	

El precio de la oferta [CONSIGNAR LA MONEDA DE LA CONVOCATORIA] incluye todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre el costo del bien a contratar; excepto la de aquellos postores que gocen de alguna exoneración legal, no incluirán en el precio de su oferta los tributos respectivos.

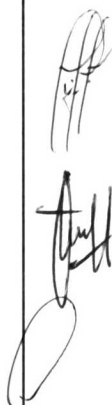
[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Importante

- *El postor debe consignar el precio total de la oferta, sin perjuicio, que de resultar favorecido con la buena pro, presente el detalle de precios unitarios para el perfeccionamiento del contrato.*
- *El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:*

"Mi oferta no incluye [CONSIGNAR EL TRIBUTO MATERIA DE LA EXONERACIÓN]"
- *El postor debe detallar en el precio de su oferta, el monto correspondiente a la prestación principal y las prestaciones accesorias.*



ANEXO N° 7

CARTA DE COMPROMISO DEL PERSONAL CLAVE

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 003-2024-DINI

Presente. -

Yo [CONSIGNAR NOMBRES Y APELLIDOS COMPLETOS] identificado con documento de identidad N° [CONSIGNAR NÚMERO DE DNI O DOCUMENTO DE IDENTIDAD ANÁLOGO], domiciliado en [CONSIGNAR EL DOMICILIO LEGAL], declaro bajo juramento:

Que, me comprometo a prestar mis servicios como personal clave para ejecutar las actividades según el numeral 6.2 del capítulo III para la Adquisición de Sistema de Protección de Correo Electrónico Anti - SPAM en caso que el postor [CONSIGNAR EL NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL POSTOR²⁰] resulte favorecido con la buena pro y suscriba el contrato correspondiente.

Para dicho efecto, declaro que mis calificaciones y experiencia son las siguientes:

A. Calificaciones

[CONSIGNAR DE SER EL CASO, LA FORMACIÓN ACADÉMICA Y/O CAPACITACIONES SEGÚN LO REQUERIDO EN EL CAPÍTULO III DE LA PRESENTE SECCIÓN DE LAS BASES].

[EL POSTOR DEBE SEÑALAR PROFESIÓN DEL PERSONAL CLAVE, ASÍ COMO EL NOMBRE DE LA UNIVERSIDAD O INSTITUCIÓN EDUCATIVA QUE EXPIDIÓ EL GRADO O TÍTULO PROFESIONAL REQUERIDO]

B. Experiencia

[CONSIGNAR DE SER EL CASO, LA EXPERIENCIA SEGÚN LO REQUERIDO EN EL CAPÍTULO III DE LA PRESENTE SECCIÓN DE LAS BASES].

N°	Cliente o Empleador	Objeto de la contratación	Fecha de inicio	Fecha de culminación	Tiempo
1					
(...)					

La experiencia total acumulada es de: [CONSIGNAR LA EXPERIENCIA TOTAL ACUMULADA EN AÑOS, MESES Y DÍAS, SEGÚN CORRESPONDA]

Asimismo, manifiesto mi disposición de ejecutar las actividades que comprenden el desempeño del referido cargo, durante el periodo de ejecución del contrato.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del personal

.....
Firma, Nombres y Apellidos del postor o Representante legal o común, según corresponda

Importante

- De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.
- El postor deberá adjuntar copia de los documentos indicados en la carta de compromiso del personal clave como acreditación del cumplimiento de la calificación y la experiencia del personal
- 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

²⁰En el caso que el postor sea un consorcio se debe consignar el nombre del consorcio o de uno de sus integrantes.

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 003-2024-DINI
Presente. -

Mediante el presente, el suscrito detalla la siguiente EXPERIENCIA EN LA ESPECIALIDAD:

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²¹	FECHA DE LA CONFORMIDAD DE SER EL CASO ²²	EXPERIENCIA PROVENIENTE ²³ DE:	MONEDA	IMPORTE ²⁴	TIPO DE CAMBIO VENTA ²⁵	MONTO FACTURADO ACUMULADO ²⁶
1										
2										
3										
4										

²¹ Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

²² **Únicamente**, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho periodo.

²³ 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. Al respecto, según la Opinión N° 216-2017/DTN *“Considerando que la sociedad matriz y la sucursal constituyen la misma persona jurídica, la sucursal puede acreditar como suya la experiencia de su matriz”*. Del mismo modo, según lo previsto en la Opinión N° 010-2013/DTN, *“... en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad incorporada o absorbida, que se extingue producto de la fusión; asimismo, si en virtud de la escisión se transfiere un bloque patrimonial consistente en una línea de negocio completa, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante podrá emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe”*.

²⁴ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

²⁵ El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

²⁶ Consignar en la moneda establecida en las bases.

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²¹	FECHA DE LA CONFORMIDAD DE SER EL CASO ²²	EXPERIENCIA PROVENIENTE ²³ DE:	MONEDA	IMPORTE ²⁴	TIPO DE CAMBIO VENTA ²⁵	MONTO FACTURADO ACUMULADO ²⁶
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

.....

Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

ANEXO N° 9

**DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)**

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 003-2024-DINI
Presente. -

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro que la experiencia que acredito de la empresa [CONSIGNAR LA DENOMINACIÓN DE LA PERSONA JURÍDICA] como consecuencia de una reorganización societaria, no se encuentra en el supuesto establecido en el numeral 49.4 del artículo 49 del Reglamento.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda**

Importante

A efectos de cautelar la veracidad de esta declaración, el postor puede verificar la información de la Relación de Proveedores Sancionados por el Tribunal de Contrataciones del Estado con Sanción Vigente en <http://portal.osce.gob.pe/rnp/content/relación-de-proveedores-sancionados>.

También le asiste dicha facultad al órgano encargado de las contrataciones o al órgano de la Entidad al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.



ANEXO N° 10

DECLARACIÓN JURADA DE RESERVA Y CONFIDENCIALIDAD

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N°003-2024-DINI
Presente.-

De nuestra consideración:

El que suscribe, (Postor y/o Representante Legal de.....), identificado con DNI N° y RUC N°, domiciliado en; al ser adjudicado con la Buena Pro del procedimiento de selección LICITACIÓN PÚBLICA N° 004-2024-DINI, **DECLARO BAJO JURAMENTO:** comprometerme a no hacer uso para beneficio personal, ni proporcionarle a terceros, por ningún motivo, la información relacionada con las actividades desarrolladas por la Dirección Nacional de Inteligencia – DINI a la que tenga acceso como consecuencia de tener que prestarle un servicio o proveerle de algún bien.

La presente disposición deberá ser respetada desde el inicio de la prestación del servicio contratado o provisión del bien adquirido e inclusive finalizadas éstas sea cual fuere el motivo de su culminación.

Todos los documentos generados por la Dirección Nacional de Inteligencia constituyen bienes a su cuidado y protección, por lo que, el suscrito se encuentra prohibido de reproducir, deteriorar o hacer mal uso de aquello que tengan en su poder en razón del servicio que presta, siendo sancionada penalmente la conducta que pretenda sustraer, retirar o extraer en provecho propio o de terceros, con fines de lucro u otros móviles, la información contenida en dispositivos manuales, mecánicos, telemáticos, electrónicos, magnéticos, análogos o bajo cualquier otro medio.

El incumplimiento de lo pactado trasgrede los siguientes artículos del Código Penal:

Artículo 165.- Violación del secreto profesional

El que, teniendo información por razón de su estado, oficio, empleo, profesión o ministerio, de secretos cuya publicación pueda causar daño, los revela sin consentimiento del interesado, será reprimido con pena privativa de la libertad no mayor de dos años y con sesenta a ciento veinte días – multa.

Artículo 330.- Revelación de secretos nacionales

El que revela o hace accesible a un Estado extranjero o a sus agentes o al público, secretos que el interés de la República exige guardarlos, será reprimido con pena privativa de la libertad no menor de cinco ni mayor de quince años.

Si el agente obra por lucro o por cualquier otro móvil innoble, la pena será no menor de diez años. Cuando el agente actúa por cual, la pena será no mayor de cuatro años.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

ANEXO N° 11

**AUTORIZACIÓN DE NOTIFICACIÓN DE LA DECISIÓN DE LA ENTIDAD SOBRE LA
SOLICITUD DE AMPLIACIÓN DE PLAZO MEDIANTE MEDIOS ELECTRÓNICOS DE
COMUNICACIÓN**

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 003-2024-DINI
Presente. -

El que se suscribe, [...], postor adjudicado y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], autorizo que durante la ejecución del contrato se me notifique al correo electrónico [INDICAR EL CORREO ELECTRÓNICO] lo siguiente:




✓ Notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal o común, según
corresponda**

Importante

La notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo se efectúa por medios electrónicos de comunicación, siempre que se cuente con la autorización correspondiente y sea posible obtener un acuse de recibo a través del mecanismo utilizado.

ANEXO N° 12

DECLARACION JURADA PARA ACREDITAR EL SUSTENTO TECNICO DE LA SOLUCION PROPUESTA

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 003-2024-DINI
Presente. -

De nuestra consideración:

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, declaro el cumplimiento de las especificaciones técnicas para lo cual se adjunta al presente anexo, el detalle del cumplimiento de cada punto indicando el folio específico de ubicación de cada uno de los aspectos técnicos solicitados, la misma que se sustenta con la documentación técnica, así como su descripción detallada.

En el supuesto de que alguna característica técnica no obre en la documentación técnica no se requerirá consignar el folio del sustento, basta con indicar el cumplimiento de tales características técnicas.

5. Características y condiciones de los bienes a contratar

5.1. Descripción y cantidad de los bienes

No.	Descripción	Cumple Si o no	Folio del sustento
5.1.1	Cantidad: Dos (02) unidades de Firewall		
5.1.2	Los equipos deben ser hardware y software integrados de tipo appliance o chassis y provistos por el mismo fabricante. No se aceptarán servidores o máquinas virtuales.		
5.1.3	El hardware ofertado deberá ser totalmente nuevo.		
5.1.4	Altura máxima de 01 RU, con sus respectivos rieles telescópicos para montaje en gabinete 19"		
5.1.5	El sistema operativo deberá ser del fabricante de la solución ofertada, el mismo deberá venir de fábrica con el "hardening" necesario, el fabricante deberá desarrollar las actualizaciones de sistema operativo, parches del software o módulos utilizados por la solución ofertada.		
5.1.6	El fabricante de la solución propuesta debe recibir actualizaciones de inteligencia de amenazas provenientes de otros fabricantes a través del Cyber Threat Alliance, con el propósito de contar con un óptimo nivel de prevención de amenazas cibernéticas. El fabricante debe aparecer como miembro en la web oficial del Cyber Threat Alliance para lo cual debe presentar la versión impresa del sitio web de Cyber Threat Alliance, acompañado del link de la página impresa.		
5.1.7	El fabricante de la solución de seguridad debe estar presente en los últimos 08 reportes de Gartner (Magic Cuadrant), en el cuadrante de Lideres para Network Enterprise Firewalls.		
5.1.8	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciados 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 el link público de los equipos propuestos donde se verifique que los modelos propuestos no están en ese listado o sustentado mediante carta del fabricante dirigido al proceso.		
5.1.9	Los sistemas operativos que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades		

	(CVE) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas. Esto se aplicará únicamente al Sistema Operativo o firmware que se instalará en la entidad sobre los equipos propuestos por el postor.		
5.1.10	<p>El sistema debe estar habilitado y configurado con las políticas de todas las funcionalidades:</p> <ul style="list-style-type: none"> • Firewall. • Control de aplicaciones. • Sistema de Prevención de Intrusos (IPS). • Antivirus o Antimalware. • Emulación de amenazas (Sandbox). • Filtrado de comando y control, antibot o antispymware.- • DNS Security. <p>Que permita detectar y bloquear (prevenir) virus y malware que se propaguen, al menos, en los siguientes protocolos: HTTP, FTP, SMB, SMTP, IMAP, POP3 y SSL o TLS, que cubran finalmente el objetivo requerido.</p>		
5.1.11	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basado en usuarios y grupos de usuarios.		
5.1.12	<p>La implementación debe ser validada por los servicios profesionales del fabricante y al finalizar la validación deberá emitir un informe de aplicación de mejores prácticas en la habilitación de todas las funcionalidades y aplicando las políticas de seguridad por cada funcionalidad. Se debe contemplar un mínimo de 4 días de los servicios profesionales del fabricante.</p> <p>Para garantizar el cumplimiento de los servicios profesionales del fabricante se deberá sustentar una declaración jurada en la presentación de la propuesta y una carta del fabricante a la firma del contrato. Al finalizar la implementación se requiere un informe de los servicios profesionales del fabricante.</p> <p>Por otro lado, se aceptará que las actividades que realice este personal sean de manera remota siempre y cuando se cumpla con algunos requisitos, por motivos de seguridad nacional, que se especificarán una vez se haya realizado la firma y perfeccionamiento del contrato. Este personal debe ser de habla hispana.</p>		
5.1.13	El proveedor deberá considerar en la implementación los servicios de Networking necesario para la implementación (configuración del core, Switches, reglas en firewall perimetral e interno y aplicación de buenas prácticas para la convivencia de la red externa con la interna).		
5.1.14	El nivel de soporte del fabricante debe ser 24 x 7 durante el periodo del contrato. Debiendo ser asistido por el propio personal del fabricante a través de su propio centro de atención, y en coordinación directa con el contratista para el seguimiento y escalamiento de los requerimientos.		
Características Técnicas de cada Firewall			
5.1.15	El throughput como mínimo debe ser 5.8 Gbps para "Threat Prevention o Threat Protection" con las funcionalidades habilitadas: Application Control, IPS, Antivirus, Anti-Bot o Antispymware y Protección contra Dia Cero con logging activo; medido en condiciones de prueba empresariales o en transacciones de aplicaciones mixtas. Asimismo, el throughput mínimo de 9 Gbps de Next Generation Firewall o Firewall con todas las funcionalidades definidas por cada fabricante medido en condiciones de prueba empresariales o en transacciones de aplicaciones mixtas. No se aceptarán otras mediciones a las indicadas		
5.1.16	Debe soportar al menos cien mil (100 000) conexiones o sesiones por segundo.		
5.1.17	Debe soportar al menos 1'000,000 de conexiones o sesiones concurrentes.		

5.1.18	Cada equipo deberá contar con dos fuentes de poder de 100-240 VAC 50-60 Hz.		
5.1.19	Las fuentes de poder podrían ser de tipo hot-swap (cambio en caliente).		
5.1.20	Cada equipo deberá tener como mínimo 8 interfaces de cobre GE RJ45.		
5.1.21	Debe incluir un (01) puerto de administración dedicado y un (01) para HA dedicado.		
5.1.22	Debe soportar alta disponibilidad en modo activo/pasivo y modo activo/activo.		
5.1.23	Administración a través de SSH y de interfaz Web segura (HTTPS).		
Prevención de amenazas			
5.1.24	Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en tiempo real en el repositorio la clasificación y/o reputación de direcciones IP y/o Dominios y/o URL y/o redes de C2 o Comando y Control y/o ataques DoS.		
5.1.25	La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.		
5.1.26	Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web, Mail (SMTP o POP3), SMB, FTP y SSL o TLS.		
5.1.27	Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real.		
5.1.28	La identificación de amenazas avanzadas camufladas en tráfico DNS deberá contar con mecanismos avanzados de detección con el objetivo de identificar ataques imposibles de mitigar con firmas y/o reputación del dominio. Para ello se requiere que el tráfico DNS sea analizado con técnicas de inteligencia artificial y/o análisis predictivo y/o machine learning en tiempo real.		
5.1.29	Debe soportar Inspección de tráfico cifrado/encryptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).		
5.1.30	Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware.		
5.1.31	Debe soportar el manejo personalizado (añadir, borrar o modificar) para registrar loC (Indicadores de Compromiso) o listas dinámicas externa, siempre y cuando se cumpla con el requerimiento solicitado.		
5.1.32	Debe tener capacidad de integración con fuente de loC de terceros (External loC) a través de direcciones web URL, con capacidades de detección y prevención o listas dinámicas externa, siempre y cuando se cumpla con el requerimiento solicitado. La aplicación y prevención de seguridad, en base a los loC o listas dinámicas externa incluidos, debe ser de manera automática, sin interacción del usuario administrador una vez aplicada a una política de seguridad.		
Funcionalidades de red			
5.1.33	Para tráfico cifrado SSL debe ser capaz de inspeccionar tráfico cifrado en TLS 1.3 y debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.		
5.1.34	Debe soportar L2 y L3.		
5.1.35	Deben soportar inspección del tráfico cifrado (SSL/TLS).		
5.1.36	Deberá soportar descifrado del tráfico considerando al menos los siguientes algoritmos: RSA y/o DHE y/o ECDHE y/o 3DES y/o RC4 y/o AES128 y/o AES256 y/o CHACHA20-POLY1305 y/o MD5 y/o SHA1 y/o SHA256 y/o SHA384.		
5.1.37	Debe soportar IPv4 e IPv6.		
5.1.38	Debe poder realizar límites de ancho de banda (upload/download) para controlar tráfico por tipo de destino, servicio y/o aplicación.		
5.1.39	Los firewalls deben soportar como mínimo 1,024 VLANs Tags 802.3ad.		
Gestión de políticas			
5.1.40	Las reglas de firewall deben poder tener limitantes y/o vigencia en base a tiempo o determinado período.		

5.1.41	El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como direcciones IP, redes, usuarios, grupos de usuarios, servicios de red, direcciones de URL y aplicaciones.		
Geolocalización			
5.1.42	Soportar la creación de políticas basadas en Geolocalización, configurando que el tráfico de determinado País y/o Países sean bloqueados o permitidos.		
5.1.43	Debe contar con la visualización de los países de origen y destino en los logs de acceso.		
5.1.44	Debe contar con la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.		
5.1.45	Las actualizaciones de las direcciones o rangos de IP publica por cada país, debe realizarse periódicamente y de manera automática.		
IPS			
5.1.46	El IPS debe contar con mecanismo de detección de amenazas de múltiples niveles o métodos: detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías, detección basada en comportamiento.		
5.1.47	A nivel de aplicación, debe incluir protecciones tipo Cross Site Scripting y/o SQL Injection y/o Command Injection e injection proteccion para DN (Distinguished Names) y/o C&C desconocidos.		
5.1.48	Las firmas de protección de IPS deben poder categorizarse según un nivel de severidad, nivel de efectividad (confianza) o explotación cloud en línea o exploit-kit y nivel consumo de recursos o fuerza bruta.		
5.1.49	Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP y/o SMTP y/o IMAP y/o DNS y/o FTP y/o SNMP y/o IMAP y/o SMB.		
5.1.50	Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos.		
5.1.51	Debe soportar Inspección de trafico encriptado HTTPS tanto Inbound como Outbound.		
5.1.52	Debe permitir adicionar excepciones a las protecciones de IPS.		
5.1.53	Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense.		
5.1.54	Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos o ataques conocidos.		
5.1.55	Detección y prevención del uso indebido de un protocolo o ataques no basados en protocolos IP, para actividad maliciosa o amenaza potencial.		
5.1.56	Detección y prevención de comunicaciones de malware tipo C&C salientes.		
5.1.57	Detección y prevención de intentos de tunelización, para intentos de fuga de datos o intentos de eludir otras medidas de seguridad, como el filtrado web.		
Protección de DNS			
5.1.58	La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de URL y recursos DNS no identificados y/o no clasificados al momento de ser registrado.		
5.1.59	La solución debe tener una capa de protección DNS, para proteccion contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA), empleando protección basada en Machine Learning, así como protección fuga o exfiltracion de información mediante DNS Tunneling, en tiempo real		
5.1.60	La solución debe contar con análisis la reputación de direcciones URL y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).		

5.1.61	La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de URL y recursos DNS no identificados y/o no clasificados al momento de ser registrado.		
Protección de amenazas desconocidas			
5.1.62	La solución debe ser capaz de emular o ejecutar los archivos identificados en el firewall de forma automática, a través del envío y posterior análisis en la nube del propio fabricante de firewall, para la emulación o ejecución de malware de día cero (sandbox).		
5.1.63	La solución debe proteger a los usuarios internos de manera que prevenga el acceso o descarga a los archivos en tanto estos son analizados en el equipo de emulación, si el archivo es benigno se entrega el archivo original al usuario y si el archivo es maligno se deniega su acceso o descarga.		
5.1.64	Cada archivo emulado en el sandbox debe generar un reporte detallado que incluya información forense sobre la actividad maliciosa originada por el archivo.		
5.1.65	El motor de emulación debe admitir varios sistemas operativos, como Windows XP y/o Windows7 y/o Windows 10.		
5.1.66	Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (personalizado y hardenizado), inyección de código a procesos permitidos o análisis de memoria en run time.		
5.1.67	Se debe emular archivos desconocidos en el sandbox.		
Control de aplicaciones y filtro Web			
5.1.68	La funcionalidad de control de aplicaciones debe tener una detección y reconocimiento de al menos 3,600 aplicaciones distintas, entre ellas: Streaming o Video, P2P, Proxy, redes sociales, Juegos o similares.		
5.1.69	Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.		
5.1.70	Debido a que diariamente se crean decenas de miles de nuevas páginas web, la solución deberá ser capaz de analizar en tiempo real si la página web tiene contenido malicioso cuando un usuario intenta acceder.		
5.1.71	Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y soportar protección al protocolo HTTP/2, esta última deberá habilitarse desde la interfaz web.		
Inventario de dispositivos de red			
5.1.72	La solución deberá contar con un módulo de descubrimiento, identificación y clasificación de dispositivos como teléfonos IP y/o cámaras de vigilancia y/o consolas de videojuegos y/o impresoras y/o dispositivos médicos y/o equipos industriales y/o equipos de seguridad y/o servidores, entre otros. Este módulo debe contar con capacidades de protección de amenazas a través de las políticas de seguridad.		
5.1.73	El descubrimiento de los dispositivos debe mostrar la marca del fabricante y/o tipo de dispositivo y/o serial y/o sistema operativo y/o dirección IP y/o dirección MAC.		
5.1.74	Debe identificar dispositivos que posean software o hardware desactualizado y vulnerable, junto con su respectivo identificador CVE.		
5.1.75	Debe hacer uso del protocolo SNMP para integrarse a los switches.		
5.1.76	Debe descubrir dispositivos inclusive si el tráfico de los dispositivos de red no pasan por los NGFW.		
Revisión de salud de los Firewall			
5.1.77	Debe contar con un módulo integrado que monitoree continuamente los firewalls, en base a sus políticas y configuración de buenas prácticas y los compare con base de datos de estándares reconocidos de la industria como mínimo Cobit y/o ISO 27001 y/o NIST 800 53 o mejores prácticas de seguridad, con la finalidad de obtener reportes gráficos detallados informes que demuestren el cumplimiento de los estándares reconocidos de la industria aplicables o mejores prácticas recomendadas.		

5.1.78	Se deberá incluir una herramienta integrada y/o externa que genere alertas si existen problemas de salud del equipo en materia de hardware y software, como mínimo: consumo de memoria, problemas de la alta disponibilidad (HA), problemas de disco duro, , expiración de licencias.		
Inteligencia de amenazas			
5.1.79	Se debe proporcionar acceso a la base de datos de inteligencia de amenazas del fabricante, el cual debe permitir hacer consultas de Hashes, Dominios y Direcciones IP, para mostrar información sobre la amenaza, a nivel de clasificación, reputación, familia de malware, comportamiento.		
VPN			
5.1.80	Debe soportar túneles VPN punto a punto (Site-to-Site) y túneles de acceso remoto para usuario final (Client-to-Site).		
5.1.81	Debe estar licenciado para soportar 50 usuarios concurrentes o simultáneos de IPSec VPN Client-to-Site, con capacidad de VPN para dispositivos Windows, Linux y MAC, y también dispositivos móviles como Android y IOS.		
5.1.82	Debe poder integrarse con Directorio Activo Microsoft u Open LDAP para crear reglas de control de acceso a través de VPN, empleando: usuarios, grupos de usuarios, maquinas, dirección IP y redes.		
5.1.83	El cliente VPN, debe instalarse sobre sistemas operativos Windows y Linux.		
5.1.84	Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado en sistema operativo Windows, que permita validar en base al nivel de cumplimiento (compliance) del host permitir, denegar o limitar el acceso a los recursos de la red interna. Por lo menos se deberá poder configurar los siguientes casos de uso siguientes: <ul style="list-style-type: none"> ▪ Software antivirus instalado y habilitado ▪ Software antivirus con la base de datos de firmas actualizada ▪ Parche de seguridad instalado o dispositivos vulnerables, según su nivel de criticidad ▪ Software de DLP instalado, el cual debe ser identificado a través de las llaves de registro o procesos del sistema operativo 		
5.1.85	La solución debe soportar autenticación de doble factor.		
Transferencia de conocimiento			
5.1.86	El proveedor deberá realzar la transferencia de conocimiento al personal de la DINI con respecto a la solución ofertada, incluyendo lo siguiente: <ul style="list-style-type: none"> • Temas: administración, configuración, monitoreo y formulación de reportes personalizadas, funcionalidades avanzadas, diagnóstico/troubleshooting, backup/restore de las configuraciones. • Cantidad: cinco (05) participantes. • 16 horas como mínimo siempre y cuando se cumpla con los temas solicitados y deben ser desarrollados antes de culminar la implementación de la solución ofertada. 		
ADMINISTRACIÓN			
5.1.87	La administración deberá ser centralizada de todos los componentes de la solución ofertada incluyendo el licenciamiento para tal fin. Se requiere que se tenga un equipo de administración y recolección, análisis de logs y generación de reportes, pudiendo separar ambos roles según recomendación del fabricante.		
5.1.88	Debe ser provisto en Appliance físico, es decir software y hardware provistos por el mismo fabricante.		
5.1.89	Debe ser del mismo fabricante de los firewalls.		

5.1.90	Debe contar con un almacenamiento mínimo de 4TB en RAID 1 o superior.		
5.1.91	Debe soportar una ingesta de 12 000 log por segundo como mínimo.		
5.1.92	La gestión de la solución debe soportar acceso por SSH, cliente o WEB (HTTPS).		
5.1.93	Debe permitir accesos concurrentes de al menos dos administradores.		
5.1.94	Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita o similar, acceso de lectura, cambio de configuraciones o similar;		
5.1.95	Generar alertas automáticas por Email, SNMP y Syslog		
5.1.96	Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horario.		
5.1.97	<p>La solución debe generar reportes personalizados, debiendo permitir al administrador determinar el contenido de los reportes con las siguientes funcionalidades:</p> <ul style="list-style-type: none"> • El contenido de los reportes deben incluir los datos en formato tabular (tablas) y/o gráficas (pie-chart, graph-chart) • Los reportes deben contar con la utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos. • Debe generar reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente o por destino. • Debe permite generar la incidencia de virus detectados y a nivel red por fuente o por destino. • Debe permitir personalizar los criterios bajo los cuales será obtenido el reporte, tales como fuentes, destinos, servicios, fechas y/o día de la semana. • Debe permitir especificar el periodo de tiempo específico para el cual el reporte va a ser obtenido. • Debe permitir enviar el reporte vía correo electrónico. <p>Los reportes serán parte del informe de implementación de la solución, no será parte de la fase de evaluación de las propuestas.</p>		

ANEXO N° 13

**DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS SERVICIOS PROFESIONALES DEL
FABRICANTE**

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 003-2024-DINI
Presente. -

De nuestra consideración:

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, declaro el cumplimiento de los servicios profesionales del fabricante para lo cual se adjunta el presente anexo mediante el cual el postor que suscribe declara:

La implementación debe ser validada por los servicios profesionales del fabricante y al finalizar la validación deberá emitir un informe de aplicación de mejores prácticas en la habilitación de todas las funcionalidades y aplicando las políticas de seguridad por cada funcionalidad. Se debe contemplar un mínimo de 4 días de los servicios profesionales del fabricante.

Al finalizar la implementación se requiere un informe de los servicios profesionales del fabricante.

Por otro lado, se aceptará que las actividades que realice este personal sean de manera remota siempre y cuando se cumpla con lo establecido en el numeral 5.1.12. del Capítulo III de las Bases del procedimiento de selección.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda**

PLIEGO DE ABSOLUCION DE CONSULTAS Y OBSERVACIONES

LICITACION PUBLICA N° 003-2024-DINI

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulacion	Sección	Numeral	Literal	Página	Consulta u Observacion	Analisis respecto de la consulta u observacion	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
1	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	3	3.1	19	Se solicita a la entidad confirmar por favor, si la instalación de los dos firewalls se debe realizar en el centro de datos Institucional? O el Firewall de Alta Disponibilidad se debe desplegar en un datacenter diferente? Por favor confirmar ciudades y direcciones de el/los centros de datos.	Se aclara que la instalación de los dos (2) firewall será en la Av. Edmundo Aguilar Sin Chornillos, la cual está indicada en las bases.	
2	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	3	3.1	19	Sírvase confirmar que la entidad suministrará en el centro de datos recursos como cableado de red (Cobre y fibra), puntos de datos y eléctricos, espacio en rack.	Se aclara que la entidad brindará los recursos como cableado de red (Cobre y fibra), puntos de datos y eléctricos, espacio en rack. Sin embargo, el contratista no elude la inclusión de todos los elementos necesarios para que los bienes/servicios ofertados funcionen correctamente de acuerdo a la modalidad llave en mano indicado en el punto 5.4.	
3	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	3	3.1	19	Basado en la consulta anterior, en caso de que el contratista tenga que suministrar cables de red (Cobre y fibra), indicar las distancias (rack, canaleta, bandejas, etc) desde los switches de red hacia la ubicación de rack que tendrán los dos firewalls.	Se aclara que la entidad brindará los recursos como cableado de red (Cobre y fibra). Sin embargo, el contratista no elude la inclusión de todos los elementos necesarios para que los bienes/servicios ofertados funcionen correctamente de acuerdo a la modalidad llave en mano indicado en el punto 5.4.	
4	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	5	5.1.13	20	Con la finalidad de poder hacer una estimación ajustada a las necesidades de la entidad, agradecemos por favor suministrar la siguiente información de la solución Checkpoint actual, para determinar el alcance de implementación: ¿Cantidad Total de Políticas a Configurar oNetworking oThreat Prevention oURL Filtering oDNS oQoS oVPN Client to Site oEtc. ¿Cantidad de Rutas ¿Cantidad VPN Site to Site ¿Cantidad de Redes ¿Cantidad de Reglas de Nat ¿Cantidad de Usuarios administradores	Se precisa que se tiene un aproximado de 500 políticas configuradas entre Networking, application control, nat, vpn site to site entre otros.	
5	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	5	5.1.20	21	¿De acuerdo con este numeral, es nuestro entendimiento que la entidad solo requiere puertos en cobre RJ45 y no requiere puertos SPF? En caso de que requiera puertos SPF, por favor indicar: ¿Cantidad interfaces SPF ¿Cantidad interfaces SPF+	Se aclara que lo requerido son puertos en cobre RJ45, los postores pueden proponer características superiores.	
6	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	5	5.1.86	24	Agradecemos a la entidad indicar si la transferencia de conocimiento debe ser dictada de forma presencial o remota.	Se aclara que la transferencia de conocimiento podrá ser realizada de forma presencial o remota considerando los temas especificados en las bases.	
7	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	5	5.1.87	24	Sírvase confirmar que solo se requiere un único appliance de Management.	Se aclara que se está solicitando como mínimo un Appliance Management que hará las funciones de administración y recolección en condiciones óptimas.	
8	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	5	5.6.1.5	26	Teniendo en cuenta que tradicionalmente los servicios de soporte se enfocan en la resolución de fallas y atención a consultas, por lo tanto, sírvase confirmar que la entidad requiere también de un servicio de administración para aplicación de configuración, casos de uso y mejora continua.	Se aclara que el soporte técnico que se está solicitando es de configuración, casos de uso y mejora continua de acuerdo a las bases.	

9	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	7	7 1 1 1 0	29	Agradecemos a la entidad indicar cuantas pruebas de disaster recovery y/o High viability se deben realizar durante la fase de implementación?	Se aclara que se debe realizar como minimo una prueba válida de disaster recovery y/o High viability una vez implementado la solución a fin de comprobar el funcionamiento	
10	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	1	1 9	14	Amablemente se informa a la entidad que en todas las plataformas de NGFW es estrictamente necesario y obligatorio contar con la licencia activada para poder iniciar con la implementación/configuración de los firewalls, motivo por el cual no es viable que la licencia sea activada desde el 22 de diciembre de 2024 como la entidad solicita Agradecemos por favor modificar este requerimiento de tal forma que la activación de la licencia sea desde el día de inicio de implementación (indicar fecha) hasta el 22 de diciembre 2027. O en su defecto, que la vigencia de la licencia sea de 3 años desde el día de inicio de implementación.	No se acoge lo solicitado, debido a que las licencias vence el 21 de diciembre de 2024 de acuerdo a lo establecido en las bases	
11	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	1	1 9	14	Entendiendo que se tiene como fecha límite de implementación el 21 de diciembre de 2024, agradecemos a la entidad indicar con que personal por parte de la entidad se asignara a este proyecto para garantizar la completa fluidez de las tareas durante la configuración y pruebas de la solución	Se aclara que los datos del personal por parte de la entidad será otorgado al inicio del contrato	
12	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	1	1 9	14	¿Entendiendo que se tiene como fecha límite de implementación el 21 de diciembre de 2024, agradecemos a la entidad indicar que sucedera con los retrasos en la implementación que sean generados por retrasos por parte de la entidad?	Se aclara que la entidad brindara las facilidades técnicas al contratistas a fin de no incurrir en retrasos	
13	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	5	5 1 97	25	Sírvase confirmar que en la implementación no se debe configurar ningún reporte personalizado, sino que en el informe final de implementación se debe entregar un listado de los reportes por defecto de la solución	No se acoge lo solicitado, es necesario para la entidad contar con el reporte personalizado de acuerdo a lo establecido en las bases	
14	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	2	2 2	16	h) Declaración Juada que indique ser representante y/o distribuidor y/o partner para la distribución y soporte de la solución ofertada En aras de garantizar información sustentatoria por parte del fabricante de la solución ofertada y considerando lo solicitado en el literal K de los requisitos para perfeccionar el contrato sírvase aceptar que para acreditar que el postor sea distribuidor autorizado sea tan solo con la carta del mismo fabricante	Se aclara que el postor podria presentar ademas de lo solicitado en las bases, la carta del fabricante que indique ser representante y/o distribuidor y/o partner para la distribución y soporte de la solución ofertada	
15	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	3 2	C 1	33	Respecto al perfil del jefe de proyecto sírvase confirmar que para acreditar la experiencia se aceptará constancia o certificado indicando el cargo de ¿Gerente de Proyecto¿ y/o ¿Project Manager¿	Se acoge lo indicado por el postor, se considerara Gerencia de Proyecto y/o Project Manager para acreditar la experiencia del personal clave requiendo como Jefe de Proyecto, debido a que existen diferentes nomenclaturas sobre el lider del proyecto	DICE: Experiencia minima de tres (3) años en implementaciones de sistemas de seguridad perimetral o de ciberseguridad del personal clave requiendo como JEFE DE PROYECTOS DEBE DECIR: Experiencia minima de tres (3) años en implementaciones de sistemas de seguridad perimetral o de ciberseguridad o Gerente de Proyecto y/o Project Manager del personal clave requiendo como JEFE DE PROYECTOS
16	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	6	6 1 2	27	Para fomentar una mayor pluralidad de postores, sírvase confirmar que para acreditar el grado academico del jefe de proyecto se aceptará Bachiller	No se acoge lo solicitado por el postor, se requiere que el personal clave requiendo como Jefe de Proyecto cuente con título profesional	
17	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	6	6 1 2	27	En aras de fomentar una mayor pluralidad de postores, sírvase confirmar que para los perfiles del personal especialista implementador y personal de soporte se pueden aceptar bachiller de electronica y de ingeniera de software como carreras afines	Se aclara que lo solicitado se dentro de las carreras afines	
18	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	6	6 1 2	27	En aras de fomentar una mayor pluralidad de postores, sírvase confirmar que para los perfiles del personal de especialista implementador y personal de soporte se podrá aceptar que un personal pueda desempeñar mas de un rol	Se acoge lo indicado por el postor, el personal clave requiendo como especialista implementador y soporte tecnico podrán ser desempeñados por el mismo personal, siempre y cuando el personal propuesto cumpla con el perfil solicitado y presente la documentación que sustenta el cumplimiento de cada perfil por separado. Se aceptara lo descrito debido a que la implementación y el soporte tecnico se dan en momentos diferentes	
19	20520967151	NEOSECURE SOCIEDAD ANONIMA CERRADA - NEOSECURE SAC	Consulta	Especifico	3 2	b	32	En aras de fomentar una mayor pluralidad de postores, sírvase confirmar que para acreditar la experiencia en bienes similares se aceptará las siguientes experiencias ¿Adquisición de Sistema de Protección y Seguridad para Red del Centro de Datos. ¿Sistema de protección y seguridad para red firewall NGFW ¿Implementación Mejoras de Seguridad Perimetral: Firewall de Nueva Generación ¿Solución Next Generation Firewall	Se acoge parcialmente lo solicitado, se aceptaran como bienes similares: Sistema de protección y seguridad para red firewall NGFW, implementación Mejoras de Seguridad Perimetral, Firewall de Nueva Generación, Solución Next Generation Firewall, por considerarse equivalentes al objeto de contratación	

20	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	2.2.1.1	h	16	Dado que resulta razonable requerir que el postor cuente con una relación comercial con el fabricante de la marca de la solución que oferta y en aras de que dicha solución pueda tener un tiempo previsible de duración -por mantenimientos y repuestos-, posibilidades de adecuación, integración o repotenciar si fuera necesario, en atención al Principio de Vigencia tecnológica, (Ver el literal g) del artículo 2 de la Ley) que es aplicable transversalmente a cualquier contratación estatal. Asimismo, dado que el Formato de Resumen Ejecutivo de las Actuaciones Preparatorias, la Entidad declaró la pluralidad de proveedores y/o marcas, en la capacidad de cumplir con el ítem del requerimiento, lo cual incluye la condición de representante, distribuidor o concesionario de la marca ofertada en el país o de empresa autorizada a comercializar la marca en el Perú por el fabricante de esta. Se solicita al Comité Especial incluir adjunta a la declaración Jurada que indique ser representante y/o distribuidor y/o partner para la distribución y soporte de la solución ofertada, la cual sustente la condición del postor y que esta condición tenga una vigencia no exceda los últimos seis (06) meses.	Se aclara que el postor podría presentar además de lo solicitado en las bases, la carta del fabricante que indique ser representante y/o distribuidor y/o partner para la distribución y soporte de la solución ofertada. Asimismo dicho documento es un requisito para el perfeccionamiento del contrato el cual deberá estar vigente.	
21	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	Específico	5.6.1	5.6.1.2	26	Dice ¿Soporte remoto para casos especializados y específicos que el área técnica lo amerite? Dado que el Principio de Transparencia, contempla el derecho a la información en la compra pública, el cual tiene esencialmente por objeto garantizar que no exista riesgo de favoritismo y arbitrariedad por parte de la Entidad convocante, para lo cual, se exige que todas las condiciones del procedimiento estén formuladas de forma clara, precisa e inequívoca en las Bases o en las respuestas brindadas en el pliego absolutorio, con el fin de que todos los postores razonablemente informados y normalmente diligentes puedan comprender su alcance exacto e interpretarlas de la misma forma. Dicho esto, se solicita al Comité Especial, que con motivo de la integración de bases se especifique y acote las actividades que se deberán considerar dentro del soporte remoto para los denominados casos especializados y específicos.	Se aclara que los casos especializados son los que el fabricante atienda, por lo tanto, se dará el acceso remoto.	
22	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	5.6	5.6.1.8	26	Dice ¿En los meses que no se cuente con atención por solicitudes de soporte técnico, el contratista debe brindar una charla de temas asociados a la plataforma acerca del uso y buenas prácticas de la solución de al menos dos (02) horas (¿)? Dado que, el Principio de Transparencia consignado en el literal c) del artículo 2 de la Ley establece que la Entidad debe proporcionar información clara y coherente con el fin que esta sea comprendida por todos los potenciales proveedores, se solicita al Comité Especial, que con motivo de la integración de bases se el número de personas que participaran en la charla de temas asociados a la plataforma acerca del uso y buenas prácticas de la solución y que esta charla solo se brindará dentro del horario laboral de la entidad.	Se aclara que la charla de 2 horas debe ser dentro del horario laboral en coordinación y aprobación del área técnica. Con respecto al número de personas que participaran en la charla, será como mínimo un (1) personal del área técnica.	
23	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	Específico	5.1	5.1.10	20	Se solicita a la entidad confirmar si el proceso de SSL o TLS se refiere específicamente al proceso de descifrado.	Se confirma que es para el proceso de descifrado al momento de detectar y bloquear virus y malware.	
24	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	5.1	5.1.25	21	Se solicita a la entidad confirmar, si el término 'prevención' hace referencia a 'bloqueo' de amenazas para el tráfico entrante y saliente.	Se aclara que el término de "prevención" es equivalente al "bloqueo".	
25	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	5.1	5.1.26	21	Se solicita a la entidad confirmar si con el término 'Web' hace referencia a 'HTTP'.	Se aclara que el término "Web" hace referencia a los protocolos de http y/o https que utiliza.	
26	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	5.1	5.1.27	21	DICE: Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real. Consulta: SE SOLICITA A LA ENTIDAD INDICAR SI LO SOLICITADO HACE REFERENCIA QUE SE REQUIERE QUE LOS NGFW BLOQUEEN ARCHIVOS MALICIOSOS.	Se aclara que el término de "prevenir" es equivalente al "bloqueo".	
27	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	5.1	5.1.42	22	Se solicita a la entidad confirmar, si el término 'geolocalización' puede referirse también a 'fuente geográfica' debido a que diferentes fabricantes tienen variación en la terminología.	Se aclara que los fabricantes manejan diferentes terminología, por lo tanto, el término de "geolocalización" es equivalente a "fuente geográfica".	
28	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	5.1	5.1.47	22	Se solicita a la entidad confirmar, si el término 'C&C' puede referirse también a 'C2' debido a que diferentes fabricantes tienen variación en la terminología.	Se aclara que los fabricantes manejan diferentes terminología, por lo tanto, se aclara que el término de "C&C" es equivalente a "C2".	
29	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	5.1	5.1.53	22	Se solicita a la entidad confirmar si el término 'IPS' (Intrusion Prevention System) se refiere específicamente al bloqueo de vulnerabilidades.	Se precisa que el IPS (sistema de prevención de intrusos) es bloqueo de vulnerabilidades o protección de vulnerabilidades.	

30	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	5 1	5 1 57	22	Se solicita a la entidad confirmar si con 'intentos de fuga de datos' pueden referirse hace referencia también como 'exfiltración de datos'	Se aclara que los fabricantes manejan diferentes terminología, por lo tanto, el término de "intentos de fuga de datos" es equivalente a "exfiltración de datos"	
31	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	5 1	5 1 64	23	Se solicita a la entidad confirmar si el término 'archivo emulado' hace referencia también como 'muestra analizada'	Se aclara que los fabricantes manejan diferentes terminología, por lo tanto, el término de "archivo emulado" es equivalente a "muestra analizada"	
32	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	5 1	5 1 66	23	Se solicita a la entidad confirmar si la detección de hypervisor debe aplicarse específicamente al malware y no al sandboxing	Se aclara que el malware no debe detectar o evadir al hypervisor del sandboxing, conforme a lo solicitado en las bases	
33	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	5 1	5 1 78	24	Se solicita a la entidad confirmar si los problemas de disco duro pueden estar relacionados con el consumo del mismo	Se aclara que lo solicitado en el numeral 5.1.78 de las bases refiere a las alertas en caso existan problemas de salud en el equipo, la misma que contempla el consumo de disco duro	
34	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	5 1	5 1 96	25	Se solicita a la entidad confirmar si se aceptarán soluciones que permitan guardar un backup automático de configuración de todos los cambios que se vayan realizando en los firewall	Se aclara que lo que se está solicitando en las bases son características mínimas, los postores pueden proponer características superiores	
35	20607015130	PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C. - PLATECCS S.A.C.	Consulta	General	6 1	6 1 2	27	Se solicita al comité especial aclarar que las certificaciones del Personal Especialista Implementador y Personal de Soporte deberán estar vigentes y no se aceptarán certificaciones con fecha de vencimiento anteriores al proceso y/o certificaciones caducadas	Se aclara que la certificación de la solución ofertada debe de estar vigente	
36	20516530686	GRUPO ELECTRODATA S.A.C.	Consulta	Específico	5 1 86		24	Dice: El proveedor deberá realizar la transferencia de conocimiento al personal de la DINI con respecto a la solución ofertada, incluyendo lo siguiente: ¿Temas: administración, configuración, monitoreo y formulación de reportes personalizadas, funcionalidades avanzadas, diagnóstico/troubleshooting, backup/restore de las configuraciones ¿Cantidad: cinco (05) participantes ¿16 horas como mínimo siempre y cuando se cumpla con los temas solicitados y deben ser desarrollados antes de culminar la implementación de la solución ofertada Consulta: Sirvase a confirmar que la transferencia de conocimientos podrá ser brindada de manera remota, lo solicitado se basa en el Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones	Se aclara que la transferencia de conocimiento podrá ser realizada de forma presencial o remota considerando los temas especificados en las bases	
37	20516530686	GRUPO ELECTRODATA S.A.C.	Consulta	Específico	5 6 1 5		26	Dice: El soporte técnico debe incluir la actualización y configuración de nuevas versiones liberadas por el fabricante, así como configuraciones, casos de uso, y mejora continua del sistema en base a buenas prácticas del fabricante, durante la vigencia del contrato. En caso se cuente con incidentes como consecuencia de realizar actualizaciones, upgrades o averías de software al momento del soporte técnico de la solución ofertada, el contratista tendrá un plazo máximo de dos (2) horas para la restauración de la información del servicio relacionado solo a la solución propuesta y no a la plataforma de correo o la información contenida en esta, la misma que se registrará en la hoja de visita técnica del contratista o correo electrónico Consulta: Sirvase a confirmar, que el plazo no aplicará en caso el incidente requiera ser escalado con el fabricante, ya que su Centro de atención técnica cuenta con un SLA de atención mas no de resolución, lo solicitado se basa en el Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones	Se aclara que el incidente debe ser atendido en los tiempos solicitados, sin embargo, en caso el incidente sea escalado con el fabricante y no cuenten con una resolución el contratista deberá proporcionar el ticket de escalamiento para realizar el seguimiento respectivo	
38	20516530686	GRUPO ELECTRODATA S.A.C.	Consulta	Específico	5 6 1 5		26	Dice: El tiempo máximo para la atención de incidentes será de 3 horas y para resolver la avería será de 3 horas posteriores como máximo, será contabilizado desde que el contratista tome conocimiento del incidente reportado (Interrupción del servicio y demora en la restauración de la información del servicio). Este tiempo no aplicará para los casos que sea necesario cambio de partes que impliquen mayor tiempo de reposición física de la pieza o repuesto afectado Consulta: Sirvase a confirmar, que el plazo no aplicará en caso el incidente requiera ser escalado con el fabricante, ya que su Centro de atención técnica cuenta con un SLA de atención mas no de resolución, lo solicitado se basa en el Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones	Se aclara que el incidente debe ser atendido en los tiempos solicitados, sin embargo, en caso el incidente sea escalado con el fabricante y no cuenten con una resolución el contratista deberá proporcionar el ticket de escalamiento para realizar el seguimiento respectivo	

39	20516530686	GRUPO ELECTRODATA S A C	Consulta	Específico	6 1 2	II	27	<p>Dice</p> <p>Personal Especialista implementador</p> <p>I Actividades</p> <p>Para la prestación Principal. Implementará la solución propuesta. migrara las políticas de todos los módulos del firewall actual (CheckPoint 5800 pudiendo afectar servicios en un horario controlado no mayor a 1 hora por caso de migración) a los nuevos equipos. formulará y firmará el informe respectivo.</p> <p>II Perfil</p> <p>El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas</p> <p>Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines. quienes debe contar con la certificación en la solución ofertada a nivel profesional o experto o ingeniero o superior brinda por la marca ofertada. Además. deben contar con experiencia mínima de dos (02) años en implementación. migración y soporte de la solución propuesta</p> <p>Consulta. A fin de permitir mayor pluralidad de postores. sirvase a confirmar que se aceptarán como carreras afines las siguientes.</p> <ul style="list-style-type: none"> - Bachiller en Ingeniería de Sistemas e Informática - Bachiller en Computación e Informática - Bachiller en Ingeniería Electrónica - Profesional Técnico en Ingeniería de Redes y Comunicaciones. Lo solicitado se basa en el Art. 2 de la Ley de Contrataciones del Estado. de conformidad con el literal a) Principio de Libre Concurrencia. literal b) Principio de Igualdad de Trato. como también Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones 	Se confirma que lo solicitado por el postor se encuentra considerado como carreras afines	
40	20516530686	GRUPO ELECTRODATA S A C	Consulta	Específico	6 1 2	II	27	<p>Dice</p> <p>Personal de Soporte</p> <p>I Actividades</p> <p>Para la prestación Accesorio. Brindará el soporte técnico a la solución implementada. emitirá y firmará el informe respectivo.</p> <p>II Perfil</p> <p>El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas</p> <p>Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines. quienes debe contar con la certificación en la solución ofertada a nivel profesional o experto o ingeniero o superior brinda por la marca ofertada. Además. deben contar con experiencia mínima de dos (02) años en soporte de la solución propuesta</p> <p>Consulta. A fin de permitir mayor pluralidad de postores. sirvase a confirmar que se aceptarán como carreras afines las siguientes.</p> <ul style="list-style-type: none"> - Bachiller en Ingeniería de Sistemas e Informática - Bachiller en Computación e Informática - Bachiller en Ingeniería Electrónica - Profesional Técnico en Ingeniería de Redes y Comunicaciones. Lo solicitado se basa en el Art. 2 de la Ley de Contrataciones del Estado. de conformidad con el literal a) Principio de Libre Concurrencia. literal b) Principio de Igualdad de Trato. como también Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones 	Se confirma que lo solicitado por el postor se encuentra considerado como carreras afines	

41	20516530686	GRUPO ELECTRODATA S A C	Consulta	Especifico	6 1 2	II	27	<p>Dice: Personal Especialista implementador</p> <p>i. Actividades Para la prestación Principal, implementará la solución propuesta, migrará las políticas de todos los módulos del firewall actual (CheckPoint 5800) pudiendo afectar servicios en un horario controlado no mayor a 1 hora por caso de migración) a los nuevos equipos, formulará y firmará el informe respectivo.</p> <p>ii. Perfil El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines, quienes debe contar con la certificación en la solución ofertada a nivel profesional o experto o ingeniero o superior brinda por la marca ofertada. Además, deben contar con experiencia mínima de dos (02) años en implementación, migración y soporte de la solución propuesta.</p> <p>Personal de Soporte 1. Actividades Para la prestación Accesorio, Brindará el soporte técnico a la solución implementada, emitirá y firmará el informe respectivo.</p> <p>ii. Perfil El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines, quienes debe contar con la certificación en la solución ofertada a nivel profesional o experto o ingeniero o superior brinda por la marca ofertada. Además, deben contar con experiencia mínima de dos (02) años en soporte de la solución propuesta.</p> <p>Consulta: Sirvase confirmar que, a fin de permitir una mayor pluralidad de postores, se aceptará que el personal especialista implementador sea el mismo que el personal de Soporte, siempre y cuando cumpla con el perfil solicitado. Teniendo en cuenta que la etapa de Soporte Técnico (Prestación Accesorio) es posterior a la etapa de implementación (Prestación Principal), lo solicitado se basa en el Art. 2 de la Ley de Contrataciones del Estado, de conformidad con el literal a) Principio de Libre Concurrencia, literal b) Principio de Igualdad de Trato, como también Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones.</p>	Se acoge lo indicado por el postor, el personal clave requerido como especialista implementador y soporte técnico podrán ser desempeñados por el mismo personal, siempre y cuando el personal propuesto cumpla con el perfil solicitado y presente la documentación que sustenta el cumplimiento de cada perfil por separado. Se aceptará lo descrito debido a que la implementación y el soporte técnico se dan en momentos diferentes.	
42	20516530686	GRUPO ELECTRODATA S A C	Consulta	Especifico	7 6 2 1		30	<p>Dice: Por interrupción del servicio por averías en la solución mayor a tres (03) horas. Se considera como consecuencia de un incidente que afecta la operatividad de la solución afectando a los usuarios que lo utilizan. Se considera desde la notificación al Contratista por parte del área usuaria posteriores a las solicitudes de soporte técnico mayor a 3 horas para la atención.</p> <p>Procedimiento ¿ El área usuaria detecta interrupción del servicio y solicita atención al contratista a través de llamada telefónica o correo electrónico a su centro de atención u otros correos que proporcione el Contratista ¿ En caso de pasado tres (03) horas continuas con la interrupción del servicio, se informará al área de Logística para la aplicación de la penalidad correspondiente.</p> <p>Consulta: Sirvase a confirmar que el plazo no aplicará en caso el incidente requiera ser escalado con el fabricante, ya que su Centro de atención técnica cuenta con un SLA de atención mas no de resolución, lo solicitado se basa en el Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones.</p>	Se aclara que las averías debe ser atendido en los tiempos solicitados, sin embargo, en caso la avería sea escalado con el fabricante y no cuenten con una resolución el contratista deberá proporcionar el ticket de escalamiento para realizar el seguimiento respectivo.	
43	20516530686	GRUPO ELECTRODATA S A C	Consulta	Especifico	7 6 2 1		30	<p>Dice: Por problemas en la restauración de la información del servicio mayor a dos (02) horas. Se aplicará como consecuencia de realizar actualizaciones, upgrades o averías de software al momento del soporte técnico de la solución ofertada.</p> <p>Procedimiento ¿ El área usuaria determina que la solución no cuenta con la configuración que permita el correcto funcionamiento del mismo. ¿ El área usuaria comunica el incidente al contratista, quien se encuentra realizando actividades sobre la solución, a partir de este momento se contabiliza el tiempo.</p> <p>En caso de que el contratista no pueda resolver el incidente dentro del plazo de dos (02) horas, se registrará la observación en la hoja de visita técnica del contratista o correo electrónico y se informará al área de Logística para la aplicación de la penalidad correspondiente.</p> <p>Consulta: Sirvase a confirmar, que el plazo no aplicará en caso el incidente requiera ser escalado con el fabricante, ya que su Centro de atención técnica cuenta con un SLA de atención mas no de resolución, lo solicitado se basa en el Art. 2 de la Ley de Contrataciones del Estado, de conformidad con el literal a) Principio de Libre Concurrencia, literal b) Principio de Igualdad de Trato, como también Artículo 16 numeral 16.1 y 16.2 de la ley de Contrataciones del Estado en concordancia con el Artículo 29 numeral 29.3 del Reglamento de la Ley de Contrataciones.</p>	Se aclara que los problemas en la restauración de la información debe ser atendido en los tiempos solicitados, sin embargo, en caso el incidente sea escalado con el fabricante y no cuenten con una resolución el contratista deberá proporcionar el ticket de escalamiento para realizar el seguimiento respectivo.	

44	20113277964	JAPAN COMPUTER SERVICE S A C	Observación	Especifico	2 2 1 1	J	16	<p>"Dentro de la documentación para la admisión de la oferta se solicita: """) Declaración jurada para acreditar el sustento técnico de la solución propuesta (Anexo N° 12). Indicar en la oferta el cumplimiento de las especificaciones técnicas mínimas requeridas, lo cual evidenciara en la documentación técnica (indicar el folio específico) del sustento (folletos, instructivos, catálogos o similares de fuentes del fabricante) que demuestre el cumplimiento de las mismas (no direcciones de sitios ni links), así como su descripción detallada en forma resaltada. Podiendo presentar los documentos en su idioma original junto con su traducción simple al castellano en caso de encontrarse en lengua extranjera. Las cartas del fabricante no podrán emplearse para el sustento técnico""</p> <p>En atención a ello, cabe señalar que, en las Bases Estandar aplicables al objeto de la convocatoria se ha establecido que, las especificaciones técnicas se acreditan con la ¿Declaración Jurada de cumplimiento de las Especificaciones Técnicas¿ (Anexo N° 3), siendo que, se podría afianzar la acreditación de algunas especificaciones técnicas del requerimiento a través de la presentación adicional folletos, instructivos, catálogos o similares, para lo cual la Entidad debe especificar con claridad qué aspectos de las características y/o requisitos funcionales serán acreditados con la documentación requerida</p> <p>OBSERVACIÓN</p> <p>En concordancia con lo establecido en la Resolución N° 2034-2018-TCE-S1, el Tribunal de Contrataciones del Estado ha establecido lo siguiente: ¿() no es posible acreditar la totalidad de especificaciones técnicas del bien ofertado con hojas técnicas, catálogos, brochures y manuales de fabricante, ello atendiendo a que la información requerida por las entidades no es homogénea y obedece a las particularidades de su necesidad¿</p> <p>Por lo tanto, debido a que NO es posible acreditar la totalidad de las especificaciones técnicas, sírvase indicar cuáles serán los puntos técnicos obligatorios a sustentar de forma detallada y documentada dentro de los ítems (5 1 1 al 5 1 97) de las Especificaciones Técnicas. Asimismo, sírvase a modificar el ANEXO N°12 de acuerdo a esta respuesta</p> <p>"</p>	<p>Se aclara que los puntos técnicos obligatorios a sustentar de forma detallada y documentada son todos los puntos solicitados en la 5 1 de las bases a excepción de los siguientes (5 1 1, 5 1 3, 5 1 5, 5 1 12, 5 1 13, 5 1 14, 5 1 45, 5 1 61, 5 1 70, 5 1 79, 5 1 81, 5 1 86, 5 1 87, 5 1 95, 5 1 96, 5 1 97), sin embargo deberá indicar el cumplimiento de las mismas en el Anexo N° 12</p>	
45	20113277964	JAPAN COMPUTER SERVICE S A C	Consulta	Especifico	5 1 86	-	24	<p>"Pag 24 Numeral 5 1 86 El proveedor deberá realizar la transferencia de conocimiento al personal de la DiNI con respecto a la solución ofertada incluyendo lo siguiente: ¿Temas administración, configuración, monitoreo y formulación de reportes personalizadas, funcionalidades avanzadas, diagnóstico/troubleshooting, backup/restore de las configuraciones ¿Cantidad: cinco (05) participantes ¿16 horas como mínimo siempre y cuando se cumpla con los temas solicitados y deben ser desarrollados antes de culminar la implementación de la solución ofertada Consulta En aras de brindar flexibilidad de horarios al personal de la entidad para la transferencia de conocimientos en mención sírvase confirmar que el presente servicio podrá darse de forma remota "</p>	<p>Se aclara que la transferencia de conocimiento podrá ser realizada de forma presencial o remota considerando los temas especificados en las bases</p>	
46	20113277964	JAPAN COMPUTER SERVICE S A C	Observación	Especifico	5 6 1 7	-	26	<p>"Pag 26 Numeral 5 6 1 7 Dice El tiempo máximo para la solución de incidentes será de 3 horas y para resolver la avería será de 3 horas posteriores como máximo, será contabilizado desde que el contratista tome conocimiento del incidente reportado (Interrupción del servicio y demora en la restauración de la información del servicio). Este tiempo no aplicará para los casos que sea necesario cambio de partes que impliquen mayor tiempo de reposición física de la pieza o repuesto afectado Observación Si bien el contratista se compromete a ir escalando el incidente en nivel de severidad y especialización de personal si la solución del mismo no es favorable y dado que la solución de un incidente depende mucho de la naturaleza del problema no existe un tiempo mínimo de resolución que pueda establecerse en el caso que la causa del problema sea por un sistema del cliente independiente a la seguridad perimetral, ello tomando en cuenta que el soporte del fabricante y del contratista sólo cubre la solución de Firewall ofertada"</p>	<p>Se aclara que el incidente debe ser atendido en los tiempos solicitados, sin embargo, en caso el incidente sea escalado con el fabricante y no cuenten con una resolución el contratista deberá proporcionar el ticket de escalamiento para realizar el seguimiento respectivo</p>	
47	20113277964	JAPAN COMPUTER SERVICE S A C	Consulta	Especifico	6 1	-	27	<p>""EN BASES INDICAN PERSONAL DE SOPORTE CONSULTA Considerando que la implementación y el soporte NO se brindarán en simultáneo, sírvase confirmar que el rol del PERSONAL DE SOPORTE podrá ser cubierto por el rol del ESPECIALISTA IMPLEMENTADOR, siempre y cuando dicha persona cumpla con las certificaciones y experiencia requerida para ambos perfiles ""</p> <p>Es decir, se podrá presentar 2 personas que cubran con el rol de Implementador y también el de Soporte, siempre y cuando cumplan con los requisitos de ambos perfiles "</p>	<p>Se acoge lo indicado por el postor, el personal clave requiendo como especialista implementador y soporte técnico podrán ser desempeñados por el mismo personal, siempre y cuando el personal propuesto cumpla con el perfil solicitado y presente la documentación que sustenta el cumplimiento de cada perfil por separado. Se aceptará lo descrito debido a que la implementación y el soporte técnico se dan en momentos diferentes</p>	

48	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 3	0	19	<p>Dice</p> <p>El hardware ofertado deberá ser totalmente nuevo</p> <p>Consulta</p> <p>De acuerdo con lo solicitado, no es posible proporcionar sustento mediante documentación o información de dominio público</p> <p>Por lo tanto, se solicita a la entidad aceptar la sustentación de este a través de una declaración jurada del postor o carta del mayorista</p>	Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases	
49	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 5	0	19	<p>Dice</p> <p>El sistema operativo deberá ser del fabricante de la solución ofertada, el mismo deberá venir de fábrica con el "hardening" necesario, el fabricante deberá desarrollar las actualizaciones de sistema operativo, parches del software o módulos utilizados por la solución ofertada</p> <p>Consulta</p> <p>De acuerdo con lo solicitado, no es posible proporcionar sustento mediante documentación o información de dominio público</p> <p>Por lo tanto, se solicita a la entidad aceptar la sustentación de este a través de una declaración jurada del postor o carta del fabricante</p>	Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases	
50	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 7	0	20	<p>Dice</p> <p>El fabricante de la solución de seguridad debe estar presente en los últimos 8 reportes de Gartner (Magic Quadrant), en el cuadrante de Líderes para Network Enterprise Firewalls</p> <p>Consulta/Observación:</p> <p>Entendemos que los reportes de analistas como Gartner, no suele ser documentación o información de dominio público. Para lograr tener acceso a esta información, se necesita llenar un formulario y realizar un pago</p> <p>Dicho lo anterior, se solicita a la entidad confirmar que se aceptarán link o enlaces de páginas web en la cual se valide que el fabricante cumple con lo solicitado, o en su defecto considerarlo como opcional</p>	No se acoge lo solicitado por el postor, dejarse a lo requerido en las bases	
51	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 9	0	20	<p>Dice</p> <p>Los sistemas operativos que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas. Esto se aplicará únicamente al Sistema Operativo o firmware que se instalará en la entidad sobre los equipos propuestos por el postor</p> <p>Consulta</p> <p>Los fabricantes publican regularmente las vulnerabilidades detectadas en las distintas versiones de sus sistemas operativos. Con el objetivo de mantener a los usuarios informados y al día, esta información se actualiza continuamente en una página web pública</p> <p>Dicho lo anterior, se solicita confirmar que se podrá presentar el link de la página web donde el fabricante publica las vulnerabilidades sobre las versiones de sus sistemas operativos, con una impresión de esta, caso contrario se podrá sustentar mediante carta de fabricante o declaración jurada</p>	Se aclara que bastaría con presentar en el Anexo N° 12 un sustento con un documento impreso de la página web considerando que las vulnerabilidades (CVE) son de información pública	

52	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5.1.10	0	20	<p>Dice:</p> <p>El sistema debe estar habilitado y configurado con las políticas de todas las funcionalidades</p> <p>¿ Firewall</p> <p>¿ Control de aplicaciones</p> <p>¿ Sistema de Prevención de Intrusos (IPS)</p> <p>¿ Antivirus o Antimalware</p> <p>¿ Emulación de amenazas (Sandbox)</p> <p>¿ Filtrado de comando y control, antibot o antispysware</p> <p>¿ DNS Security</p> <p>Que permita detectar y bloquear (prevenir) virus y malware que se propaguen, al menos, en los siguientes protocolos: HTTP, FTP, SMB, SMTP, IMAP, POP3 y SSL o TLS, que cubran finalmente el objetivo requerido</p> <p>Consulta</p> <p>Se solicita a la entidad confirmar si al referirse a SSL o TLS hace referencia al proceso de desencriptación que realiza el firewall para tener visibilidad del tráfico cifrado</p>	Se confirma que es para el proceso de descifrado al momento de detectar y bloquear virus y malware	
53	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5.1.13	0	20	<p>Dice:</p> <p>El proveedor deberá considerar en la implementación los servicios de Networking necesario para la implementación (configuración del core, Switches, reglas en firewall perimetral e interno y aplicación de buenas prácticas para la convivencia de la red externa con la interna)</p> <p>Consulta:</p> <p>Debido que el requerimiento no hace referencia a ninguna tecnología de parte del fabricante, no se podría sustentar con documentación pública el requerimiento</p> <p>Dicho lo anterior, se solicita a la entidad que se pueda sustentar el requerimiento con una declaración jurada del postor</p>	Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases	
54	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5.1.14	0	20	<p>Dice:</p> <p>El nivel de soporte del fabricante debe ser 24 x 7 durante el periodo del contrato. Debiendo ser asistido por el propio personal del fabricante a través de su propio centro de atención, y en coordinación directa con el contratista para el seguimiento y escalamiento de los requerimientos</p> <p>Consulta:</p> <p>Debido que no se encuentra sustento de documentación pública donde se indique que el postor debe de tenerse una coordinación con el contratista para el seguimiento y escalamientos de los requerimientos</p> <p>Dicho lo anterior, se solicita a la entidad que se pueda sustentar con documentación del servicio de soporte del fabricante y una declaración jurada que sustente lo siguiente: ¿Debiendo ser asistido por el propio personal del fabricante a través de su propio centro de atención, y en coordinación directa con el contratista para el seguimiento y escalamiento de los requerimientos?</p>	Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases	
55	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5.1.18	0	21	<p>Dice:</p> <p>Cada equipo deberá contar con dos fuentes de poder de 100-240 VAC 50-60 Hz</p> <p>Consulta:</p> <p>Se solicita a la entidad que se pueda acompañar al documento de sustento la lista de materiales para referenciar que se cuenta con dos fuentes poder, con la finalidad de reforzar el sustento de lo requerido</p>	Se aclara que el postor en caso considere conveniente podría adicionalmente indicar el número de parte o similar con la ficha técnica o documentación que la sustenta	

56	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 19	0	21	<p>Dice</p> <p>Las fuentes de poder podrian ser de tipo hot-swap (cambio en caliente)</p> <p>Consulta</p> <p>Se solicita a la entidad aclarar que al referirse a hot-swap (cambio en caliente) hace referencia a que se realizara el remplazo de una fuente poder sin generar una interrupción de servicio.</p>	Se aclara que las fuentes de poder de tipo hot-swap (cambio en caliente) son opcionales	
57	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 20	0	21	<p>Dice</p> <p>Cada equipo debera tener como minimo 8 interfaces de cobre GE RJ45</p> <p>Consulta</p> <p>Se solicita a la entidad confirmar que se aceptaran los terminos interfaces de cobre GE o puertos RJ45</p>	Se aclara que lo que los terminos de "cobre GE o puertos RJ45" es equivalente al "GE RJ45"	
58	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 24	0	21	<p>Dice</p> <p>Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en tiempo real en el repositorio la clasificación y/o reputación de direcciones IP y/o Dominios y/o URL y/o redes de C2 o Comando y Control, y/o ataques DoS</p> <p>Consulta:</p> <p>Con la finalidad de brindar el mejor sustento tecnico para el entendimiento de la entidad, se solicita a la entidad confirmar si se aceptaran terminos similares como</p> <p>Repositorio de inteligencia de amenazas en nube del propio fabricante o servicio en nube de prevención avanzada de amenazas</p>	Se aclara que lo solicitado es equivalente al repositorio de inteligencia de amenazas en nube, tener en cuenta que debe ser del propio fabricante	
59	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 25	0	21	<p>Dice</p> <p>La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente</p> <p>Consulta</p> <p>Se solicita a la entidad confirmar, que se aceptaran los terminos de entrante y saliente o carga y descarga</p>	Se aclara que el termino de "entrante y saliente" es equivalente al "carga y descarga"	
60	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 26	0	21	<p>Dice</p> <p>Debera realizar analisis de malware y bloquearlos en al menos los siguientes protocolos: Web, Mail (SMTP o POP3), SMB, FTP y SSL o TLS</p> <p>Consulta</p> <p>Debido que web no es un protocolo, la entidad estaria generando una confusion con lo requerido, con la finalidad de brindar el mejor sustento posible, se solicita a la entidad aclarar que, al indicar Web, hace referencia a los protocolos HTTP y/o HTTPS</p>	Se aclara que el termino "Web" hace referencia a los protocolos de http y/o https que utiliza	
61	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 27	0	21	<p>Dice</p> <p>Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real</p> <p>Consulta</p> <p>Las soluciones de Next Generation Firewall o Firewall, no realizan la prevención de la infección de archivos, lo que hace esta es bloquear el tráfico de archivos maliciosos.</p> <p>Dicho lo anterior, se solicita a la entidad aclarar si se requiere que la solución brinde bloqueo de archivos maliciosos como (Word, Excel, PowerPoint, PDF) en tiempo real</p>	Se aclara que el termino de "prevenir" es equivalente al "bloqueo"	

62	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 28	0	21	<p>Dice</p> <p>La identificación de amenazas avanzadas camufladas en tráfico DNS deberá contar con mecanismos avanzados de detección con el objetivo de identificar ataques imposibles de mitigar con firmas y/o reputación del dominio. Para ello se requiere que el tráfico DNS sea analizado con técnicas de inteligencia artificial y/o análisis predictivo y/o machine learning en tiempo real.</p> <p>Consulta</p> <p>Se solicita a la entidad confirmar que se aceptarán fabricantes que cuenten con identificación de amenazas avanzadas camufladas en tráfico DNS que deberá contar con mecanismos avanzados y/o múltiples fuentes de detección con el objetivo de identificar ataques imposibles de mitigar con firmas y/o reputación del dominio. Para ello se requiere que el tráfico DNS sea analizado con técnicas de inteligencia artificial y/o análisis predictivo y/o machine learning en tiempo real.</p>	Se aclara que lo que se está solicitando en las bases son características mínimas, los postores pueden proponer características superiores.	
63	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 29	0	21	<p>Dice</p> <p>Debe soportar Inspección de tráfico cifrado/encryptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).</p> <p>Consulta</p> <p>Debido que se comprende que HTTPS es el protocolo utilizado para la navegación web, se solicita a la entidad confirmar que se aceptarán soluciones que soporten inspección de tráfico cifrado/encryptado sobre protocolo HTTPS o web o servidor web, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).</p>	Se aclara que lo que se está solicitando en las bases son características mínimas, los postores pueden proponer características superiores.	
64	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 30	0	21	<p>Dice</p> <p>Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware.</p> <p>Consulta</p> <p>Entendemos que lo solicitado, se refiere a el bloqueo de sitios web categorizado y/o identificados como malware.</p> <p>Dicho lo anterior, se solicita a la entidad confirmar que el punto hace referencia al bloqueo de sitios web categorizados como malware permitiendo mitigar el riesgo asociado a estos sitios.</p>	Se aclara que el término de "bloqueo de sitios web categorizados" es equivalente al punto 5 1 30.	
65	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 32	0	21	<p>Dice</p> <p>Debe tener capacidad de integración con fuente de IoC de terceros (External IoC) a través de direcciones web URL, con capacidades de detección y prevención o listas dinámicas externa, siempre y cuando se cumpla con el requerimiento solicitado. La aplicación y prevención de seguridad, en base a los IoC o listas dinámicas externa incluidos, debe ser de manera automática, sin interacción del usuario administrador una vez aplicada a una política de seguridad.</p> <p>Consulta</p> <p>De acuerdo con lo solicitado, no es posible proporcionar sustento mediante documentación o información de dominio público.</p> <p>Por lo tanto, se solicita a la entidad aceptar la sustentación de este a través de una declaración jurada del postor o carta del mayorista.</p>	No se acoge, deberá ceñirse a lo indicado en las bases, esta característica de seguridad debe tener el sustento técnico.	
66	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 39	0	22	<p>Dice</p> <p>Los firewalls deben soportar como mínimo 1 024 VLANs tags 802 3ad.</p> <p>Consulta</p> <p>Se solicita a la entidad aclarar que el requerimiento consta de que la solución debe soportar mínimo 1 024 VLANs tags y 802 3ad, debido que son dos temas diferentes.</p>	Se aclara que lo referido en el numeral 5 1 39 son dos temas diferentes.	

67	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 42	0	22	<p>Dice</p> <p>Soportar la creación de políticas basadas en Geolocalización, configurando que el tráfico de determinado Pais y/o Países sean bloqueados o permitidos</p> <p>Consulta</p> <p>Con la finalidad de brindar el mejor sustento posible, se solicita a la entidad confirmar que se aceptarán los términos de geolocalización o fuente geográfica</p>	Se entiende que los fabricantes manejan diferentes terminología. Por lo tanto, se aclara que el término de "geolocalización" es equivalente a "fuente geográfica"	
68	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 45	0	22	<p>Dice</p> <p>Las actualizaciones de las direcciones o rangos de IP publica por cada pais, debe realizarse periódicamente y de manera automática</p> <p>Consulta</p> <p>Debido que no se cuenta con documentación publica la cual indique lo requerido, se solicita a la entidad confirmar que se aceptará como sustento una carta de fabricante o declaración jurada del postor para este requerimiento</p>	Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases	
69	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 47	0	22	<p>Dice</p> <p>A nivel de aplicación, debe incluir protecciones tipo Cross Site Scripting y/o SQL Injection y/o Command Injection e injection protection para DN (Distinguished Names) y/o C&C desconocidos</p> <p>Consulta</p> <p>Con la finalidad de no generar confusiones a la entidad con la terminología propuesta por cada fabricante, se solicita a la entidad confirmar que se aceptarán los términos C&C o C2 desconocidos</p>	Se entiende que los fabricantes manejan diferentes terminología. Por lo tanto, se aclara que el término de "C&C" es equivalente a "C2 desconocidos"	
70	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 50	0	22	<p>Dice</p> <p>Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos</p> <p>Consulta</p> <p>Se solicita a la entidad confirmar que se aceptarán soluciones que detecten y bloqueen tráfico o url relacionadas a peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos o elude puerto</p>	Se aclara que lo que se está solicitando en las bases son características mínimas, los postores pueden proponer características superiores	
71	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 52	0	22	<p>Dice</p> <p>Debe permitir adicionar excepciones a las protecciones de IPS</p> <p>Consulta</p> <p>Debido que una excepción de protección de IPS se realizaría básicamente realizando excepciones a ciertas firmas para omitir la protección de estas</p> <p>Dicho lo anterior, se solicita a la entidad confirmar que se aceptarán soluciones que permitan adicionar excepciones a las protecciones de IPS o firmas de amenazas</p>	Se aclara que lo señalado por el postor refiere a terminologías equivalentes	
72	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 53	0	22	<p>Dice</p> <p>Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense</p> <p>Consulta</p> <p>Con la finalidad de brindar un mejor sustento técnico, no todos los fabricantes cuentan la denominación de IPS para la funcionalidad requerida, en algunos casos se utiliza la denominación protección de vulnerabilidades</p> <p>Dicho lo anterior, se solicita a la entidad confirmar que se aceptará soluciones que deban capturar paquetes automáticamente de eventos de IPS o protección de vulnerabilidades para proveer un mejor análisis forense</p>	Se aclara que esta característica de seguridad debe tener el sustento técnico, muy independientemente de las terminologías de cada fabricante	

73	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 54	0	22	<p>Dice</p> <p>Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos o ataques conocidos.</p> <p>Consulta</p> <p>Debido que, para realizar una prevención de una vulnerabilidad, se debe primero detectar esta, caso contrario, no se sabría que prevenir.</p> <p>Dicho lo anterior, se solicita a la entidad confirmar que se aceptarán soluciones que realicen la prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos o ataques conocidos.</p>	<p>Definirse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico.</p>	
74	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 55	0	22	<p>Dice</p> <p>Detección y prevención del uso indebido de un protocolo o ataques no basados en protocolos IP, para actividad maliciosa o amenaza potencial.</p> <p>Consulta</p> <p>Se comprende que el término prevención difiere de acciones, las cuales se pueden realizar para cumplir el término de prevención, la acción de bloqueo es una manera de prevenir.</p> <p>Dicho lo anterior, se solicita a la entidad confirmar si se aceptarán soluciones que cuenten con la capacidad de Detección y prevención o bloqueo del uso indebido de un protocolo o ataques no basados en protocolos IP, para actividad maliciosa o amenaza potencial.</p>	<p>Definirse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico, teniendo en cuenta que el término "prevención" es equivalente a "bloqueo".</p>	
75	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 57	0	22	<p>Dice</p> <p>Detección y prevención de intentos de tunelización, para intentos de fuga de datos o intentos de eludir otras medidas de seguridad, como el filtrado web.</p> <p>Consulta</p> <p>Se solicita a la entidad confirmar si se aceptarán los términos fuga de datos o exfiltración de datos o robo de datos.</p>	<p>Se aclara que los términos "o exfiltración de datos o robo de datos" es equivalente al término "fuga de datos".</p>	
76	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 64	0	23	<p>Dice</p> <p>Cada archivo emulado en el sandbox debe generar un reporte detallado que incluya información forense sobre la actividad maliciosa originada por el archivo.</p> <p>Consulta</p> <p>Se solicita a la entidad confirmar si se aceptarán los términos archivo emulado o muestra analizada siempre y cuando se encuentre en el mismo contexto.</p>	<p>Se aclara que los fabricantes manejan diferentes terminología, por lo tanto, el término de "archivo emulado" es equivalente a "muestra analizada".</p>	

77	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 66	0	23	<p>Dice</p> <p>Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (personalizado y hardenizado), inyección de código a procesos permitidos o análisis de memoria en run time</p> <p>Consulta</p> <p>El requerimiento hace referencia que el sandboxing debe de detectar hypervisores, se comprende que la detección de hypervisores, no la realiza ninguna solución de sandboxing en el mundo. En su lugar, las soluciones de sandboxing utilizan hypervisores personalizados y herdenizados</p> <p>Dicho lo anterior, se solicita a la entidad aclarar si lo solicitado quiere decir que la solución de sandboxing no debe permitir la evasión de malware utilizando un hypervisor (personalizado y hardenizado), inyección de código a procesos permitidos o análisis de memoria en run time</p>	Se aclara que el malware no debe detectar o evadir al hypervisor del sandboxing, conforme a lo solicitado en las bases	
78	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 68	0	23	<p>Dice</p> <p>La funcionalidad de control de aplicaciones debe tener una detección y reconocimiento de al menos 3,600 aplicaciones distintas, entre ellas: Streaming o Video, P2P, Proxy, redes sociales, Juegos o similares</p> <p>Consulta</p> <p>Debido que el fabricante constantemente se encuentra realizando actualizaciones a las aplicaciones detectadas, este no indica un número exacto de aplicaciones detectadas</p> <p>Con la finalidad de sustentar el requerimiento, se solicita a la entidad que opcionalmente se pueda sustentar lo requerido con una carta del fabricante o el enlace del portal de aplicaciones detectadas y reconocidas por el fabricante</p>	Señarse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico	
79	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 69	0	23	<p>Dice</p> <p>Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, paginas de adultos</p> <p>Consulta</p> <p>Debido que no todos los fabricantes cuentan con las mismas categorías, se solicita a la entidad confirmar que se aceptaran soluciones que ofrezcan categorías similares como</p> <p>Proxy o Proxy-avoidance-and-anonymizers</p> <p>Paginas de adultos o adultos</p>	Se precisa que lo consultado son términos equivalentes a lo solicitado, por lo que se aceptara lo indicado	
80	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 71	0	23	<p>Dice</p> <p>Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y soportar protección al protocolo HTTP/2, esta última deberá habilitarse desde la interfaz web</p> <p>Consulta</p> <p>Con la finalidad de brindar el mejor sustento técnico, se solicita a la entidad confirmar que se aceptaran el termino implementación o uso</p>	Se precisa que lo consultado son términos equivalente a lo solicitado, por lo que se aceptara lo indicado	

81	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 71	0	23	<p>Dice</p> <p>Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y soportar protección al protocolo HTTP/2, esta última deberá habilitarse desde la interfaz web</p> <p>Consulta</p> <p>Con la finalidad de brindar el mejor sustento técnico, se solicita a la entidad confirmar que se aceptará que la habilitación desde la interfaz web sea opcional, debido que otros fabricantes lo traen habilitados por default</p>	No se acepta lo solicitado, dado que se requiere que la habilitación sea por una interfaz web para una gestión adecuada	
82	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 72	0	23	<p>Dice</p> <p>La solución deberá contar con un módulo de descubrimiento, identificación y clasificación de dispositivos como teléfonos IP y/o cámaras de vigilancia y/o consolas de videojuegos y/o impresoras y/o dispositivos médicos y/o equipos industriales y/o equipos de seguridad y/o servidores, entre otros. Este módulo debe contar con capacidades de protección de amenazas a través de las políticas de seguridad</p> <p>Consulta</p> <p>Debido que no todos los fabricantes cuentan con las mismas formas de trabajo, sin embargo, se cumple con la finalidad requerida</p> <p>Se solicita a la entidad confirmar que se aceptarán soluciones que cuenten con capacidades de protección de amenazas a través de políticas de seguridad o recomendaciones de políticas según el comportamiento de la red</p>	Definirse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de política de seguridad debe tener el sustento técnico	
83	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 75	0	23	<p>Dice</p> <p>Debe hacer uso del protocolo SNMP para integrarse a los switches</p> <p>Consulta</p> <p>Debido que no todos los fabricantes cuentan con las mismas formas de trabajo, sin embargo, se cumple con la finalidad requerida</p> <p>Se solicita a la entidad confirmar que se aceptarán soluciones que hagan uso del protocolo SNMP para integrarse o consultar a los switches</p>	Se confirma que se aceptarán soluciones que hagan uso del protocolo SNMP para integrarse o consultar a los switches, dado que la función del SNMP es supervisar la infraestructura tecnológica dentro de ello a los switches	
84	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 78	0	24	<p>Dice</p> <p>Se deberá incluir una herramienta integrada y/o externa que genere alertas si existen problemas de salud del equipo en materia de hardware y software, como mínimo: consumo de memoria, problemas de la alta disponibilidad (HA), problemas de disco duro, expiración de licencias</p> <p>Consulta</p> <p>Con la finalidad de brindar un mejor sustento técnico, se solicita a la entidad confirmar que se aceptarán las siguientes alertas similares:</p> <p>Consumo de memoria: uso de memoria alcanza umbral crítico</p> <p>Problema de disco duro: capacidad máxima de disco</p>	Definirse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico	

85	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 81	0	24	<p>Dice</p> <p>Debe estar licenciado para soportar 50 usuarios concurrentes o simultáneos de IPsec o SSL VPN Client-to-Site con capacidad de VPN para dispositivos Windows Linux y MAC y también dispositivos móviles como Android y IOS.</p> <p>Consulta</p> <p>De acuerdo a lo indicado en este punto hace referencia a cantidad de usuarios para la funcionalidad de vpn ssl o vpn ipsec para soportar los diferentes sistemas operativos</p> <p>Tener en consideración que a nivel de cantidades de usuarios concurrentes no se dispone de información de dominio público por ende se solicita a la entidad que la cantidad de usuarios solicitados para esta funcionalidad se pueda sustentar a través de una declaración jurada por parte del postor o carta del fabricante</p>	Se aclara que para este punto solo debe indicarse el cumplimiento en el Anexo N° 12 de las bases	
86	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 84	0	24	<p>Dice</p> <p>Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado en sistema operativo Windows que permita validar en base al nivel de cumplimiento (compliance) del host permitir denegar o limitar el acceso a los recursos de la red interna Por lo menos se deberá poder configurar los siguientes casos de uso siguientes</p> <p>¿Software antivirus instalado y habilitado</p> <p>¿Software antivirus con la base de datos de firmas actualizada</p> <p>¿Parche de seguridad instalado o dispositivos vulnerables según su nivel de criticidad</p> <p>¿Software de DLP instalado el cual debe ser identificado a través de las llaves de registro o procesos del sistema operativo</p> <p>Consulta</p> <p>Se solicita a la entidad confirmar que se aceptarán los términos como antivirus o antimalware en el punto requerido</p>	Se precisa que lo consultado son terminos equivalente a lo solicitado por lo que se aceptara lo indicado	
87	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 84	0	24	<p>Dice</p> <p>Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado en sistema operativo Windows que permita validar en base al nivel de cumplimiento (compliance) del host permitir denegar o limitar el acceso a los recursos de la red interna Por lo menos se deberá poder configurar los siguientes casos de uso siguientes</p> <p>¿Software antivirus instalado y habilitado</p> <p>¿Software antivirus con la base de datos de firmas actualizada</p> <p>¿Parche de seguridad instalado o dispositivos vulnerables según su nivel de criticidad</p> <p>¿Software de DLP instalado el cual debe ser identificado a través de las llaves de registro o procesos del sistema operativo</p> <p>Consulta</p> <p>De acuerdo a lo solicitado en este punto respecto a la funcionalidad de software de dip instalado el cual debe ser identificado a través de las llaves de registro o procesos del sistema operativo Debido que no se cuenta con información pública disponible que sustente lo requerido se solicita la ampliación y/o apertura de la siguiente manera</p> <p>Sírvase confirmar que aceptarán soluciones que Deban permitir configurar una postura de seguridad del equipo con el cliente VPN instalado en sistema operativo Windows que permita validar en base al nivel de cumplimiento (compliance) del host permitir denegar o limitar el acceso a los recursos de la red interna Por lo menos se deberá poder configurar los siguientes casos de uso siguientes</p> <p>¿Software antivirus instalado y habilitado</p> <p>¿Software antivirus con la base de datos de firmas actualizada</p> <p>¿Parche de seguridad instalado o dispositivos vulnerables según su nivel de criticidad</p> <p>¿Software de DLP instalado</p>	Definirse a lo solicitado en las bases no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico	

88	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 86	0	24	<p>Dice:</p> <p>El proveedor deberá realizar la transferencia de conocimiento al personal de la DINI con respecto a la solución ofertada incluyendo lo siguiente:</p> <p>¿ Temas: administración, configuración, monitoreo y formulación de reportes personalizadas, funcionalidades avanzadas, diagnóstico/troubleshooting, backup/restore de las configuraciones</p> <p>¿ Cantidad: cinco (05) participantes</p> <p>¿ 16 horas como mínimo siempre y cuando se cumpla con los temas solicitados y deben ser desarrollados antes de culminar la implementación de la solución ofertada</p> <p>Consulta:</p> <p>Debido que lo requerido es una transferencia de conocimientos, esta no podrá ser sustentada mediante documentación pública, por lo que se solicita a la entidad confirmar si lo requerido se podrá sustentar mediante una declaración jurada.</p>	Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases.	
89	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 93	0	25	<p>Dice:</p> <p>Debe permitir accesos concurrentes de al menos dos administradores.</p> <p>Consulta:</p> <p>Se solicita a la entidad confirmar que se aceptará el término concurrentes o simultáneos.</p>	Se precisa que lo consultado son términos equivalente a lo solicitado, por lo que se aceptará lo indicado.	
90	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 94	0	25	<p>Dice:</p> <p>Definición de perfiles de acceso a la consola con permiso granular como: acceso a escritura, acceso de lectura o similar, cambio de configuraciones o similar.</p> <p>Consulta:</p> <p>Con la finalidad de presentar el mejor sustento técnico para el entendimiento de la entidad, se solicita a la entidad confirmar que se aceptarán términos similares como los siguientes:</p> <p>Perfiles: roles</p> <p>Lectura: readonly</p>	Se precisa que lo consultado son términos equivalente a lo solicitado, por lo que se aceptará lo indicado.	
91	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 96	0	25	<p>Dice:</p> <p>Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horario.</p> <p>Consulta:</p> <p>Con la finalidad de tener claro el requerimiento, se solicita a la entidad confirmar si se aceptarán ofertas que soporten backup/restore o copia de seguridad de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar o programar backups de configuración o copia de seguridad en un determinado día y horario o utilizar un formato de 24 horas para programar la exportación.</p>	Se refiere a lo solicitado en las bases, no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico.	
92	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	6 1 2	0	27	<p>Dice:</p> <p>Personal Especialista implementador</p> <p>Consulta:</p> <p>Dado que los flujos de trabajo pueden variar significativamente entre empresas, estamos limitando la participación de postores a aquellos que cuenten con al menos dos implementadores y dos profesionales de soporte. Reconocemos que algunos postores pueden tener un esquema en el que el personal de soporte también se encargue de la implementación. Sin embargo, esta medida busca garantizar una sinergia efectiva entre la implementación y el servicio postventa ofrecido.</p> <p>Dicho lo anterior, se solicita a la entidad confirmar, que únicamente se requiera 1 personal de soporte y 1 personal de implementación.</p>	Se refiere a lo solicitado en las bases, ya que son las condiciones mínimas requeridas para el personal propuesto.	

93	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	6 1 2	0	27	<p>Dice</p> <p>Personal de Soporte</p> <p>Consulta</p> <p>Dado que los flujos de trabajo pueden variar significativamente entre empresas, estamos limitando la participación de postores a aquellos que cuenten con al menos dos implementadores y dos profesionales de soporte. Reconocemos que algunos postores pueden tener un esquema en el que el personal de soporte también se encargue de la implementación. Sin embargo, esta medida busca garantizar una sinergia efectiva entre la implementación y el servicio postventa ofrecido.</p> <p>Dicho lo anterior, se solicita a la entidad confirmar que únicamente se requiera 1 personal de soporte y 1 personal de implementación.</p>	Definirse a lo solicitado en las bases, ya que son las condiciones mínimas requeridas para el personal propuesto.	
94	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 95	0	25	<p>Dice</p> <p>Generar alertas automáticas por Email, SNMP y Syslog</p> <p>Consulta</p> <p>Con la finalidad de brindar una apertura de postores, enviar diferentes fuentes de correo puede generar confusiones al recibir alertas de diferentes fuentes.</p> <p>Dicho lo anterior, se solicita a la entidad confirmar que se aceptarán alertas automáticas por Email (SMTP) y/o SNMP y/o Syslog.</p>	Se aclara que se aceptará Generar alertas automáticas por Email, Email (SMTP) o SNMP o Syslog.	
95	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 77	0	23	<p>Dice</p> <p>Debe contar con un módulo integrado que monitoree continuamente los firewalls, en base a sus políticas y configuración de buenas prácticas y los compare con base de datos de estándares reconocidos de la industria como mínimo Cobit y/o ISO 27001 y/o NIST 800 53 o mejores prácticas de seguridad, con la finalidad de obtener reportes gráficos detallados, informes que demuestren el cumplimiento de los estándares reconocidos de la industria aplicables o mejores prácticas recomendadas.</p> <p>Consulta</p> <p>Entendemos que lo solicitado en este punto va orientado a mejorar la postura de seguridad de los equipos firewalls en la infraestructura de la entidad.</p> <p>Dicho lo anterior, se solicita a la entidad confirmar que se aceptarán soluciones que cuenten con un módulo integrado que monitoree continuamente los firewalls o evaluación continua de la postura de seguridad en base a las buenas prácticas.</p>	Definirse a lo solicitado en las bases, no se acepta lo propuesto, esta característica de seguridad debe tener el sustento técnico.	
96	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 70	0	23	<p>Dice</p> <p>Debido a que diariamente se crean decenas de miles de nuevas páginas web, la solución deberá ser capaz de analizar en tiempo real si la página web tiene contenido malicioso cuando un usuario intenta acceder.</p> <p>Consulta</p> <p>Tal como se solicita el requerimiento de forma literal, no es posible sustentar con información de dominio público.</p> <p>Dicho lo anterior, se solicita a la entidad confirmar que se aceptarán declaración jurada o carta de fabricante para la sustentación de dicho punto.</p>	Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases.	

97	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 33	0	21	<p>Dice:</p> <p>Para tráfico cifrado SSL debe ser capaz de inspeccionar tráfico cifrado en TLS 1.3 y debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante</p> <p>Consulta</p> <p>Se comprende que al referirse a inspeccionar tráfico cifrado en TLS 1.3 y debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante, hace referencia que se debe obtener visibilidad completa y prevenir amenazas conocidas y desconocidas en el tráfico TLSv 1.3</p>	Definirse a lo solicitado en las bases, se esta solicitando funcionalidades basicas y el postor puede proponer adicionalmente funcionalidades superiores	
98	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 79	0	24	<p>Dice:</p> <p>Se debe proporcionar acceso a la base de datos de inteligencia de amenazas del fabricante, el cual debe permitir hacer consultas de Hashes, Dominios y Direcciones IP, para mostrar información sobre la amenaza, a nivel de clasificación, reputación, familia de malware, comportamiento</p> <p>Consulta:</p> <p>Debido que se requiere que la solución tenga acceso a una base de datos de inteligencia y se detalle las consultas que se logra obtener de este, no es posible sustentar este requerimiento con documentación de dominio publico</p> <p>Dicho lo anterior, se solicita a la entidad confirmar que sea aceptará que el sustento sea mediante una declaración jurada del postor o una carta del fabricante</p>	Se aclara que para este punto solo debe indicarse el cumplimiento, en el Anexo N° 12 de las bases	
99	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 46	0	22	<p>Dice:</p> <p>El IPS debe contar con mecanismo de detección de amenazas de multiples niveles o métodos, detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías, detección basada en comportamiento</p> <p>Consulta:</p> <p>Se solicita a la entidad confirmar que al menos se aceptaran soluciones que cuenten con el módulo de IPS o protección de vulnerabilidades el cual cuente con mecanismos de detección de amenazas de multiples niveles o métodos o capas, detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías o características anómalas en la red, detección basada en comportamiento o comportamiento malicioso</p>	Definirse a lo solicitado en las bases, esta característica de seguridad debe tener el sustento técnico	
100	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 48	0	22	<p>Dice:</p> <p>Las firmas de protección de IPS deben poder categorizarse según un nivel de severidad, nivel de efectividad (confianza) o explotación cloud en línea o exploit-kit y nivel consumo de recursos o fuerza bruta</p> <p>Consulta:</p> <p>Debido que el texto literal indica que las firmas se deban de categorizar de más de 4 formas, impide la participación y sustento técnico del requerimiento</p> <p>Dicho lo anterior, se solicita a la entidad confirmar que al menos se aceptaran soluciones que los módulos de IPS o protección de vulnerabilidades categoricen las firmas de protección según el nivel de severidad y/o nivel de efectividad (confianza) y/o explotación cloud en línea y/o exploit-kit y/o nivel consumo de recursos o fuerza bruta</p>	Definirse a lo solicitado en las bases, esta característica de seguridad debe tener el sustento técnico	

101	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 58	0	22	<p>Dice</p> <p>La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de URL y recursos DNS no identificados y/o no clasificados al momento de ser registrado</p> <p>Consulta</p> <p>La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de URL o sitio web y recursos DNS o dominios no identificados y/o no clasificados al momento de ser registrado</p>	Se precisa que lo consultado son términos equivalente a lo solicitado, por lo que se aceptará lo indicado	
102	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 59	0	22	<p>Dice</p> <p>La solución debe tener una capa de protección DNS para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA), empleando protección basada en Machine Learning, así como protección fuga o exfiltración de información mediante DNS Tunneling, en tiempo real</p> <p>Consulta</p> <p>Debido lo requerido en este punto, no es posible sustentar con documentación de dominio publico, se solicita a la entidad que al menos se considere lo siguiente con la finalidad de ampliar la participación de psotores</p> <p>La solución debe tener una capa de protección DNS para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA) o identificación y bloqueo de amenazas basadas en DGA empleando protección o técnicas basada en Machine Learning o ML, así como protección fuga o exfiltración de información o datos mediante DNS Tunneling, en tiempo real</p>	Se precisa que lo consultado son términos equivalente a lo solicitado, por lo que se aceptará lo indicado	
103	20524531861	THINK NETWORKS PERU S A C	Consulta	Especifico	5 1 60	0	23	<p>Dice</p> <p>La solución debe contar con analisis la reputación de direcciones URL y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C)</p> <p>Consulta</p> <p>Debido lo requerido en este punto, no es posible sustentar con documentación de dominio publico, se solicita a la entidad que al menos se considere lo siguiente con la finalidad de ampliar la participación de postores</p> <p>Dicho lo anterior, sirvase confirmar, que aceptarán soluciones que al menos cuenten con analisis la reputación y/o contenido de direcciones URL o web y los dominios externos (DNS) o categorías DNS a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C)</p>	Se precisa que lo consultado son términos equivalente a lo solicitado, por lo que se aceptará	
104	20552075341	IMPERIA SOLUCIONES TECNOLOGICAS S A C	Consulta	Especifico	2 2 1 1	j	16	<p>Dice: "Indicar en la oferta, el cumplimiento de las especificaciones técnicas mínimas requeridas, lo cual se evidenciará en la documentación técnica."</p> <p>Consulta:</p> <p>Considerando que no todos los puntos técnicos exigidos en bases se pueden encontrar en documentación publica de los fabricantes, se solicita a la Entidad confirmar que se aceptará como sustento de cumplimiento una carta de fabricante para aquellos puntos que no estén disponibles en folletos, instructivos, catalogos o similares de fuentes de la marca, toda vez que es el mismo fabricante la fuente autorizada para validar el cumplimiento de las características solicitadas</p>	Se aclara que los puntos técnicos obligatorios a sustentar de forma detallada y documentada son todos los puntos solicitados en la 5.1 de las bases a excepción de los siguientes (5.1.1, 5.1.3, 5.1.5, 5.1.12, 5.1.13, 5.1.14, 5.1.45, 5.1.61, 5.1.70, 5.1.79, 5.1.81, 5.1.86, 5.1.87, 5.1.95, 5.1.96, 5.1.97), sin embargo deberá indicar el cumplimiento de las mismas en el Anexo N° 12	
105	20552075341	IMPERIA SOLUCIONES TECNOLOGICAS S A C	Consulta	Especifico	3 1 5 1 4	a	19	<p>Dice: "Altura máxima 01 RU, con sus respectivos rieles telescópicos para montaje en gabinete 19" "</p> <p>Consulta:</p> <p>Considerando que los fabricantes proporcionan los accesorios adecuados para el montaje de sus equipos, se solicita a la Entidad que se considerará que los equipos ofertados cuenten con sus respectivos rieles telescópicos y/o sus soportes de montaje para su instalación en gabinete 19"</p>	Se aclara que el postor debe de considerar los accesorios necesarios para el montaje de los equipos Firewall de acuerdo a los solicitado en el punto 5.1.4	

106	20552075341	IMPERIA SOLUCIONES TECNOLOGICAS S A C	Consulta	Especifico	3.1.5.1.13	a	20	<p>Dice: "El proveedor deberá considerar en la implementación los servicios de Networking necesario para la implementación (configuración del core, Switches, reglas en firewall perimetral e interno y aplicación de buenas prácticas para la convivencia de la red externa con la interna)." "</p> <p>Consulta</p> <p>Considerando que se requiere que los servicios de implementación incluyan la configuración de equipos terceros a los ofertados por el postor, se solicita a la Entidad confirmar la cantidad de equipos a intervenir, las marcas, la vigencia del soporte del fabricante de los equipos a intervenir, los accesos y permisos de configuración a los equipos. Así mismo, confirmar que las configuraciones estarán limitadas a los alcances de capacidad y licenciamiento de los equipos de la Entidad.</p>	Se aclara que el servicio de Networking es la misma solución y no en otro equipamiento, para que fluya el tráfico en los diferentes equipos de la red (Core, Switches, firewall interno) para la convivencia de la red externa con la interna.	
107	20552075341	IMPERIA SOLUCIONES TECNOLOGICAS S A C	Consulta	Especifico	3.1.6.1.2	b	27	<p>Personal Especialista implementador</p> <p>Dice: " El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas. Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines." "</p> <p>Consulta</p> <p>Sirvase a la Entidad confirmar que se considerará las carreras de Ingeniería Electrónica, y/o Ingeniería de Seguridad y Auditoría Informática, y/o Redes y Comunicaciones de Datos, y/o Ingeniería de Telecomunicaciones como afines para el perfil de especialista implementador.</p>	Se confirma que lo solicitado por el postor se encuentra considerado como carreras afines.	
108	20552075341	IMPERIA SOLUCIONES TECNOLOGICAS S A C	Consulta	Especifico	3.1.6.1.2	c	27	<p>Personal de Soporte</p> <p>Dice: " El contratista debe contar dentro de su personal técnico con por lo menos dos (02) especialistas. Técnico profesional titulado en computación o afines o bachiller en sistemas o afines o ingeniero titulado en sistemas o afines." "</p> <p>Consulta</p> <p>Sirvase a la Entidad confirmar que se considerará las carreras de Ingeniería Electrónica, y/o Ingeniería de Seguridad y Auditoría Informática, y/o Redes y Comunicaciones de Datos, y/o Ingeniería de Telecomunicaciones como afines para el perfil de personal de soporte.</p>	Se confirma que lo solicitado por el postor se encuentra considerado como carreras afines.	