



BASES INTEGRADAS

BASES ESTÁNDAR DE LICITACIÓN PÚBLICA PARA LA CONTRATACIÓN DE BIENES

LICITACIÓN PÚBLICA N° 001-2023/OSIPTEL

CONTRATACIÓN DE BIENES

**“PROYECTO DE SEGURIDAD DE INFRAESTRUCTURA
TECNOLÓGICA”**

PAC: 15



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.rnp.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 accesorias, 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-emitar-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 : Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL
RUC N° : 20216072155
Domicilio legal : Calle De La Prosa 136 – San Borja
Teléfono: : 225-1313
Correo electrónico: : comiteespecial@osiptel.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del “Proyecto de Seguridad de Infraestructura Tecnológica”.

No. De Ítem Paquete	Denominación	Tipo de Prestación	Sub ítem	Cantidad
1	Proyecto de Seguridad de Infraestructura Tecnológica	Prestación Principal	Seguridad Perimetral: Cortafuegos	2
			Seguridad NDR (Network Detection and Response)	1
		Prestación Accesorio	Gestión del Servicio	36 meses

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Resolución de la Oficina de Administración y Finanzas N° 00119-2023-OAF/OSIPTEL de fecha 21 de abril de 2023.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Directamente Recaudados

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 a 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 siguiente:

Plazo de la Prestación Principal:

i. Entrega, Implementación y Puesta en operación del Equipamiento

1. Todo el equipamiento provisto por el contratista deberá ser entregado, instalado, configurado y/o afinado, y puesto en operación en las oficinas de la institución dentro de los 75 días calendarios contados a partir del día siguiente de la firma de contrato².
2. Dentro de este periodo deben considerarse las labores de configuración/reconfiguración/afinamiento que sea necesario realizar sobre el equipamiento propiedad de la institución a fin de garantizar un óptimo desempeño de la plataforma tecnológica institucional³. Todas estas labores deberán ser ejecutadas por el contratista⁴ sin costo adicional para la institución.
3. Hitos
 - a. Inicio del periodo: al día siguiente de la firma del contrato
 - b. **Plan de Implementación:** se debe presentar como máximo a los 7 días siguientes de la firma del contrato.
 - c. **Acta de Aceptación de Plan de Implementación:** se debe firmar como máximo a los 14 días siguientes de la firma del contrato
 - d. **Acta de Entrega, Implementación y Puesta en Operación del Equipamiento** dentro de los 75 días del plazo de la prestación principal.

Plazo de la Prestación Accesorio:

i. Inicio del servicio

El servicio dará inicio al día siguiente de la firma del “Acta de Entrega, Implementación y Puesta en Operación del Equipamiento”

A. Mantenimiento preventivo y correctivo por parte del contratista

36 meses

B. Soporte remoto e implementación de políticas de seguridad

6 meses

C. Transferencia de conocimiento y capacitación

Hasta 2 meses después de concluido el servicio de soporte remoto e implementación de políticas de seguridad

En concordancia con lo establecido en el expediente de contratación.

1.10. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

² Aplica también para equipamiento en nube pública.

³ Esto incluye también las labores de retiro de operación y/o transferencia de configuraciones del equipamiento (propiedad de la institución) que la institución considere que ya no va a ser requerido luego de la implementación del presente servicio (ejemplo: cortafuegos, enrutadores, filtro de contenidos, entre otros).

⁴ El contratista es íntegramente responsable de las actividades que lleve a cabo su equipo humano y de las consecuencias que éstas pudiesen tener en la infraestructura de la institución, debiendo subsanar junto a la entidad ante cualquier incidente que se pudiese presentar como producto del accionar de éste (ejemplos: reconfiguración de equipos, reposición de cables y conectores, reposición de equipos, entre otros.).



Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/ 6.70 (Seis y 70/100 soles) en Tesorería de la Entidad. El Lugar para realizar el pago y obtener las Bases es en Calle de la Prosa 136, San Borja, en el horario de 08:45 a 16:45 horas.

Importante

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

1.11. BASE LEGAL

- Decreto Legislativo N° 1440, Decreto Legislativo del Sistema Nacional de Presupuesto Público.
- Ley N° 31638 de Presupuesto del Sector Público para el Año Fiscal 2023.
- Ley N° 31639 de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2023.
- Texto Único Ordenado de la Ley N° 30225 - Ley de Contrataciones del Estado y sus modificatorias aplicables.
- Decreto Supremo N° 344-2018-EF, Reglamento de la Ley de Contrataciones del Estado y sus modificatorias aplicables.
- Ley N° 27444 – Ley del Procedimiento Administrativo General.
- Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública, aprobado por Decreto Supremo N° 043-2003-PCM.
- Ley N° 29973 - Ley General de la Persona con Discapacidad.
- Código Civil.
- Directivas y Opiniones del OSCE.
- Decreto Supremo N° 052-2008-PCM que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales
- Cualquier otra disposición legal vigente que permita desarrollar el objeto de la convocatoria, que no contravenga lo regulado por la Ley de Contrataciones del Estado.

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 documentos⁵, la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

- a) Declaración jurada de datos del postor. (**Anexo N° 1**)
- b) 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 – PIDE⁶ 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.

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

⁵ La omisión del índice no determina la no admisión de la oferta.

⁶ 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)**⁷
- 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.

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 acápites “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:

- a) Garantía de fiel cumplimiento del contrato.
- b) Garantía de fiel cumplimiento por prestaciones accesorias.
- c) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.
- d) 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 (de acuerdo al modelo adjunto).
- e) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- f) 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 – PIDE⁸ y

⁷ 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.

⁸ 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 y correo electrónico para efectos de la notificación durante la ejecución del contrato.
- h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación⁹ (**Anexo N° 11**).
- i) Detalle de los precios unitarios del precio ofertado¹⁰.
- j) Detalle del precio de la oferta de cada uno de los bienes que conforman el paquete¹¹.
- k) Además, se deberá presentar la documentación que acrediten el cumplimiento del perfil exigido para los dos especialistas requeridos (Esta documentación será revisada por el Área Usaria de la prestación), de acuerdo al siguiente detalle:

“01 Especialista Implementador en seguridad y redes”

- **Bachiller**¹² o Profesional titulado en las carreras de sistemas y/o computación y/o electrónica y/o telecomunicaciones y/o redes y/o comunicaciones y/o informática (Se acreditará con copia simple del Título o copia simple del registro nacional de grados académicos y títulos profesionales de la SUNEDU).
- Contar, como mínimo, con certificación oficial vigente a nivel Experto o **Profesional o Equivalente**¹³ por parte del Fabricante/Desarrollador ofertado esto se acreditará con copia simple de los certificados correspondientes a cada acreditación/certificación requerida¹⁴.

“01 Especialista de Soporte en seguridad y redes”

- Egresado técnico y/o bachiller en las carreras de sistemas y/o computación y/o electrónica y/o telecomunicaciones y/o redes y/o comunicaciones y/o informática (Se acreditará con copia simple del Título o copia simple del registro nacional de grados académicos y títulos profesionales de la SUNEDU o cualquier documento que acredite lo solicitado).
- Contar con certificación y/o acreditación del fabricante ofertado, esto se acreditará con copia simple de los certificados correspondientes a cada acreditación/certificación requerida¹⁵.

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*

⁹ En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

¹⁰ Incluir solo en caso de la contratación bajo el sistema a suma alzada.

¹¹ Incluir solo en caso de contrataciones por paquete.

¹² Se agrega a las bases de acuerdo a la observación N° 18 y 19 del participante TELEFONICA DEL PERU SAA. Y la consulta N° 32 del participante AI INVERSIONES PALO ALTO II S.A.C.

¹³ Se agrega a las bases de acuerdo a la consulta N° 33 del participante AI INVERSIONES PALO ALTO II S.A.C.

¹⁴ Se aclara que en cada documento presentado debe encontrarse presente, de forma legible, el código del certificado o su información; esto con la finalidad de que el área usuaria pueda validar las certificaciones y/o acreditaciones en el sitio web y/o con comunicación del fabricante/desarrollador.

¹⁵ Se aclara que en cada documento presentado debe encontrarse presente, de forma legible, el código del certificado o su información; esto con la finalidad de que el área usuaria pueda validar las certificaciones y/o acreditaciones en el sitio web y/o con comunicación del fabricante/desarrollador.



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 Haya¹⁶.*
- *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 Virtual; ¹⁷ <https://serviciosweb.osiptel.gob.pe/MesaPartesVirtual/> o en Mesa de Partes situada en Calle De La Prosa 136 – San Borja, de lunes a viernes dentro del horario de 08:45 a 16:45 horas.

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 en pagos a cuenta, de acuerdo al siguiente detalle:

1. **Prestación Principal: Equipamiento:** Se pagará el 100% del monto total de la Prestación Principal: Equipamiento, previa conformidad de la misma.
2. **Prestación Accesorio: Gestión del Servicio:** Se pagará el monto de la prestación accesorio de manera prorrateada en treinta y seis (36) partes iguales de manera mensual, contabilizando a partir del día siguiente de la firma del “**Acta de Entrega, Implementación y Puesta en Operación del Equipamiento**” (ver apartado “**Sobre la adquisición de los bienes**”), previa conformidad del área usuaria.

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

Prestación principal:

- Recepción del área de almacén.
- Conformidad de la prestación efectuada por la Oficina de Tecnologías de la Información.
- Comprobante de pago.

Prestación Accesorio:

¹⁶ Según lo previsto en la Opinión N° 009-2016/DTN.

¹⁷ De conformidad con los lineamientos de la Resolución de Presidencia Ejecutiva N° 047-2022-PD/OSIPTEL, y, Resolución de Presidencia Ejecutiva N° 071-2022-PD/OSIPTEL.

- Conformidad de la prestación efectuada de la Oficina de Tecnologías de la Información.
- Comprobante de pago.

Dicha documentación se debe presentar en Mesa de Partes situada en Calle De La Prosa 136 – San Borja, de lunes a viernes dentro del horario de 08:45 a 16:45 horas y/o Mesa de Partes Virtual; <https://serviciosweb.osiptel.gob.pe/MesaPartesVirtual/>. La atención por Mesa de Partes Virtual del OSIPTEL es 24/7.



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

ESPECIFICACION TECNICA

I. DENOMINACIÓN DE LA CONTRATACIÓN:

PROYECTO DE SEGURIDAD DE INFRAESTRUCTURA TECNOLÓGICA	
Nro. PAC:	15
POI relacionado:	2.1 Elaborar los requerimientos técnicos de la infraestructura tecnológica para dar soporte a los servicios informáticos ofrecidos a nuestros usuarios (internos y ciudadano).

II. FINALIDAD PÚBLICA

Realizar la adquisición de equipamiento que provea al OSIPTEL de mecanismos que permitan mejorar las capacidades de seguridad digital en materia de infraestructura tecnológica, reforzando los pilares de confidencialidad, disponibilidad e integridad de la plataforma de TI de la institución y contribuyendo al normal desempeño de los funcionarios del OSIPTEL en sus labores de regulación, supervisión, fiscalización, emisión de normas, solución de controversias y atención de usuarios de telecomunicaciones.

III. ANTECEDENTES

OSIPTEL cuenta con la necesidad de tener un equipamiento de seguridad perimetral propio para su infraestructura tecnológica que pueda ser gestionado y monitoreado, así como brindar las herramientas necesarias para la prevención de ataques e incidentes.

IV. DEFINICIONES

A lo largo del presente documento, cuando se utilice el término “equipamiento” se estará haciendo referencia a todo componente físico y/o lógico¹⁸, salvo que se indique de forma explícita lo contrario.

A lo largo del presente documento, cuando se utilice el término “la institución” se estará haciendo referencia al OSIPTEL, salvo que se indique de forma explícita lo contrario.

A lo largo del presente documento, cuando se utilice el término “área usuaria” se estará haciendo referencia a la Oficina de Tecnologías de la Información – OTI del OSIPTEL, salvo que se indique de forma explícita lo contrario.

V. DESCRIPCIÓN DEL OBJETO

Es necesario adquirir equipamiento que dote al OSIPTEL de mecanismos que le permitan mejorar las capacidades de seguridad digital en materia de infraestructura tecnológica, reforzando los pilares de seguridad perimetral de la plataforma de TI de la institución. De igual forma que se den las capacidades técnicas para que el equipo pueda ser gestionado, administrado y monitoreado, esto a través de capacitación y acompañamiento

5.1 PRESTACION PRINCIPAL: EQUIPAMIENTO

La presente adquisición debe contemplar, como mínimo, lo siguiente:

A. Provisión de equipamiento

- 1) Todo el equipamiento provisto deberá ser de la misma marca, fabricante y/o desarrollador¹⁹.
- 2) El contratista deberá proveer el equipamiento listado en el **Anexo N° 01**
- 3) El equipamiento provisto por el contratista se instalará en el centro de datos de la institución y los servicios complementarios en la nube del fabricante y/o contratista de corresponder.
 - a. El equipamiento del contratista podrá ser retirado de las instalaciones de la institución bajo alguna de las siguientes circunstancias:
 - i. Reemplazo por garantía; en cuyo caso deberá entregarse equipamiento de características similares o superiores a las del equipamiento retirado. El contratista deberá asumir cualquier labor de transporte, instalación, configuración y/o afinamiento, o alguna otra que fuese necesaria. Esto no representará ningún costo adicional para la entidad.

¹⁸ Se considerará equipamiento físico y lógico: todo equipo, componente, pieza, accesorio, cable, conector y/o elemento físico de hardware, así como también, todo software, firmware, licencia, membresía, aplicativo y/o elemento no físico.

¹⁹ Esto con la finalidad de agilizar las gestiones de soporte, mantenimiento, garantía, entre otros de cara al fabricante. Asimismo, se busca eliminar inconvenientes de compatibilidad y/o comunicación entre equipamiento heterogéneo. Esta prestación es de gran criticidad para la entidad y requiere la máxima celeridad en la gestión del equipamiento.

- ii. Inspección técnica en el centro de atención del contratista o del fabricante/desarrollador; en cuyo caso deberá entregarse equipamiento de características similares o superiores a las del equipamiento retirado durante todo el periodo que el equipamiento inicial permanezca en revisión/repación. El contratista deberá asumir cualquier labor de transporte, instalación, configuración y/o afinamiento, o alguna otra que fuese necesaria. Esto no representará ningún costo adicional para la entidad.
 - iii. Reemplazo preventivo o proactivo por parte del fabricante o contratista²⁰; en cuyo caso deberá entregarse equipamiento de características similares o superiores a las del equipamiento retirado. El contratista deberá asumir cualquier labor de transporte, instalación, configuración y/o afinamiento, o alguna otra que fuese necesaria. Esto no representará ningún costo adicional para la entidad.
 - iv. Alguna otra circunstancia no prevista en el presente documento y que cuente con la autorización previa del área usuaria. Esto no representará ningún costo adicional para la entidad.
 - v. Para todos los casos antes descritos será imperativo contar con la autorización del área usuaria antes de proceder con el retiro/reemplazo del equipamiento. Asimismo, para todos los casos antes descritos, el contratista deberá asumir cualquier labor y coste de transporte, instalación, configuración y/o afinamiento, o alguna otra que fuese necesaria; es decir, estas actividades no representarán ningún costo adicional para la entidad.
- 4) El equipamiento provisto por el contratista deberá ser entregado (o puesto en operación, para el caso de servicios en nube) siguiendo los plazos indicados en el apartado **"Sobre la adquisición de los bienes"**.
 - 5) El contratista deberá asumir toda labor de instalación, configuración y/o afinamiento sobre el equipamiento provisto, según le sea indicado por el personal del área usuaria; esto durante el periodo de Soporte remoto e implementación de políticas de seguridad, ver apartado **"Sobre la adquisición de los bienes"**.
 - 6) El equipamiento provisto por el contratista debe incluir licencias, membresías, software, tarjetas, conectores, interfaces, cables y todo componente (físico o lógico) necesario para su puesta en operación, la explotación completa de todas sus funcionalidades y su inclusión dentro de la infraestructura de la institución.
 - 7) El contratista debe garantizar durante el periodo de garantía comercial del equipamiento la descarga/obtención de actualizaciones de software, de sistema operativo, software de gestión, firmware y demás que fuesen necesarios, directamente desde el sitio web del fabricante/desarrollador (o a través de alguna otra fuente respaldada por este último) con la finalidad de mantener el equipamiento actualizado según las recomendaciones del fabricante/desarrollador.
 - a. El contratista deberá mantener todo el equipamiento provisto actualizado con los últimos parches, actualizaciones, versiones de software, configuraciones, firmware y demás que determine/recomiende el fabricante/desarrollador durante el periodo de Mantenimiento preventivo y correctivo por parte del contratista.
 - 8) Todo el equipamiento deberá ser implementado, configurado y operado siguiendo las buenas prácticas y recomendaciones del fabricante/desarrollador.
 - 9) El equipamiento provisto por el contratista deberá contar con soporte y garantía por parte del fabricante/desarrollador durante todo el periodo de la garantía comercial del equipamiento (tres años, ver apartado **"Sobre la adquisición de los bienes"**) y esto debe acreditarse mediante carta del fabricante/desarrollador (ver apartado **"Entregables"**).

5.2 PRESTACION ACCESORIA: GESTION DEL SERVICIO

A. Mantenimiento preventivo y correctivo por parte del contratista

- 1) El mantenimiento preventivo y correctivo del equipamiento se extenderá por el periodo de la garantía comercial del equipamiento tres años (36 meses):
 - a. El presente apartado detalla las características del mantenimiento físico y lógico que deberá cumplir el equipamiento provisto.
 - b. El mantenimiento debe cubrir la totalidad del equipamiento comprendido en la presente contratación.
 - c. Sobre el mantenimiento preventivo:
 - i. El contratista es responsable de realizar mantenimientos preventivos sobre el equipamiento provisto, de acuerdo con lo siguiente:
 1. En caso el contratista encuentre pertinente realizar mantenimientos preventivos sobre su equipamiento, deberá coordinar con el área usuaria la realización de estos. Esto con la finalidad de no interrumpir las operaciones en la institución.
 2. Los protocolos y medidas para la realización del mantenimiento preventivo sobre los equipos son responsabilidad de la entidad.
 3. El mantenimiento preventivo mínimo exigible deberá requerir limpieza externa física, revisión de operatividad del equipo, revisión de posibles mejoras de las políticas de seguridad y aplicación de actualizaciones de software, previa validación y programación con el área usuaria.²¹
 - d. Sobre el mantenimiento correctivo
 - i. El servicio de mantenimiento correctivo deberá ser brindado siguiendo el siguiente protocolo:
 1. Ante la falla de algún elemento/componente del equipamiento comprendido en la contratación, el contratista notificará de forma inmediata al área usuaria.
 - a. En caso la avería hubiese sido detectada durante la ejecución de un mantenimiento preventivo, se entenderá que el contratista ha sido notificado de la avería en un corto plazo.
 - b. Como parte de su comunicación, el contratista notificará las acciones de mantenimiento correctivo a ejecutar sobre el equipamiento a fin de

²⁰ Se considerará "Reemplazo preventivo o proactivo" a las situaciones en las cuales, a fin de prevenir un posible fallo advertido por el contratista/fabricante o de ofrecer un equipo de características tecnológicas superiores, se ofrece a la institución el cambio del equipo a fin de garantizar el óptimo desempeño de la plataforma y el estricto cumplimiento de las exigencias de la contratación.

²¹ Se agrega a las bases de acuerdo a la consulta N° 42 del participante TELEFONICA DEL PERU SAA



- corregir el incidente. Asimismo, notificará las posibles consecuencias/impacto de las acciones a realizar sobre las operaciones de la institución.
2. Luego de recibida la comunicación, el área usuaria evaluará las acciones recomendadas por el contratista, así como su impacto en las operaciones, y notificará al contratista su conformidad para iniciar las labores.
 - a. El área usuaria se reserva el derecho de solicitar al contratista planes de acción alternativos en caso considere que el impacto en las operaciones es demasiado alto.
 - b. El área usuaria se reserva el derecho de solicitar que las acciones correctivas se ejecuten en un periodo de tiempo específico (día y hora exactos) así como también de solicitar que las acciones correctivas se ejecuten de forma remota y/o presencial en las oficinas de la institución.
 3. En caso fuese necesaria la gestión de garantía ante el fabricante, el contratista es responsable de realizar todas las acciones pertinentes y mantener informada al área usuaria sobre el estado de la atención.
 4. El contratista deberá notificar al área usuaria cuando el incidente haya sido superado.
 - ii. Toda labor adicional que pudiese ser requerida para la correcta ejecución del mantenimiento correctivo (documentación, escalada al fabricante, entre otras) serán contempladas dentro de los tiempos exigidos en el presente documento (ver apartado “**Niveles de servicio y penalidades**”). No se otorgarán ampliaciones de plazos a los tiempos estipulados a menos que la razón de la demora sea responsabilidad íntegra de la institución.
 - iii. Toda labor comprendida dentro del mantenimiento correctivo deberá ser asumida por el contratista sin costo alguno para la institución.
 - iv. El contratista deberá mantener constante comunicación con el área usuaria informando el estado de cada atención de mantenimiento correctivo que se reporte.
 - v. **el servicio de mantenimiento correctivo incluye procedimiento de creación, análisis o afinamiento de políticas o perfiles de seguridad durante los 36 meses del servicio.**²²
 - vi. **De presentarse un incidente de seguridad, brindar la solución o remediación del evento forma parte del alcance del mantenimiento correctivo.**²³
- 2) Es responsabilidad íntegra del contratista implementar los mecanismos de seguridad que considere pertinentes para garantizar la integridad de su equipamiento físico (candados de seguridad, etiquetas de “*piel de cebolla*”, sellos, entre otros); siempre y cuando los mencionados mecanismos no impidan la óptima explotación de las capacidades del equipamiento.
- 3) Se realizará el mantenimiento preventivo 1 vez al año previa coordinación con el área usuaria.

B. Soporte remoto e implementación de políticas de seguridad

- 1) El contratista será responsable de la gestión, monitoreo remoto e implementación de políticas de seguridad a solicitud del área usuaria de todo el equipamiento consignado en el presente proceso de adquisición (Listado en el **Anexo N° 01**) por un periodo de seis (06) meses en modalidad de horario laboral (modo 5x8).
- 2) La gestión del servicio debe incluir, como mínimo, lo siguiente:
 - a. Atención de requerimientos efectuados por el área usuaria (configuración, reconfiguración, afinamiento, solicitudes de información, elaboración de informes, entre otros).
 - i. Durante la implementación y ejecución del servicio, el área usuaria comunicará al contratista el tratamiento (notificar al área usuaria, cerrar comunicaciones, mitigar, ignorar, entre otras) que deberá darse a cada tipo de evento que se pudiese identificar en la plataforma de seguridad.
 - ii. El tratamiento para cada evento estará sujeto a los tiempos especificados en el apartado “**Niveles de servicio y penalidades**”.
 - b. Atención de incidentes de seguridad que se presenten en la red de datos de la institución (sucesos que afectan el óptimo desempeño de la red de datos institucional o que representen algún riesgo para los pilares de la seguridad (integridad, confidencialidad y disponibilidad) o en alguno de los componentes de la plataforma contratada.
 - c. Solución/remediación de brechas e incidentes de seguridad en el equipamiento de comunicaciones de la institución²⁴:
 - i. El contratista deberá aplicar las configuraciones y/o remediaciones pertinentes en los equipos de comunicaciones a fin de cerrar brechas de seguridad identificadas.
 - ii. La institución brindará los accesos correspondientes al contratista para que pueda desempeñar estas labores.
 - d. Durante el periodo del servicio gestión y monitoreo (soporte remoto activo), y a solicitud de la institución, el contratista deberá realizar la configuración del equipamiento provisto (o de los equipos de comunicaciones propiedad de la institución) que requieran acciones de remediación de seguridad, como resultado de los diversos servicios realizados en la institución como, por ejemplo: servicios de *Ethical Hacking* y/o otras auditorías de seguridad.
 - i. Toda actividad de remediación que deba ejecutarse debe ser coordinada con el área usuaria, y consignada mediante “**Acta de actividad de remediación**”.
- 3) El contratista deberá brindar acceso a todos los componentes del equipamiento al personal del área usuaria, bajo solicitud de esta última, a fin de poder realizar una supervisión adecuada del servicio. El personal del área

²² Se agrega en las bases de acuerdo a la consulta N° 39 del participante TELEFONICA DEL PERU SAA

²³ Se agrega en las bases de acuerdo a la consulta N° 40 del participante TELEFONICA DEL PERU SAA

²⁴ Como parte de la implementación del equipamiento adquirido, el equipamiento provisto por el contratista tendrá acceso a la red de datos institucional y a los equipos que la conforman, por ello, el contratista (a través de la labor de monitoreo) podrá determinar cuándo alguna configuración y/o condición particular de algún equipo de comunicaciones ponga en riesgo la seguridad de la información institucional. Adicionalmente, la institución brindará al contratista acceso a los equipos de comunicaciones a fin de poder realizar las labores descritas en el presente.

usuaria deberá manejar credenciales de acceso diferenciadas a fin de poder hacer seguimiento a las labores realizadas por cada usuario.

- a. Esto incluye la configuración de notificaciones y/o alertas en los diversos componentes del equipamiento a fin de que el personal del área usuaria se mantenga informado del estado de la solución.
- 4) La institución podrá solicitar que los requerimientos de atención (reconfiguraciones, revisiones, afinamientos, entre otros) que se generen como parte del servicio, mientras este se encuentre activo, sean atendidos a través de su plataforma de Mesa de Ayuda.
 - a. Para este fin, la institución facilitará al personal del contratista acceso a la mencionada plataforma y brindará instrucción respecto a su correcto uso.
 - b. En caso la institución no lo considere pertinente, o no le sea viable, brindar acceso al contratista a su solución de Mesa de Ayuda, se utilizarán los medios de comunicación estipulados en la **"Ficha de contactos"** (ver apartado **"Entregables"**) sin embargo, la institución se reserva el derecho de solicitar el uso de su plataforma de Mesa de Ayuda en cualquier momento durante la duración del servicio (ver apartado **"Sobre la adquisición de los bienes"**).
- 5) Todos los requerimientos, incidentes, solicitudes, labores de monitoreo y demás, atendidos dentro del servicio, deberán ser atendidos por el personal especialista del contratista.
 - a. En primera instancia, el personal del contratista laborará desde sus propias instalaciones para atender los incidentes, solicitudes y demás labores contempladas en el presente documento.
 - i. Estas labores deberá ejecutarlas haciendo uso de una conexión segura hacia la infraestructura de la entidad. Esta conexión debe ser del tipo VPN o VPN S2S según se evalúe más viable durante el periodo de **"Entrega, Implementación y Puesta en operación del Equipamiento"** (ver apartado **"Sobre la adquisición de los bienes"**) o según lo determine el área usuaria.
 - b. Las labores propias a la **"Soporte Remoto"** deberán ser realizadas por el personal especialista del contratista y deberán ser atendidas en jornada laboral (5x8, 5 días de la semana: lunes a viernes, 8 horas laborales, durante los seis meses de duración).
 - c. De considerarlo estrictamente necesario, la institución podrá solicitar que el personal del contratista desarrolle algunas funciones de emergencia o muy importantes en sus instalaciones, para lo cual:
 - i. La institución comunicará al contratista la necesidad de contar con el personal in-situ por un limitado tiempo, no mayor a 3 días hábiles al mes, previa aceptación. El contratista deberá disponer que su personal inicie labores en las instalaciones de la institución en un plazo no mayor a 24 horas hábiles contadas desde el momento de la aceptación de la solicitud. La mencionada solicitud será comunicada al contratista a través de los canales de atención pertinentes (ver apartado **"Entregables"**).
 - ii. Durante el periodo de tiempo que el personal del contratista se encuentre desarrollando labores en las instalaciones de la institución, ésta última le brindará acceso a la red de fluido eléctrico, a la red de datos institucional, a internet y a mobiliario, a fin de que dicho personal pueda cumplir cabalmente con lo requerido como parte del contrato.
 - d. Todo cambio en el personal del contratista deberá ser notificado mediante carta dirigida al área usuaria y adjuntando toda la documentación necesaria respecto al personal reemplazante²⁵.
 - i. El personal reemplazante deberá cumplir, como mínimo, el perfil exigido en el presente documento.
 - ii. La notificación de cambio de personal deberá realizarse, como mínimo, 3 días calendarios antes del inicio de labores del personal reemplazante en el presente proyecto.
- 6) Toda la gestión del equipamiento²⁶ dentro del servicio deberá ser llevada a cabo por el personal técnico especialista del contratista. El equipo de trabajo deberá estar compuesto, como mínimo, por:
 - a. Un (01) **"Especialista implementador de la solución de seguridad y redes"**
 - b. Un (01) **"Especialista de soporte en seguridad y redes"** que se encargará de la gestión y monitoreo del servicio.

C. Transferencia de conocimiento y capacitación

El contratista deberá brindar capacitación y transferencia de conocimiento al personal del área usuaria respecto a todo el equipamiento y tecnologías relacionadas al presente proyecto. El perfil encargado de la capacitación debe ser el **"Especialista implementador de la solución de seguridad y redes"**.

- 1) En lo referido a capacitación al personal del área usuaria, el contratista deberá brindar, capacitación para un mínimo de 5 participantes, con un tiempo mínimo de 20 horas lectivas:
 - a. Capacitación:
 - i. Implementación de una solución integrada de defensa contra amenazas
 - ii. Investigación y mitigación de la defensa integrada contra amenazas
 - iii. Se deberá emitir certificados por el contratista

Todas las capacitaciones serán brindadas por el contratista bajo un esquema propuesto que podrá notificar su programación de la capacitación con un mínimo de 48 horas de anticipación. Además, todas las capacitaciones serán otorgadas en las instalaciones del centro de instrucción o en las instalaciones de la institución según las necesidades del área usuaria (en caso se lleven a cabo en las instalaciones de la institución, este brindará únicamente acceso a sistema eléctrico e internet; será responsabilidad del contratista brindar todo el equipamiento y material adicional necesario para llevar a cabo la capacitación).
- 2) En lo referido a la transferencia de conocimiento, el contratista deberá brindar, al personal del área usuaria, información y detalle técnico sobre cada labor que se realice durante las etapas de implementación, reconfiguración o soporte. Incluyendo la redacción/entrega de manuales o instructivos con detalle técnico e imágenes (a pedido del área usuaria, de considerarlo pertinente) se firmará un acta de transferencia de

²⁵ Es responsabilidad íntegra del contratista presentar la documentación por la mesa de partes virtual del OSIPTEL

²⁶ Esto incluye gestiones de garantía ante el fabricante/desarrollador y las labores pertinentes en las oficinas del OSIPTEL estipuladas en el apartado **"Sobre la adquisición de los bienes"**



conocimiento al concluir el servicio de soporte remoto e implementación de políticas de seguridad entre área usuaria y el especialista implementador de la solución de seguridad y redes.

VI. SOBRE LA ADQUISICIÓN DE LOS BIENES DE LA PRESTACION PRINCIPAL

- 2) Lugar de entrega de bienes del **Anexo N° 01**:
 - a. Los bienes serán entregados en el almacén del OSIPTEL situado en:
 - i. Calle De La Prosa 136 – San Borja.
- 3) Plazos de ejecución:
 - a. Se ejecutará respetando los siguientes periodos:

Plazo de la Prestación Principal:

i. Entrega, Implementación y Puesta en operación del Equipamiento

1. Todo el equipamiento provisto por el contratista deberá ser entregado, instalado, configurado y/o afinado, y puesto en operación en las oficinas de la institución dentro de los 75 días calendarios contados a partir del día siguiente de la firma de contrato²⁷.
2. Dentro de este periodo deben considerarse las labores de configuración/reconfiguración/afinamiento que sea necesario realizar sobre el equipamiento propiedad de la institución a fin de garantizar un óptimo desempeño de la plataforma tecnológica institucional²⁸. Todas estas labores deberán ser ejecutadas por el contratista²⁹ sin costo adicional para la institución.
3. Hitos
 - a. Inicio del periodo: al día siguiente de la firma del contrato
 - b. **Plan de Implementación**: se debe presentar como máximo a los 7 días siguientes de la firma del contrato.
 - c. **Acta de Aceptación de Plan de Implementación**: se debe firmar como máximo a los 14 días siguientes de la firma del contrato
 - d. **Acta de Entrega, Implementación y Puesta en Operación del Equipamiento** dentro de los 75 días del plazo de la prestación principal.

Plazo de la Prestación Accesoría:

ii. Inicio del servicio

El servicio dará inicio al día siguiente de la firma del "Acta de Entrega, Implementación y Puesta en Operación del Equipamiento"

A. Mantenimiento preventivo y correctivo por parte del contratista

36 meses

B. Soporte remoto e implementación de políticas de seguridad

6 meses

C. Transferencia de conocimiento y capacitación

Hasta 2 meses después de concluido el servicio de soporte remoto e implementación de políticas de seguridad

VII. DOCUMENTOS PARA LA FIRMA DE CONTRATO

El postor que adjudique la Buena Pro deberá presentar, dentro de los documentos para el perfeccionamiento del contrato.

Además, se deberá presentar la documentación que acrediten el cumplimiento del perfil exigido para los dos especialistas requeridos, de acuerdo al siguiente detalle:

"01 Especialista Implementador en seguridad y redes"

- **Bachiller**³⁰ o Profesional titulado en las carreras de sistemas y/o computación y/o electrónica y/o telecomunicaciones y/o redes y/o comunicaciones y/o informática (Se acreditará con copia simple del Título o copia simple del registro nacional de grados académicos y títulos profesionales de la SUNEDU).
- Contar, como mínimo, con certificación oficial vigente a nivel Experto o Profesional o Equivalente³¹ por parte del Fabricante/Desarrollador ofertado esto se acreditará con copia simple de los certificados correspondientes a cada acreditación/certificación requerida³².

"01 Especialista de Soporte en seguridad y redes"

- Egresado técnico y/o bachiller en las carreras de sistemas y/o computación y/o electrónica y/o telecomunicaciones y/o redes y/o comunicaciones y/o informática (Se acreditará con copia simple del Título o copia simple del registro

²⁷ Aplica también para equipamiento en nube pública.

²⁸ Esto incluye también las labores de retiro de operación y/o transferencia de configuraciones del equipamiento (propiedad de la institución) que la institución considere que ya no va a ser requerido luego de la implementación del presente servicio (ejemplo: cortafuegos, enrutadores, filtro de contenidos, entre otros).

²⁹ El contratista es íntegramente responsable de las actividades que lleve a cabo su equipo humano y de las consecuencias que éstas pudiesen tener en la infraestructura de la institución, debiendo subsanar junto a la entidad ante cualquier incidente que se pudiese presentar como producto del accionar de éste (ejemplos: reconfiguración de equipos, reposición de cables y conectores, reposición de equipos, entre otros.).

³⁰ Se agrega a las bases de acuerdo a la observación N° 18 y 19 del participante TELEFONICA DEL PERU SAA. Y la consulta N° 32 del participante AI INVERSIONES PALO ALTO II S.A.C.

³¹ Se agrega a las bases de acuerdo a la consulta N° 33 del participante AI INVERSIONES PALO ALTO II S.A.C.

³² Se aclara que en cada documento presentado debe encontrarse presente, de forma legible, el código del certificado o su información; esto con la finalidad de que el área usuaria pueda validar las certificaciones y/o acreditaciones en el sitio web y/o con comunicación del fabricante/desarrollador.



nacional de grados académicos y títulos profesionales de la SUNEDU o cualquier documento que acredite lo solicitado).

- Contar con certificación y/o acreditación del fabricante ofertado, esto se acreditará con copia simple de los certificados correspondientes a cada acreditación/certificación requerida ³³.

Esta documentación será revisada/validada por el área usuaria del servicio.

VIII. ENTREGABLES

Es responsabilidad íntegra del contratista presentar la documentación dicha documentación se debe presentar en Mesa de Partes del OSIPTEL situada en calle de La Prosa 136 – San Borja - Lima, dentro del horario de 08:45 a 16:45 horas de lunes a viernes o a través de la Mesa de Partes Virtual; <https://serviciosweb.osiptel.gob.pe/MesaPartesVirtual/> en un solo archivo de 10 MB como máximo, habilitada las 24 horas, los 7 días de la semana.

8.1. PRESTACION PRINCIPAL: EQUIPAMIENTO

1) Ficha de contactos

- Documento que debe consignar los medios de contacto con el personal del contratista; como mínimo, debe consignar:
 - Medios de contacto de coordinador: Personal, correo electrónico y número telefónico.
 - Medios de contacto de servicio/gestión: Personal, correo electrónico y número telefónico.
 - Medios de contacto de emergencia: Personal y número móvil.
- En caso los canales de atención del contratista a través de los cuales la institución deba reportar averías o solicitudes de atención sean distintos de los indicados en el punto anterior, dichos canales de atención (central telefónica, *call center*, correo electrónico, entre otros) deberán también ser consignados en la presente “**Ficha de Contactos**”.
- Documento que debe ser presentado, como máximo, dentro de 05 días calendarios contados a partir del día siguiente de la firma de contrato.
- Documento de presentación única.

2) Plan de implementación

- Documento que debe consignar el plan de implementación del equipamiento provisto por el contratista (el detalle del periodo de “**Entrega, Implementación y Puesta en operación del Equipamiento**” (ver apartado “**Sobre la adquisición de los bienes**”). Debe considerar, como mínimo:
 - Entrega, revisión y prueba del equipamiento.
 - Instalación del equipamiento.
 - Configuración del equipamiento.
 - Pruebas y verificación de operatividad.
- Documento que debe ser presentado, como máximo, dentro de 07 días calendarios contados a partir del día siguiente de la firma de contrato.
- Documento de presentación única.
- El “**Plan de implementación**” debe ser aceptado por el área usuaria a través de la suscripción de un “**Acta de Aceptación de Plan de Implementación**” en conjunto con el especialista implementador en seguridad y redes.
 - En caso el área usuaria tuviese observaciones sobre el “**Plan de Implementación**” presentado por el contratista, éstas serán comunicadas a la Unidad de Abastecimiento del OSIPTEL en el plazo legal, para la notificación al contratista indicando claramente el plazo para su subsanación por mesa de partes virtual.

3) Carta de garantía del fabricante

- Documento que debe consignar que el fabricante/desarrollador brinda garantía sobre todo el equipamiento/licenciamiento provisto por el contratista durante todo el periodo de garantía comercial (03 años), el cual se encuentra listado en el **Anexo N° 01** del presente documento.
- Documento que debe ser presentado, como máximo, dentro de los 75 días calendarios contados a partir del día siguiente de la firma de contrato.
- Documento de presentación única.

8.2. PRESTACION ACCESORIA: GESTION DEL SERVICIO

Informe mensual del servicio

- De forma mensual, el contratista deberá remitir un informe del servicio que debe consignar las atenciones, requerimientos, incidentes, “**Actas de Actividad de Remediación**” y demás hechos relevantes ocurridos durante el periodo mensual correspondiente. Se tomará como fecha de inicio del primer mes contado desde el día siguiente de la firma del “**Acta de Entrega, Implementación y Puesta en Operación del Equipamiento**”.
- Documento que debe ser presentado luego de culminado el periodo mensual correspondiente a través de la Mesa de Partes Física o Virtual del OSIPTEL.
- Documento que debe ser presentado, como máximo, dentro de 10 días calendarios contados a partir del día siguiente de finalizado el periodo mensual correspondiente.

Transferencia de conocimiento y capacitación

³³ Se aclara que en cada documento presentado debe encontrarse presente, de forma legible, el código del certificado o su información; esto con la finalidad de que el área usuaria pueda validar las certificaciones y/o acreditaciones en el sitio web y/o con comunicación del fabricante/desarrollador.



El contratista deberá presentar el acta de transferencia de conocimiento y certificados de capacitación hasta 10 días calendarios de concluido el servicio de Transferencia de conocimiento y capacitación

IX. NIVELES DE SERVICIO Y PENALIDADES

9.1 Niveles de Servicio

- a. El contratista deberá cumplir los niveles de servicio estipulados a continuación, en la **Tabla N° 01**, desde el momento de la firma del Acta de Entrega, Implementación y Puesta en Operación del Equipamiento, contabilizados dentro de su período de monitoreo que es en modalidad 5x8:

Ítem	Descripción	Tiempos de atención
1	Diagnosticar y comunicar el plan de acción frente a la falla de alguno de los componentes del servicio (ver apartado " Mantenimiento correctivo ")	02 horas hábiles desde la aparición del incidente ³⁴
2	Tiempo de resolución de incidentes	04 horas hábiles desde el reporte de diagnóstico del incidente ³⁵
3	Actualización de componentes, licencias, membresías, sistemas operativos, firmware, controladores y demás componentes donde sea aplicable el término.	8 horas hábiles x 5 días laborables
4	Tiempo de atención de las solicitudes y/o requerimientos (ver apartado " Soporte remoto e implementación de políticas de seguridad ")	02 horas hábiles desde la generación de la solicitud/requerimiento ³⁶
5	Monitoreo de los servicios y equipamiento que comprenden la plataforma contratada. (ver apartado " Soporte remoto e implementación de políticas de seguridad ")	8 horas hábiles x 5 días laborables
6	Actividad de Remediación	Según lo establecido en el " Acta de Actividad de Remediación "
7	Tratamiento de eventos en la plataforma de seguridad (ver apartado " Soporte remoto e implementación de políticas de seguridad ") ³⁷	02 horas hábiles desde la generación del evento

Tabla N° 01 Niveles de servicio aplicables

9.2 Penalidades

a) Penalidad Por Mora

En caso de retraso injustificado del contratista en la ejecución de la prestación principal objeto del contrato, el OSIPTEL aplicará automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente formula:

$$\text{Penalidad Diaria} = 0.01 * \text{Monto del Contrato} * \text{cada día de atraso}$$

b) Otras Penalidades

- Se aplicarán penalidades siempre que se atribuya al contratista responsabilidad sobre el incumplimiento de los niveles de servicio estipulados en el punto anterior o en el presente documento.
- Las penalidades contempladas serán cobradas por el OSIPTEL, de manera automática, de cualquier pago pendiente, además, serán ejecutadas sin perjuicio de la ejecución de garantías de fiel cumplimiento de contrato, la aplicación de otras penalidades, la resolución del contrato, la responsabilidad civil y las acciones legales pertinentes.
- En la **Tabla N° 02** se detallan las penalidades aplicables según los niveles de servicio incumplidos.

Ítem	Condición	Factor de calculo
------	-----------	-------------------

³⁴ En caso alguno de los componentes del equipamiento provisto emitiese cualquier tipo de alerta (luminosa, sonora, vía correo electrónico, vía SMS, o de cualquier tipo), se contabilizará el cumplimiento de los tiempos estipulados desde el momento en que dicha alerta fue emitida, independientemente de si el contratista lo notificó a la institución, siempre considerado esta contabilidad dentro del horario de su gestión y monitoreo (modo 5x8).

³⁵ En caso el alguno de los componentes del equipamiento provisto emitiese una alerta, se contabilizará el cumplimiento de los tiempos estipulados desde el momento en que dicha alerta fue emitida siempre considerado esta contabilidad dentro del horario de su gestión y monitoreo (modo 5x8).

³⁶ El OSIPTEL podrá solicitar que ciertas solicitudes/requerimientos sean atendidos en una fecha o momento en particular, en dicho caso no se tomará en cuenta el tiempo límite de 24 horas hábiles; sin embargo, para efectos de la penalización en caso de incumplimiento, se considerará incumplimiento si es que el pedido no ha sido atendido en la fecha o momento especificado por la institución y, por ende, se procederá con la aplicación de la penalidad correspondiente.

³⁷ Dada la enorme variedad de eventos que se pueden presentar en los diversos componentes del equipamiento contratado (correos electrónicos retenidos, identificación de tráfico anómalo, entre otros), el área usuaria irá estableciendo, a lo largo del periodo de ejecución del servicio, el tratamiento que se dará a cada uno de estos eventos; este tratamiento será notificado a través de los medios pertinentes consignados en la "**Ficha de contactos**". A continuación, se ejemplifica el escenario mencionado:

- Ejemplo 1: El área usuaria puede determinar que cada vez que el equipamiento contratado retenga un correo electrónico dirigido hacia una dirección en particular, entonces se le notifique.
- Ejemplo 2: El área usuaria puede determinar que cada vez que el equipamiento contratado identifique tráfico inusual hacia un determinado host en la red, entonces se bloquee el puerto de red correspondiente.

			Procedimiento
1	Por incumplimiento en la presentación de la documentación indicada en el apartado "Entregables-Prestación Principal" .	1 UIT	Por cada entregable y por cada día calendario de retraso
2	Por incumplimiento en la presentación de la documentación indicada en el apartado "Entregables-Prestación Accesorio" .	5% de la UIT	Por cada entregable y por cada día calendario de retraso
3	Por incumplimiento en los tiempos de atención de solicitudes, solución de incidentes y problemas (ver apartado "Niveles de servicio").	10% de la UIT	Por cada Ocurrencia
4	Por incumplimiento en las labores de monitoreo (ver apartado "Gestión del servicio").	10% de la UIT	Por cada Ocurrencia ³⁸
5	Por incumplimiento de alguno de los puntos mencionados en el apartado "Confidencialidad" .	5 UIT	Por cada Ocurrencia
6	Por incumplimiento de las condiciones establecidas en el "Acta de actividad de remediación" .	10% de la UIT	Por cada Ocurrencia ³⁹
7	Por incumplir en mantener actualizada la plataforma de seguridad (Ver Ítem 3 de la "Tabla N° 01 : Niveles de servicio aplicables").	10% de la UIT	Por cada Ocurrencia

Tabla N° 02 Penalidades aplicables

El % de la UIT se aplicará de acuerdo al momento en qué se realice la falta.

9.3 Excepciones

Se permitirá no respetar los **Niveles de Servicio** y, por ende, no se aplicarán penalidades en situaciones de catástrofe, eventos naturales (terremotos, desplazamientos, lluvias, huacos, entre otros), eventos excepcionales (accidentes en las instalaciones como: aniego, incendio, derrumbe, entre otros) y/o manifestaciones sociales (huelgas, paros, activismo, entre otros).

Esto se respetará siempre y cuando el contratista presente la justificación respectiva adjuntando la documentación que la sustente.

X. CONFIDENCIALIDAD

La empresa contratista se compromete a guardar la más absoluta reserva de la información relacionada a la ejecución del contrato, a fin de garantizar la seguridad e integridad de los procesos, programas, datos e información pertenecientes a la institución, así como a no violar la confidencialidad, seguridad y propiedad de los archivos, programas y sistemas de aplicación, absteniéndose, a efectuar cualquier tipo de cambio, transacción, modificación y adición de información a los archivos, programas y sistemas de aplicación, no pudiendo facilitar a terceros, bajo ningún concepto, información alguna, sin la respectiva autorización por escrito de la institución.

El proveedor deberá mantener estricta confidencialidad sobre la información a que tendrá acceso durante la ejecución del contrato, y no podrá disponer de la misma para fines distintos al desarrollo de este. Al término de este deberá devolver todos los documentos que se le hayan entregado como objeto de la contratación. Esto incluye tanto material impreso como material grabado en medio digital.

Cualquier copia, publicación, divulgación, distribución, total o parcial de la información sin autorización expresa por parte de la institución o con fines no autorizados por esta, serán motivo para la inmediata rescisión del vínculo contractual y del inicio de las acciones legales que la institución considere pertinentes.

El proveedor deberá mantener un adecuado resguardo de los datos de carácter personales en tratamiento como producto del presente contrato. Asimismo, deberá dar estricto cumplimiento con lo establecido en la ley N° 29733 – Ley de Protección de Datos Personales, su Reglamento aprobado mediante el Decreto Supremo N° 003-2013-JUS, así como el Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, y modifica la indicada Ley N° 29733; pudiendo adoptarse además buenas prácticas como las contenidas en la Directiva de Seguridad elaborada por la Autoridad Nacional de Protección de Datos Personales.

Asimismo, el proveedor debe considerar que son otras obligaciones contractuales las siguientes:

- La información y documentos proporcionados por la institución para la ejecución del contrato, así como los resultados que se obtengan de esta, son de uso exclusivo para el desarrollo de las actividades inherentes a la contratación e íntegramente propiedad de la entidad.
- Conservar y tratar como reservada toda la información que se declare información confidencial. Esta no será revelada en ningún caso y bajo ningún motivo sin el consentimiento previo y por escrito de la institución.
- Limitar el acceso a la información confidencial de forma tal que sólo sea accesible a aquellas personas que necesariamente deban involucrarse en las conversaciones, tratativas y/o acuerdos mantenidos con la institución.
- No divulgar ni transferir a terceros la información a la que pudiera tener acceso él o su personal, siendo que, de ser el caso, responderá legalmente por los daños y perjuicios causados.

³⁸ En caso un incidente y/o alerta, notificada/advertida por la plataforma (ver apartado **"Gestión del servicio"**) y no atendida por un periodo mayor a 02 horas hábiles (dentro del período 5x8); se considerará como incumplimiento sobre las tareas de monitoreo y, por ende, se procederá a aplicar la penalidad especificada.

³⁹ En caso las actividades no sean completadas en el transcurso del mes en el que se hubiese acordado, el OSIPTEL se reserva el derecho de aplicar la penalidad indicada en los meses sucesivos hasta que la falta haya sido subsanada.



- Comprometerse a guardar la información confidencial en un archivo especial que posea las condiciones suficientes de seguridad.

Las presentes condiciones de confidencialidad no serán aplicables a información que:

- Resulte accesible al público por causa distinta del incumplimiento de la obligación de confidencialidad por la parte receptora (el contratista).
- Haya sido publicada con anterioridad a la fecha de la firma de contrato.
- Sea independientemente desarrollada por la parte receptora (el contratista), siempre que no se hubiese utilizado para ello ningún tipo de información proporcionada por la institución.
- Deba ser revelada para dar cumplimiento de una orden de naturaleza judicial o administrativa, en cuyo caso la parte receptora (el contratista) deberá informar a la institución en forma inmediata a la sola recepción de la citada orden.

XI. REQUISITOS DE CALIFICACION

A	CAPACIDAD TÉCNICA Y PROFESIONAL	
A.1	EXPERIENCIA PERSONAL	<p>DEL</p> <p>Requisito:</p> <ul style="list-style-type: none"> • Un (01) “Especialista implementador en seguridad y redes” Experiencia laboral mínima de cuatro (04)⁴⁰ años como implementador de soluciones de ciberseguridad, seguridad informática y/o tecnología de la información. • Un (01) “Especialista de soporte en seguridad y redes” Experiencia laboral mínima de un (01) año⁴¹ como gestor de soporte y/o mesa de ayuda y/o soporte técnico de seguridad informática y/o equipamiento de tecnología de la información. <p>Acreditación:</p> <ul style="list-style-type: none"> • La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.
B	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD	
B.1	FACTURACIÓN	<p>Requisito:</p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/. 1,000,000.00 (Un millón 00/100 soles), por la contratación de bienes similares al objeto de la convocatoria, durante un periodo de ocho (08) años a la fecha de la presentación de ofertas.</p> <p>Se consideran bienes similares a los siguientes:</p> <ul style="list-style-type: none"> • Equipamiento y/o soluciones de seguridad informática. • Equipos y/o soluciones de respuesta ante incidentes informáticos. • Equipos y/o soluciones de seguridad en infraestructura tecnológica. • Equipos y/o soluciones para outsourcing de tecnología y/o TI • Equipos y/o soluciones de infraestructura tecnológica en centro de datos: redes, comunicaciones, seguridad, procesamiento, etc. • Garantías comerciales de equipamiento informático, soporte técnico y/o tecnológico, servicios de mesa de ayuda, service desk o help desk. • Solución de Balanceador⁴² • Equipos firewall⁴³ • Equipamiento y/o soluciones de infraestructura tecnológica en centro de datos: redes, comunicaciones, seguridad, procesamiento también se considerarán balanceadores de enlaces y/o switches en general y/o servidores.⁴⁴ <p>Acreditación:</p> <p>Copia simple de contratos u órdenes de servicios, y su respectiva conformidad por la prestación efectuada; o comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con Boucher de depósito o reporte de estado de cuenta o que la cancelación figure en el comprobante de pago, 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° 7 referido a la Experiencia del Postor.</p>

⁴⁰ Se cambia en las bases de acuerdo a la consulta N° 21 del participante TELEFONICA DEL PERU SAA

⁴¹ Se cambia en las bases de acuerdo a la consulta N° 02 del participante IT BUSINESS & SUPPORT SOCIEDAD ANONIMA CERRADA - ITB SUPPORT S.A.C. y consulta N° 28 del participante TELEFONICA DEL PERU SAA

⁴² Se agrega en las bases de acuerdo a la consulta N° 27 del participante TELEFONICA DEL PERU SAA

⁴³ Se agrega en las bases de acuerdo a la consulta N° 35 del participante AI INVERSIONES PALO ALTO II S.A.C.

⁴⁴ Se agrega en las bases de acuerdo a la consulta N° 36 del participante AI INVERSIONES PALO ALTO II S.A.C.

	<p>En el caso de servicios de ejecución periódica, solo se considera como experiencia la parte del contrato que haya sido ejecutada 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, se entenderá que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso de que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p> <p>Cuando en los contratos, órdenes de servicios 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 servicios o de cancelación del comprobante de pago, según corresponda.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 7 referido a la Experiencia del Postor.</p>
--	---

XII. CONFORMIDAD

1. Toda conformidad será emitida por la Oficina de Tecnologías de la Información – OTI.
2. La conformidad sobre la prestación principal: equipamiento se emitirá luego de presentados los siguientes entregables (ver apartado “**Entregables**”):
 - a. Ficha de contactos.
 - b. Plan de implementación (adjuntando la respectiva “*Acta de Aceptación de Plan de Implementación*”).
 - c. Carta de garantía del fabricante.
 - d. Acta de Entrega, Implementación y Puesta en Operación del Equipamiento.
3. La conformidad sobre la Prestación Accesoría: Gestión del Servicio se dará mensualmente; y se emitirá luego de presentado el “**Informe mensual del servicio**” por parte del contratista.

XIII. FORMA DE PAGO

El pago se realizará de la siguiente forma:

1. **Prestación Principal: Equipamiento:** Se pagará el 100% del monto total de la Prestación Principal: Equipamiento, previa conformidad de la misma.
2. **Prestación Accesoría: Gestión del Servicio:** Se pagará el monto de la prestación accesoria de manera prorrateada en treinta y seis (36) partes iguales de manera mensual, contabilizando a partir del día siguiente de la firma del “**Acta de Entrega, Implementación y Puesta en Operación del Equipamiento**” (ver apartado “**Sobre la adquisición de los bienes**”), previa conformidad del área usuaria.



XIV. **ANEXOS**

Anexo N° 01

SOBRE LA ADQUISICIÓN DE LOS BIENES

El presente anexo detalla el equipamiento que deberá ser provisto por el contratista como parte de la presente contratación.

Todo el equipamiento deberá ser de la misma marca/fabricante y contar con garantía comercial contratada de 03 años.

En caso alguno de los componentes del equipamiento (adicionalmente a aquellos especificados como “físico” o “hardware”) requiriese ser instalado sobre un servidor o **appliance**, entonces el contratista deberá proveer los servidores/**appliance** necesarios para garantizar el óptimo funcionamiento de la solución, la explotación completa de todas las funcionalidades del equipamiento, la alta disponibilidad de todos los componentes del servicio y el cumplimiento de todas las condiciones estipuladas en el presente. El equipamiento físico provisto por el contratista (servidores/**appliance**) deberá ser del mismo fabricante que el resto de las soluciones.

En todos los casos, la institución brindará las condiciones adecuadas para la instalación y correcto almacenaje de los equipos físicos (gabinetes, energía estabilizada, red de datos, UPS, entre otros).

En todos los casos, el equipamiento deberá permitir el envío de registros de eventos mediante el protocolo SYSLOG. La institución comunicará oportunamente al contratista los datos de la plataforma a la cual deberán remitirse los registros de eventos.

Los componentes del equipamiento que deberá brindar el contratista son:

1) Ítem 1 – Seguridad Perimetral

A nivel físico (*hardware*), para la seguridad perimetral se deberán proveer los equipos especificados en la **Tabla N° 03** y cuyas características se detallan líneas abajo.

Equipo Físico (Hardware)	Cortafuegos (Firewall)
Cantidad	2
Tipo de equipo	Servidor/ <i>appliance</i> para gabinete de 19 pulgadas Altura máxima de 1RU
Gestión	- 01 puerto de gestión 10/100/1000 Base-T - 01 puerto consola RJ-45 serial - 01 interfaz USB
Interfaces de red	- (08) interfaces de red RJ-45 10/100/1000 Base-T - (08) interfaces 10G SFP+ (debe incluir los Transceiver SR)
Almacenamiento	- (01) dispositivo SSD - SSD debe tener una capacidad mínima de 480 GB como mínimo
Ventilación	- Deben incluirse todos los ventiladores y elementos de refrigeración.
Alimentación	- Mínimo 01 fuentes de poder redundante - Debe soportar hot-swap; cambiar las fuentes sin afectar la operación del equipo. - Se deben incluir todos los cables de alimentación necesarios y en configuración
Accesorios	- Debe incluir todo accesorio necesario para su correcto ensamblaje. - Debe incluir todo accesorio necesario para su correcto montaje en un gabinete de 19 pulgadas (esto incluye tornillos, rieles, soportes y demás) ⁴⁵ . - Debe incluir todo componente físico, lógico y de licenciamiento para su óptimo funcionamiento. - Todos los componentes (tarjetas, conectores, kits de montaje y demás) deben ser del mismo fabricante.

Tabla N° 03: Equipos de Seguridad Perimetral

El equipamiento deberá contar con las siguientes características (por cada equipo):

- El dispositivo no deberá tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas durante los meses transcurridos del 2023, para sus sistemas operativos (SO) que operan en los Firewall de seguridad propuestos/ofertados, de no cumplir con este requisito, no serán aceptados. [\(Se considerada la cantidad de vulnerabilidad contabilizadas durante el presente año hasta el 22 de mayo del 2023\).](#)⁴⁶
- Cada dispositivo debe proporcionar, como mínimo, un throughput de 7.4 Gbps de Threat Protection/Prevention (Firewall+IPS+Control de Aplicaciones + Antivirus + Sandboxing) medido en Enterprise Mix Traffic ó Enterprise Test Conditions.
- El dispositivo debe soportar, como mínimo, 16 millones de conexiones concurrentes.
- El dispositivo debe soportar, como mínimo, 230,000 nuevas conexiones por segundo
- Debe proporcionar un throughput de 17 Gbps en Next Generation Firewall medido en Enterprise Mix Traffic ó Enterprise Test Conditions.
- El dispositivo debe soportar una cantidad de usuarios ilimitados en modo “Cortafuegos” (“Firewall”).
- El dispositivo debe soportar, como mínimo, 1024 interfaces virtuales (VLANs).

⁴⁵ En caso se encontrase disponible un kit de montaje para el equipo por parte del fabricante, este deberá ser incluido.

⁴⁶ Se agrega en las bases de acuerdo la consulta N° 04 del participante UNITY PERU S.A.C.

- h. El dispositivo debe soportar esquemas de operación en modo ruteado y modo transparente ó modo bridge.
- i. El dispositivo debe contar con capacidad para integrar esquemas de red NAT/PAT ("Network Address Translation" / "Port Address Translation").
- j. El dispositivo debe contar con un mecanismo de control basado en técnicas "statefull inspection"
- k. El dispositivo deberá permitir la configuración de políticas de calidad de servicio y rate limit
- l. El dispositivo deberá de soportar mecanismos de alta disponibilidad activo-pasivo.
- m. El dispositivo debe soportar direccionamiento IPv6 para su operación y en todas las funcionalidades descritas en el presente.
- n. El dispositivo debe soportar la operación en modo transparente ó modo bridge y Gateway; además en ambos modos debe soportar IPv6.
- o. El dispositivo debe tener la capacidad de soportar el protocolo Netflow o similares para poder tener información del estado de las sesiones de manera granular.
- p. El dispositivo debe soportar ser accedido mediante una línea de comando segura HTTPS y CLI (SSH) con la finalidad realizar configuraciones mediante estos medios.
- q. El dispositivo debe soportar Protocol Independent Multicast (PIM) e Internet Group Management Protocol (IGMP) para aplicaciones tipo multicast.
- r. El dispositivo debe soportar mecanismos de filtrado de tráfico basado en "tags" (etiquetas)
- s. El dispositivo debe integrarse a CISCO ISE (Security Group Tags) para la construcción de reglas de acceso

t. **Funcionalidad a nivel de control de aplicaciones**

En lo referente a Control de Aplicaciones, el equipamiento deberá contar con las siguientes características:

- i. El dispositivo debe permitir filtrar aplicaciones bajo los siguientes criterios (como mínimo):
 - 1. Categoría
 - 2. Riesgo
 - 3. Tipo.
- ii. La tecnología ofrecida deberá contar con capacidad de extracción de amenazas en archivos MS Office y Adobe PDF, mediante CDR (Content Disarm Reconstruction).
- iii. El dispositivo debe permitir limitar el número y tipos aplicaciones que están autorizadas para funcionar en la red.
- iv. El dispositivo debe poder controlar las aplicaciones en cualquier puerto.
- v. El dispositivo debe detectar de forma automatizada, como mínimo, 6000 aplicaciones y categorizarlas por riesgo y relevancia empresarial.
- vi. El dispositivo debe poder identificar de forma automatizada, al menos, 800 tipos protocolos de aplicación dentro de las cuales están: Adobe Flash, Facebook, Facetime, LinkedIn, LogMeIn, Netflix, UltraSurf, entre otros.
- vii. El dispositivo debe controlar el uso de las aplicaciones a través de las acciones estándar:
 - 1. "Allow"
 - 2. "Monitor"
 - 3. "Block"
 - 4. "Interactive Block"
- viii. El dispositivo debe permitir la creación de reglas para controlar el uso de aplicaciones a través de las siguientes condiciones:
 - 1. Zona
 - 2. Red
 - 3. VLAN
 - 4. Usuarios
 - 5. Puertos
- ix. El dispositivo debe permitir bloquear tráfico por geolocalización; ya sea por país o continente.
- x. El dispositivo deberá incluir un sistema de integración con Directorio Activo (**Microsoft Active Directory**), que provea las siguientes características:
 - 1. Deberá permitir la integración con el directorio activo de la red para tener un mapeo de usuario e IP utilizada actualmente.
 - 2. Deberá permitir tener la información de contacto de los usuarios que están siendo atacados.
 - 3. Los eventos de seguridad reportados deberán mostrar el usuario que está generando o recibiendo el ataque
 - 4. Deberá de poder generar un mapa de eventos de seguridad generados/recibidos por usuario.
 - 5. Deberá de poder generar un mapa de tráfico generado/recibido por usuario.
 - 6. Deberá ser capaz de mantener un mapa de los usuarios, ip actual, tipo de aplicación usada, y un historial de las IPS que ese usuario ha usado en el tiempo.

u. **Funcionalidad a nivel de Prevención de Intrusos:**

En lo referente a Prevención de Intrusiones, el equipamiento deberá contar con las siguientes características:

- i. El motor de inspección del sistema de prevención de intrusos debe contar con todo lo necesario (licenciamiento, componentes físicos y lógicos, entre otros) para explotar al máximo sus funcionalidades.
- ii. El IPS debe incluir al menos los siguientes mecanismos de detección: exploit signatures, protocol anomalies, application controls y behavior-based detection.
- iii. Los módulos de IPS de Firewall, deben estar integrados ofreciendo de esta manera, protección multicapa.
- iv. Debe inspeccionar el tráfico SSL
- v. Debe tener protección contra ataques DoS
- vi. 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 y correlación de múltiples elementos.
- vii. El IPS debe proveer al menos dos políticas o perfiles precargados, para ser usados inmediatamente.



- viii. El dispositivo debe ser capaz de inspeccionar el tráfico asociado a distintos segmentos de redes diferentes (en lugar de tener una sola política por interfaz).
- ix. El dispositivo debe contar, como mínimo, con las siguientes técnicas de análisis de tráfico:
 - 1. Identificación del protocolo a través del puerto utilizado
 - 2. Identificación de protocolos que utilizan puertos aleatorios
 - 3. Identificación de protocolos en forma independiente del puerto utilizado
- x. El dispositivo debe ser resistente a diversas técnicas de **URL obfuscation** en ataques basados en HTML.
- xi. El dispositivo debe soportar los siguientes tipos de respuestas:
 - 1. Bloquear
 - 2. Ignorar
 - 3. Guardar en un log
 - 4. Enviar correo electrónico
 - 5. SNMP
- xii. El dispositivo debe monitorear y proteger los segmentos de datos, con tráfico activo de red pasando por él, lo que permite prevenir los ataques de estos segmentos y bloqueado en tiempo real.
- xiii. El dispositivo debe de soportar la identificación y protección de ataques en protocolos de **Voice over IP (VoIP)** sobre SIP.
- xiv. El dispositivo debe proveer la detección de anomalías de tráfico
- xv. El dispositivo debe permitir tener la flexibilidad de controlar políticas a nivel de dispositivo, puerto, VLAN y direcciones IP.
- xvi. El dispositivo debe de proveer monitoreo de segmentos de red en “modo promiscuo” analizando encabezamiento (**header**) y el área de datos (**payload**) de los paquetes que transitan en la red (**deep packet inspection**), detectando ataques y tráfico no autorizado o sospechoso.
- xvii. El dispositivo debe poder realizar capturas de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y ENC (estándar para el software de análisis de protocolos). El archivo puede ser usado para hacer **playback** del ataque⁴⁷. Se aceptarán propuestas que consideren la captura de tráfico para el análisis de evidencia en formato compatible con **libpcap** (compatible a su vez con TCPDUMP), y opcionalmente en formato ENC.
- xviii. El dispositivo debe ser capaz de proporcionar mayor visibilidad sobre cómo se consume el ancho de banda, ya sea por dirección o puerto, permitiendo ayudar en la solución de problemas de interrupciones o degradaciones de rendimiento de la red. (sin necesidad de hardware o software separado).
- xix. El dispositivo debe proveer la capacidad de realizar un respaldo de la configuración de la plataforma en tiempo real, o por un horario definido.
- xx. El dispositivo debe soportar **IP Reputation**, además debe permitir la creación de listas negras y listas blancas y debe contar con una base de datos propia,
- xxi. El dispositivo debe contar con, al menos, las siguientes de objetos de **IP Reputation**:
 - 1. *Bots*
 - 2. *CnC*
 - 3. *Malware*
 - 4. *Attacker*
 - 5. *Suspicious*
- xxii. El dispositivo debe soportar integración a través del Directorio Activo (**Microsoft Active Directory**) para determinar el comportamiento de la red a través de direcciones IP asociadas a los eventos sospechosos.
- xxiii. El dispositivo debe contar con la capacidad de crear reglas que permitan enviar tráfico directamente a través del dispositivo sin que sea inspeccionado.
- xxiv. El dispositivo deberá de proveer protección contra **DoS** y **DDoS** (inundación de ataques tipo “**SYN DOS**”).
- xxv. El dispositivo debe permitir la funcionalidad de gestión SNMP e integrarse a productos de red de terceros para proporcionar indicadores clave de estado operacional a grupos de operaciones de red y de operaciones de seguridad.
- xxvi. El dispositivo debe de proveer la opción de consulta, de un histórico de los eventos sucedidos en los equipos ofertados desde la consola principal, con el fin de realizar análisis forense.
- xxvii. El dispositivo debe proteger contra ataques sobre aplicaciones Web como:
 - 1. *shell command injections*
 - 2. *Server-site injection*
 - 3. *cross-site scripting*
 - 4. *directory traversal*.
- xxviii. El dispositivo debe ser capaz de reducir significativamente el esfuerzo del operador y la aceleración de respuesta a las amenazas por dar prioridad a las alertas de forma automática.
- xxix. El dispositivo debe ser capaz de proporcionar de forma automática los adecuados controles permitiendo la protección del tráfico enviado a través de puertos de comunicación no estándares.
- xxx. El dispositivo deberá ser capaz de detectar anomalías de tráfico en la red, en base a los patrones de tráfico identificados.
- xxxi. El dispositivo deberá tener una funcionalidad de “**packet level**” para realizar actividades de análisis forense
- xxxii. El dispositivo deberá soportar el remontaje de paquetes TCP fragmentados.
- xxxiii. El dispositivo deberá soportar la búsqueda de firmas por nombre a través de la interfaz gráfica.
- xxxiv. El dispositivo deberá soportar la desfragmentación de paquetes IP fragmentados y/o coincidentes.
- xxxv. El dispositivo deber contar con cobertura de filtros que protejan las vulnerabilidades de **Microsoft Internet Explorer**.

⁴⁷ Se aceptarán propuestas que consideren la captura de tráfico para el análisis de evidencia en formato compatible con **libpcap** (compatible a su vez con TCPDUMP), y opcionalmente en formato ENC

- xxxvi. El dispositivo debe estar basado sobre firmas en vulnerabilidades permitiendo la detección de ataques desconocidos o variaciones de ataques conocidos.

v. **Funcionalidad a nivel de Protección contra Malware, Malware Avanzado y Amenazas Desconocidas (sandboxing):**

- i. La solución debe proteger contra ataques de día cero y malware desconocido antes de que una firma de protección estática sea creada.
- ii. La solución debe ser parte de una arquitectura de protección contra prevención de amenazas multicapa.
- iii. La solución debe tener disponibilidad de despliegue en la nube o en sitio, en caso que sea en sitio el sandboxing tiene que realizado en un equipo dedicado para esta finalidad.
- iv. El motor debe detectar llamadas API, cambios en el sistema de archivos, cambios en el registro, conexiones de red, procesos de sistema.
- v. El motor de emulación debe ser capaz de inspeccionar, emular, prevenir y compartir los resultados de los eventos de sandboxing con la infraestructura anti malware.
- vi. La solución debe ser capaz de soportar escaneo de links dentro de correos para detección de malware desconocido.
- vii. La solución debe tener capacidad de anti-evasión, para que el malware no pueda detectar su ejecución dentro de un ambiente de Sandboxing.
- viii. El motor de emulación debe tener capacidad de detección anti-vm.
- ix. Debe ser capaz de emular apagados y reinicios de las máquinas, para ver la reacción del Malware una vez esto ocurre.
- x. Debe contar con una funcionalidad de eliminar contenido malicioso o explotable en documentos.
- xi. Debe eliminar contenido explotable, incluido el contenido activo y los objetos incrustados, y que pueda reconstruir archivos para eliminar amenazas potenciales y entrega rápidamente contenido desinfectado a los usuarios, conocido como tecnología de Desarmado y Reconstrucción de Contenido (CDR).
- xii. Los equipos deben tener integrada la detección y prevención de virus y amenazas (anti-malware).
- xiii. La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.
- xiv. Debe tener capacidad de protección de pre-infección del malware que fue identificado en los archivos.
- xv. Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), Mail (SMTP o POP3), SMB y FTP.
- xvi. Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real.
- xvii. Base de datos local de firmas de malware locales que contiene las firmas comúnmente usadas, URL y sus reputaciones.
- xviii. Utiliza el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar el repositorio para la reputación de URL y la clasificación antivirus. Las actualizaciones de firmas de antivirus, se realiza de manera automatizada y programable.
- xix. Debe soportar Inspección de tráfico cifrado/encryptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).
- xx. Debe tener capacidad de clasificación y análisis de archivos y posterior validación en el repositorio de inteligencia de amenazas en nube del propio fabricante, sin generar un impacto en el rendimiento de la red.
- xxi. Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware. Debe contar con un mecanismo de almacenamiento en caché para verificar las URL a las cuales se acceden, o en su defecto, enviar al repositorio de inteligencia de amenazas en nube del propio fabricante para determinar si estas URLs están permitidas o no, parase detener el intento antes de que se produzcan daños en la red.
- xxii. Debe tener capacidades de inspección y prevención de amenaza en el canal cifrado SSH, con las siguientes capacidades:
- xxiii. Bloquear ataques en canal SSH.
- xxiv. Bloquea la transmisión de virus a través de los protocolos SCP y SFTP.
- xxv. Prevenir el descifrado de contraseñas en fuerza bruta de servidores SSH/SFTP.
- xxvi. Prevenir el reenvío de puertos SSH (Port Forwarding).
- xxvii. Prevenir el uso de criptografía vulnerable en el canal SSH.
- xxviii. Prevenir el uso de clientes y servidores SSH vulnerables.
- xxix. Prevenir el uso del puerto 22 para otros protocolos que no sean SSH.
- xxx. Debe soportar el manejo personalizado (añadir, borrar o modificar) para la alimentación de IoC (Indicadores de Compromiso), en formato CSV y/o Structured Threat Information Expression (STIX).
- xxxi. 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. La aplicación y prevención de seguridad, en base a los IoC incluidos, debe ser de manera automática, sin interacción del usuario administrador.
- xxxii. La solución debe proveer una herramienta que haga descubrimiento de "bots" dentro de la red. Dicha herramienta debe bloquear la comunicación que intenten establecer los equipos infectados "bots" hacia las redes de los atacantes en Internet (botnet).
- xxxiii. La solución debe incluir al menos los siguientes métodos de identificación:
 1. Identificación de direcciones web de Comando y Control utilizadas por los criminales para controlar los bots.
 2. Identificación de patrones (fingerprints) de comunicación utilizada por cada familia de bots.
 3. Identificación de comportamiento de bots.



- xxxiv. La solución debe contar con un repositorio en la nube del propio fabricante para la identificación de direcciones y patrones de comunicación de “botnet”. El Anti-Bot se debe actualizar continuamente de manera automática.
 - xxxv. La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de direcciones IP, URL y recursos DNS no identificados y/o no clasificados.
 - xxxvi. 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.
 - xxxvii. La solución debe contar con análisis la reputación de direcciones URL, direcciones IP 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).
 - xxxviii. Funcionalidad de detección de amenazas avanzadas persistentes de nueva generación, específicamente diseñado para proteger a la institución contra ataques cibernéticos, malware, Botnets y amenazas avanzadas persistentes similares.
 - xxxix. La solución debe utilizar una Red de Inteligencia Global que le permita beneficiarse de la información recogida por los esfuerzos de investigación del fabricante/desarrollador.
 - xl. El servicio de actualización de información/amenazas deberá operar sobre un canal seguro (HTTPS).
 - xli. La solución debe proporcionar detección y protección en las comunicaciones desde y hacia los servicios de internet, contra los ataques de Malware de día cero, *exploits*, *botnets* y Ataques Persistentes Avanzados (APT).
 - xl.ii. Deberá detectar todas las fases de los ataques modernos: exploit, infección a partir de código malicioso, y comunicación a servidores de comando y control (**Callback**); para permitir un análisis del ciclo de vida completo del ataque.
 - xl.iii. La solución deberá tener también la capacidad de detectar software malicioso que se aprovecha de vulnerabilidades conocidas y/o sitios web maliciosos.
 - xl.ii. La solución debe proporcionar protección contra ataques originados en la web, como descargas de archivos maliciosos y acciones de devolución de llamada (**callback**) de malware
 - xl.ii. La solución debe detectar la amenaza sin necesidad de conocer la firma, es decir, a través del comportamiento de la propia amenaza.
 - xl.ii. La solución debe ser capaz de ejecutar el código sospechoso, acceso URL's y diversos tipos de archivos en un entorno virtual de inspección. Para ello realizará tanto análisis estático (basado en reglas) como dinámico (basado en comportamiento).
 - xl.ii. Debe soportar la ejecución e inspección, como mínimo, de los siguientes tipos de archivos: documentos de la suite MS Office (en todas sus versiones), documentos PDF, archivos ejecutables, archivos comprimidos y archivos multimedia.
 - xl.ii. La solución debe contar con mecanismos de reseteo de la conexión de tráfico detectado como malicioso.
 - xl.ii. La solución debe permitir la identificación de las direcciones IP de origen de los ataques (geo-localización).
 - xl.ii. El proceso de detección de malware del entorno virtual en nube deberá ser capaz de:
 - 1. Análisis dinámico.
 - 2. Análisis de patrones y aprendizaje de máquina.
 - 3. Poder detectar malware de tipo día cero.
 - xl.ii. La solución debe tener la capacidad de bloquear llamadas a servidores remotos (**Callbacks**, llamadas de Comando & Control) en el caso de ataques del tipo “**Zero Day**” y amenazas persistentes. Protegiendo los equipos que pudiesen haberse comprometido y se encuentren realizando llamadas a servidores remotos desde la red corporativa.
 - xl.ii. Las máquinas virtuales deberán contar con técnicas que eviten la detección como tales por parte de las propias APT's
 - xl.ii. Contar con un módulo que emita reportes de al menos:
 - 1. Reportes sobre las principales Alertas (actividad actual o histórica).
 - 2. Reportes en un rango de fechas y rango de direcciones IP.
 - 3. Reportes detallados de llamadas a servidores remotos, identificando cuando sea posible la geolocalización de la IP.
 - 4. Poder definir reportes personalizados y moldes de reportes para su uso recurrente.
 - 5. Contar con un tablero de control (**Dashboard**) que permita personalizar la información presentada en él acerca de amenazas, servicios de comando y control, posibles firmas asociadas, severidad y otros campos, y poder generar un reporte a partir de este **Dashboard** personalizado.
 - xl.ii. La solución debe permitir enviar notificaciones en diversos formatos, ya sean estas por **Syslog**, SNMP o correo electrónico. Las notificaciones deben contener la Información mínima necesaria, como el nombre de host o IP del equipo afectado.
- w. **Funcionalidad a nivel de Filtrado URL:**
En lo referente a Filtrado URL, el equipamiento deberá contar con las siguientes características
- i. El sistema debe permitir la configuración de filtrado URL basado en la reputación y la categoría de las páginas en Internet.
 - ii. El sistema debe contar con un sistema de inteligencia de amenazas para validar la reputación de las URLs e IPs solicitadas por los usuarios en la navegación.
 - iii. El filtrado URL debe permitir la creación de perfiles de acceso sobre al menos 80 categorías web.
 - iv. El sistema debe permitir la creación de listas blancas y negras para páginas web definidas por el administrador.
 - v. El sistema debe permitir la creación de políticas de filtrado URL basado en direcciones IP y usuarios del dominio.
 - vi. El sistema debe permitir la integración con el Directorio Activo (Microsoft Active Directory) para la identificación de los usuarios del dominio.



- vii. La solución debe permitir la creación de políticas de DNS a fin de crear listas negras y blancas del tráfico basado en el nombre del dominio solicitado por el usuario.
- viii. La solución debe categorizar las aplicaciones y URLs por factor de riesgo
- ix. Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario.
- x. Las bases de datos de control de aplicaciones deben actualizarse por un servicio basado en la nube.
- xi. La solución debe proporcionar un mecanismo para limitar el uso de aplicaciones basadas en el consumo de ancho de banda.
- xii. La solución debe tener mecanismos para categorizar y filtrar tráfico de navegación cifrado HTTPS sin necesidad de realizar inspección SSL.

x. **Plataforma de Administración de seguridad:**

Se deberá contar con un sistema de administración centralizada que permita gestionar y monitorear los equipos **NGFW** descritos en el presente.

La plataforma deberá contar con una consola de administración de seguridad que permita administrar, correlacionar y priorizar eventos permitiendo; seguimiento en tiempo real de ataques o usos indebidos, tratamiento de eventos, creación automática de incidentes y excepciones, en caso dicha consola debiese ser implementada fuera de los equipos NGFW, el contratista deberá proporcionar el equipamiento (appliance) necesario tal y como se ha estipulado previamente en el presente documento.

La solución deberá contar con una consola independiente externa para la gestión & correlación de log, la cual deberá ser del mismo fabricante del Firewall.

Debe permitir un almacenamiento mínimo de 2 TB (suma de todos los discos) para los logs, con el fin de “no” debe degradar la performance de la solución de Firewall; el cual no debe existir límite a nivel de licenciamiento con respecto a la cantidad de almacenamiento de cantidad de logs por día, almacenamiento total de logs, y capacidad de procesamiento de logs por segundo

Deberá contar como mínimo con 4 interfaces de cobre RJ45.

La mencionada consola deberá contar con las siguientes funcionalidades básicas:

- i. Debe permitir la administración y correlación de los logs de todos los equipos de seguridad ofertados.
- ii. Debe tener la funcionalidad de Administración de Políticas.
- iii. Debe soportar diferentes perfiles de administrador, incluyendo al menos los siguientes: read/write y read/only.
- iv. Las comunicaciones entre todos los componentes deben establecer comunicaciones seguras a través del uso de certificados para el cifrado.
- v. El sistema de administración centralizada debe soportar reportes en formato texto y gráfico, con exportación en los formatos PDF y CSV ó EXCEL.
- vi. El sistema de administración centralizada debe soportar la correlación de patrones de ataques (múltiples eventos identificados como un único ataque). Esto se refiere a que la solución ofertada sea lo suficientemente inteligente para que pueda identificar eventos similares y los pueda relacionar como una sola anomalía, con aplicaciones del mismo fabricante.
- vii. El sistema de administración centralizada debe soportar consola remota con interfaz gráfica (GUI) ó consola remota Web en formato gráfico para el uso en modo de consulta, perfiles diferentes de usuarios.
- ix. El sistema de administración debe proveer la capacidad de visualizar las versiones de software y hardware de los equipos desde la consola principal y desde cada equipo por separado.
- x. El sistema de administración centralizada debe soportar auditoria de las actividades de los usuarios.
- xi. El sistema de administración centralizada debe soportar actualización remota de los equipos.
- xii. El sistema de administración centralizada debe generar reportes en forma automática y enviarlos a una cuenta de correo electrónico para agilizar el proceso de análisis.
- xiii. El sistema de administración centralizada debe contar con herramientas integradas para tener visibilidad en forma de graficas en tiempo real e historial sobre el estado de salud, como mínimo de: CPU, interfaces, memoria, performance, disco, temperatura.
- xiv. El sistema de administración centralizada debe tener la posibilidad de realizar análisis de inteligencia con facilidad. Ello incluye análisis basados en el contexto lógico del evento siendo evaluado. El usuario debe poder navegar y analizar, con facilidad, más de un millón de eventos al día.
- xv. El sistema de administración centralizada debe incluir reportes previamente definidos. La consola debe tener la capacidad de producir métricas gráficas y reportes de comparación con base en segmentos de tiempo. La información en los reportes debe estar disponible para un grupo de activos, para todo un sitio o para toda una empresa. Asimismo, el usuario debe poder llegar hasta estos reportes para visualizar los detalles pertinentes.
- xvi. El sistema de administración centralizada debe ser compatible con múltiples opciones para responder automáticamente a las amenazas detectas ya sea por alertas automatizados y/o remediación del Cortafuegos.
- xvii. El sistema de administración centralizada debe proporcionar la capacidad de seleccionar informes pre-definidos y la posibilidad completa de personalización y generación de nuevos reportes.
- xviii. El sistema de administración centralizada debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para permitir a los eventos y registro de datos sean compartidos con la red externa y las aplicaciones de gestión de seguridad, tales como plataformas de sistemas de gestión y registro de las herramientas de gestión.



2) Item 2 - SEGURIDAD NDR (NETWORK DETECTION AND RESPONSE)

1. Requerimientos generales del fabricante de la solución de NDR:

- a) El fabricante de la solución ofertada, debe tener un resultado igual o superior al 72% de efectividad en prevención de amenazas de día cero (Zero Day), en la última evaluación de ciberseguridad de "Next Generation Firewall (NGFW) Security Benchmark" realizada por MIERCOM el año 2023.
- b) El fabricante debe estar presente en el cuadrante de Líderes (Leaders) en los últimos 05 reportes de Gartner "Magic Quadrant for Enterprise Network Firewalls" (Cuadrante Mágico para Firewalls de Redes Empresariales).
- c) Deberá ofertar un appliance dimensionado para 1200 usuarios como mínimo

2. Requerimientos generales de la solución de NDR requerida:

- a) Se requiere una solución avanzada de NDR (Network Detection and Response) del tipo SaaS (Software as a Service) para el análisis, detección y respuesta ante amenazas cibernéticas en las redes de datos corporativas, que permite tener una visibilidad completa de las amenazas y contar con la automatización para las operaciones de seguridad.
- b) El servicio debe operar desde la propia nube del fabricante y deberá ser del propio fabricante de los equipos de seguridad firewall y/o appliances de emulación de amenazas pre-existentes en la entidad.
- c) El servicio deberá recopilar información y telemetría desde los sensores de red instalados localmente en las instalaciones del cliente. *(Se solicita un (01) equipo del tipo appliance. Los equipos de red de OSIPTEL enviarán el tráfico al appliance NDR mediante port mirror/SPAN y vlan mirror/SPAN. Dicho sensor debe contar con al menos 08 interfaces de 01 Gbps para conectar a los diversos segmentos de red a analizar como parte de la función de NDR).*⁴⁸
- d) El fabricante deberá ser responsable de la operatividad, disponibilidad y actualizaciones de la plataforma NDR en la nube, durante toda la vigencia del soporte técnico.

3. Funcionalidades de la solución de NDR requerida:

- a) La solución NDR debe descubrir, investigar y responder ante los ataques o eventos de seguridad de manera oportuna e inteligente. Debe emplear tecnología de IA (inteligencia artificial) para la visibilidad de la red en tiempo real en los entornos de nube pública, privada y en las instalaciones (on-premise).
- b) La identificación de amenazas se debe realizar de manera automática a través de los sensores NDR. Se debe emplear técnicas de IA complementado con técnicas de visualización avanzadas para permitir a los analistas de seguridad, identificar aquellos ataques que evadieron otras defensas o medidas de seguridad.
- c) Los sensores NDR no deben requerir ninguna regla de configuración o política, ni tampoco una modificación en el enrutamiento o la topología de la red. Los sensores NDR se conectan en modo de monitor para procesar el tráfico reflejado (port-span) y/o en modo de puente (bridge on-line).
- d) Los sensores NDR deben procesar todo el tráfico de red Norte/Sur y Este/Oeste, sin ningún tipo de impacto en el.
- e) La solución de NDR debe ser capaz de identificar tráfico anómalo, activos vulnerables e infectados, movimiento lateral, comportamiento sospechoso de usuarios y aplicaciones.
- f) Capacidades de Identificación y Captura:

- La solución de NDR, incorpora, consolida y correlaciona los registros de eventos de los sensores físicos y/o virtuales, combinando visibilidad local, perimetral y de red en la nube del fabricante para ser analizada y presentado en una consola única de Ciberseguridad.

- La solución de NDR nos brinda visualización de aplicaciones y amenazas en tiempo real, aprovechando las capacidades de inteligencia de amenazas con las que cuenta el fabricante en su propia infraestructura de nube y las complementa con una amplia base de evaluación de riesgos y finger-print de aplicaciones, para detectar cualquier anomalía. La combinación de técnicas de IA e inteligencia en nube, brinda información inmediata sobre los patrones de tráfico y reduce el nivel de ruido o falso-positivos.

- La solución de NDR debe brindar clasificación del tráfico de red anómalo, empleando una combinación de análisis automatizado y análisis humano, que en conjunto entreguen información oportuna, precisa y relevante para una respuesta eficaz ante los ataques cibernéticos. Mediante los controles automatizados se deben detectar comportamientos anómalos, y mediante la inteligencia humana se debe identificar patrones de comportamiento no autorizado, descartar falsos positivos, categorizar eventos por motivo e intención e identificar cursos de acción efectivos y seguros. Esta metodología empleada en la solución NDR nos debe permitir la identificación de los vectores de ataque iniciales, así como los hosts y datos comprometidos posteriormente.

- La solución de NDR debe emplear análisis de comportamiento (Behavior Analytics) mediante motores de IA para identificar el comportamiento de red malicioso, y posteriormente generar automáticamente los Indicadores de Compromiso (IoC).

- La solución de NDR debe brindar una topología de amenazas y mapeo de actividad, que permita ver el tráfico de red, flujo de datos y comportamiento anómalo.

⁴⁸ Se agrega en las bases de acuerdo a la consulta N° 01 del participante IT BUSINESS & SUPPORT SOCIEDAD ANONIMA CERRADA - ITB SUPPORT S.A.C.

- La solución de NDR debe tener capacidad de integración con soluciones SIEM y SOAR, y también la definir la captura selectiva de paquetes como parte del análisis.

g) Capacidades de Prevención:

- La solución de NDR debe tener capacidad de prevención en la cadena de eliminación de amenazas (kill-chain), tanto antes como después de la infección. *(el sensor NDR debe contar con un rendimiento para análisis de prevención de amenazas de 2.5 Gbps, considerando las capacidades de análisis de anti-bot, antivirus y malware de día cero, en condiciones de tráfico empresarial y/o tráfico mixto).*⁴⁹

- La solución de NDR debe mostrar los IoC (Indicadores de Compromiso) que deben bloquearse en la red.

- La solución de NDR debe permitir la automatización de repositorios de IoC administrados. Los tipos de indicadores de IoC admitidos incluyen: la reputación de IP y URL, el hash de archivos y aplicaciones (MD5 y SHA), los campos de correo electrónico, así como las firmas de Snort y Yara.

- Los indicadores de IoC se pueden introducir en la solución NDR utilizando formatos y protocolos estándar de la industria, tales como las API STIX/TAXII, CSV y REST.



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:

⁴⁹ Se agrega en las bases de acuerdo la consulta N° 03 del participante UNITY PERU S.A.C.

3.2. REQUISITOS DE CALIFICACIÓN

A	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 1 000 000.00 (Un Millón y 00/100 Soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran bienes similares a los siguientes:</p> <ul style="list-style-type: none"> • Equipamiento y/o soluciones de seguridad informática. • Equipos y/o soluciones de respuesta ante incidentes informáticos. • Equipos y/o soluciones de seguridad en infraestructura tecnológica. • Equipos y/o soluciones para outsourcing de tecnología y/o TI • Equipos y/o soluciones de infraestructura tecnológica en centro de datos: redes, comunicaciones, seguridad, procesamiento, etc. • Garantías comerciales de equipamiento informático, soporte técnico y/o tecnológico, servicios de mesa de ayuda, service desk o help desk. • Solución de balanceador⁵⁰ • Equipos firewall⁵¹ • Equipamiento y/o soluciones de infraestructura tecnológica en centro de datos: redes, comunicaciones, seguridad, procesamiento también se considerarán balanceadores de enlaces y/o switches en general y/o servidores.⁵² <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 pago⁵³, 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 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.</p> <p>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</p>

⁵⁰ Se agrega a las bases de acuerdo a la consulta N° 27 del participante TELEFONICA DEL PERU SAA

⁵¹ Se agrega a las bases de acuerdo a la consulta N° 35 del participante AI INVERSIONES PALO ALTO II S.A.C.

⁵² Se agrega a las bases de acuerdo a la consulta N° 36 del participante AI INVERSIONES PALO ALTO II S.A.C.

⁵³ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

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

(...)

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

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".

B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.1	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <ul style="list-style-type: none"> • Un (01) "Especialista implementador en seguridad y redes" Experiencia laboral mínima de cuatro (04)⁵⁴ años como implementador de soluciones de ciberseguridad, seguridad informática y/o tecnología de la información. • Un (01) "Especialista de soporte en seguridad y redes" Experiencia laboral mínima de un (01) año⁵⁵ como gestor de soporte y/o mesa de ayuda y/o soporte técnico de seguridad informática y/o equipamiento de tecnología de la información. <p><u>Acreditación:</u></p> <p>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.</p> <div data-bbox="311 1332 1441 1803"> <p>Importante</p> <ul style="list-style-type: none"> • <i>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.</i> • <i>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.</i> • <i>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.</i> • <i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i> </div>

Importante

⁵⁴ Se cambia en las bases de acuerdo a la consulta N° 21 del participante TELEFONICA DEL PERU SAA

⁵⁵ Se cambia en las bases de acuerdo a la consulta N° 02 del participante IT BUSINESS & SUPPORT SOCIEDAD ANONIMA CERRADA - ITB SUPPORT S.A.C. y consulta N° 28 del participante TELEFONICA DEL PERU SAA

- *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	
<p><u>Evaluación:</u></p> <p>Se evaluará considerando el precio ofertado por el postor.</p> <p><u>Acreditación:</u></p> <p>Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).</p>	<p>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> $P_i = \frac{O_m \times PMP}{O_i}$ <p> <i>i</i> = Oferta <i>P_i</i> = Puntaje de la oferta a evaluar <i>O_i</i> = Precio <i>i</i> <i>O_m</i> = Precio de la oferta más baja <i>PMP</i> = Puntaje máximo del precio </p> <p style="text-align: right;">100 puntos</p>
PUNTAJE TOTAL	100 puntos⁵⁶

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.

⁵⁶ 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 del “Proyecto de Seguridad de Infraestructura Tecnológica”, que celebra de una parte el **Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL**, en adelante **LA ENTIDAD**, con RUC N° 20216072155, con domicilio legal en Calle De La Prosa N° 136 – San Borja, 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° 001-2023/OSIPTEL** para la contratación del “Proyecto de Seguridad de Infraestructura Tecnológica”, 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 la contratación del “Proyecto de Seguridad de Infraestructura Tecnológica”.

CLÁUSULA TERCERA: MONTO CONTRACTUAL

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

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 PAGO⁵⁷

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en soles, en pagos a cuenta, de acuerdo al siguiente detalle:

1. **Prestación Principal: Equipamiento:** Se pagará el 100% del monto total de la Prestación Principal: Equipamiento, previa conformidad de la misma.
2. **Prestación Accesorio: Gestión del Servicio:** Se pagará el monto de la prestación accesorio de manera prorrateada en treinta y seis (36) partes iguales de manera mensual, contabilizando a partir del día siguiente de la firma del “**Acta de Entrega, Implementación y Puesta en Operación del Equipamiento**” (ver apartado “**Sobre la adquisición de los bienes**”), previa conformidad del área usuaria.

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.

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

⁵⁷ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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 75 días calendario, el mismo que se computa desde el día siguiente de la firma de contrato, de acuerdo al siguiente detalle:

- i. **Entrega, Implementación y Puesta en operación del Equipamiento**
 1. Todo el equipamiento provisto por el contratista deberá ser entregado, instalado, configurado y/o afinado, y puesto en operación en las oficinas de la institución dentro de los 75 días calendarios contados a partir del día siguiente de la firma de contrato⁵⁸.
 2. Dentro de este periodo deben considerarse las labores de configuración/reconfiguración/afinamiento que sea necesario realizar sobre el equipamiento propiedad de la institución a fin de garantizar un óptimo desempeño de la plataforma tecnológica institucional⁵⁹. Todas estas labores deberán ser ejecutadas por el contratista⁶⁰ sin costo adicional para la institución.
 3. Hitos
 - a. Inicio del periodo: al día siguiente de la firma del contrato
 - b. **Plan de Implementación:** se debe presentar como máximo a los 7 días siguientes de la firma del contrato.
 - c. **Acta de Aceptación de Plan de Implementación:** se debe firmar como máximo a los 14 días siguientes de la firma del contrato
 - d. **Acta de Entrega, Implementación y Puesta en Operación del Equipamiento** dentro de los 75 días del plazo de la prestación principal.

CLÁUSULA SEXTA: PRESTACIONES ACCESORIAS⁶¹

Las prestaciones accesorias tienen por objeto la Gestión del Servicio, de acuerdo al siguiente detalle:

- A. Mantenimiento preventivo y correctivo por parte del contratista
- B. Soporte remoto e implementación de políticas de seguridad
- C. Transferencia de conocimiento y capacitación

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

El plazo de ejecución de las prestaciones accesorias es de treinta y seis (36) meses, el mismo que se computa desde el día siguiente de la firma del “Acta de Entrega, Implementación y Puesta en Operación del Equipamiento”, de acuerdo al siguiente detalle:

- i. **Inicio del servicio**

⁵⁸ Aplica también para equipamiento en nube pública.

⁵⁹ Esto incluye también las labores de retiro de operación y/o transferencia de configuraciones del equipamiento (propiedad de la institución) que la institución considere que ya no va a ser requerido luego de la implementación del presente servicio (ejemplo: cortafuegos, enrutadores, filtro de contenidos, entre otros).

⁶⁰ El contratista es íntegramente responsable de las actividades que lleve a cabo su equipo humano y de las consecuencias que éstas pudiesen tener en la infraestructura de la institución, debiendo subsanar junto a la entidad ante cualquier incidente que se pudiese presentar como producto del accionar de éste (ejemplos: reconfiguración de equipos, reposición de cables y conectores, reposición de equipos, entre otros.).

⁶¹ 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.



El servicio dará inicio al día siguiente de la firma del “Acta de Entrega, Implementación y Puesta en Operación del Equipamiento”

A. Mantenimiento preventivo y correctivo por parte del contratista

36 meses

B. Soporte remoto e implementación de políticas de seguridad

6 meses

C. Transferencia de conocimiento y capacitación

Hasta 2 meses después de concluido el servicio de soporte remoto e implementación de políticas de seguridad.

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:

- De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la Carta Fianza 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.
- Garantía fiel cumplimiento por prestaciones accesorias: [CONSIGNAR EL MONTO], a través de la Carta Fianza 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 de los bienes de la prestación principal será otorgada por área de almacén y la conformidad se dará de la siguiente manera:

4. La conformidad sobre la prestación principal: equipamiento se emitirá luego de presentados los siguientes entregables:
 - a. Ficha de contactos.
 - b. Plan de implementación (adjuntando la respectiva “Acta de Aceptación de Plan de Implementación”).
 - c. Carta de garantía del fabricante.
 - d. Acta de Entrega, Implementación y Puesta en Operación del Equipamiento.
5. La conformidad sobre la Prestación Accesorias: Gestión del Servicio se dará mensualmente; y se emitirá luego de presentado el “**Informe mensual del servicio**” por parte del contratista.

Las conformidades se darán en el plazo máximo de [CONSIGNAR SIETE (7) DÍAS O MÁXIMO QUINCE (15) DÍAS, EN CASO SE REQUIERA EFECTUAR PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LA OBLIGACIÓN] días de producida la recepción de los



entregables requeridos.

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 un (01) año contado a partir de la conformidad 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

- d. Se aplicarán penalidades siempre que se atribuya al contratista responsabilidad sobre el incumplimiento de los niveles de servicio estipulados en el punto anterior o en el presente documento.
- e. Las penalidades contempladas serán cobradas por el OSIPTEL, de manera automática, de cualquier pago pendiente, además, serán ejecutadas sin perjuicio de la ejecución de



garantías de fiel cumplimiento de contrato, la aplicación de otras penalidades, la resolución del contrato, la responsabilidad civil y las acciones legales pertinentes.

- f. En la **Tabla** se detallan las penalidades aplicables según los niveles de servicio incumplidos.

Ítem	Condición	Factor de calculo	Procedimiento
1	Por incumplimiento en la presentación de la documentación indicada en el apartado "Entregables-Prestación Principal" .	1 UIT	Por cada entregable y por cada día calendario de retraso
2	Por incumplimiento en la presentación de la documentación indicada en el apartado "Entregables-Prestación Accesorio" .	5% de la UIT	Por cada entregable y por cada día calendario de retraso
3	Por incumplimiento en los tiempos de atención de solicitudes, solución de incidentes y problemas (ver apartado "Niveles de servicio").	10% de la UIT	Por cada Ocurrencia
4	Por incumplimiento en las labores de monitoreo (ver apartado "Gestión del servicio")	10% de la UIT	Por cada Ocurrencia ⁶²
5	Por incumplimiento de alguno de los puntos mencionados en el apartado "Confidencialidad"	5 UIT	Por cada Ocurrencia
6	Por incumplimiento de las condiciones establecidas en el "Acta de actividad de remediación"	10% de la UIT	Por cada Ocurrencia ⁶³
7	Por incumplir en mantener actualizada la plataforma de seguridad (Ver Ítem 3 de la "Tabla N° 01 : Niveles de servicio aplicables").	10% de la UIT	Por cada Ocurrencia

El % de la UIT se aplicará de acuerdo al momento en qué se realice la falta.

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.

⁶² En caso un incidente y/o alerta, notificada/advertida por la plataforma (ver apartado **"Gestión del servicio"**) y no atendida por un periodo mayor a 02 horas hábiles (dentro del período 5x8); se considerará como incumplimiento sobre las tareas de monitoreo y, por ende, se procederá a aplicar la penalidad especificada.

⁶³ En caso las actividades no sean completadas en el transcurso del mes en el que se hubiese acordado, el OSIPTEL se reserva el derecho de aplicar la penalidad indicada en los meses sucesivos hasta que la falta haya sido subsanada.

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 CONTROVERSIAS⁶⁴

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: CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACION

LA ENTIDAD precisa que en el ítem 6.10 – Relación con proveedores – del documento de “*Políticas de seguridad de la información – PO-PE01.2.3-001*”⁶⁵ se encuentran considerados los lineamientos correspondientes a fin de cautelar la seguridad de la información por parte del OSIPTEL.

EL CONTRATISTA se obliga a conservar y tratar como reservada toda la información que se declare como Información Confidencial.

La Información Confidencial no será revelada en ningún caso y bajo ningún motivo por EL CONTRATISTA, sin el consentimiento previo y por escrito de LA ENTIDAD, salvo por lo dispuesto en la presente cláusula. En este sentido, EL CONTRATISTA se compromete a limitar el acceso a la Información Confidencial de forma tal que sólo sea accesible a aquellas personas que necesariamente deban involucrarse en las conversaciones, tratativas y/o acuerdos mantenidos con LA ENTIDAD.

EL CONTRATISTA se compromete a no divulgar ni transferir a terceros la información a la que pudiera tener acceso él o su personal, siendo que, de ser el caso, EL CONTRATISTA responderá

⁶⁴ 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).

⁶⁵ Información que se brindará al momento de la suscripción de este contrato, mediante el acta respectiva.



legalmente por los daños y perjuicios causados.

EL CONTRATISTA se compromete a guardar la Información Confidencial en un archivo especial que posea las condiciones suficientes de seguridad.

CLÁUSULA VIGÉSIMA: 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 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: Calle de La Prosa N° 136 – San Borja

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 Digitales⁶⁶.

⁶⁶ 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° 001-2023/OSIPTEL

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 compra⁶⁷

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.

⁶⁷ 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.

Importante

Cuando se trate de consorcios, la declaración jurada es la siguiente:

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 001-2023/OSIPTEL

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 compra⁶⁸

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]

⁶⁸ 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.

.....
**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.



ANEXO N° 2

DECLARACIÓN JURADA (ART. 52 DEL REGLAMENTO DE LA LEY DE CONTRATACIONES DEL ESTADO)

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 001-2023/OSIPTEL
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.



Documento adjunto del Anexo 2 – Bases de Procedimientos de Selección

Decreto Supremo N° 082-2019-EF – TUO Ley 30225

Artículo 11. Impedimento

11.1 Cualquiera sea el régimen legal de contratación aplicable, están impedidos de ser participantes, postores, contratistas y/o subcontratistas, incluso en las contrataciones a que se refiere el literal a) del artículo 5, las siguientes personas:

a) El Presidente y los Vicepresidentes de la República, los Congresistas de la República, los Jueces Supremos de la Corte Suprema de Justicia de la República, los titulares y los miembros del órgano colegiado de los Organismos Constitucionales Autónomos, en todo proceso de contratación mientras ejerzan el cargo y hasta doce (12) meses después de haber dejado el mismo.

b) Los Ministros y Viceministros de Estado en todo proceso de contratación mientras ejerzan el cargo; luego de dejar el cargo, el impedimento establecido para estos subsiste hasta (12) meses después y solo en el ámbito de su sector.

c) Los Gobernadores, Vicegobernadores y Consejeros de los Gobiernos Regionales. En el caso de los Gobernadores y Vicegobernadores, el impedimento aplica para todo proceso de contratación mientras ejerzan el cargo; luego de dejar el cargo, el impedimento establecido para estos subsiste hasta doce (12) meses después y solo en el ámbito de su competencia territorial. En el caso de los Consejeros de los Gobiernos Regionales, el impedimento aplica para todo proceso de contratación en el ámbito de su competencia territorial durante el ejercicio del cargo y hasta doce (12) meses después de haber concluido el mismo.

d) Los Jueces de las Cortes Superiores de Justicia, los Alcaldes y los Regidores. Tratándose de los Jueces de las Cortes Superiores y de los Alcaldes, el impedimento aplica para todo proceso de contratación durante el ejercicio del cargo; luego de dejar el cargo, el impedimento establecido para estos subsiste hasta doce (12) meses después y solo en el ámbito de su competencia territorial. En el caso de los Regidores el impedimento aplica para todo proceso de contratación en el ámbito de su competencia territorial, durante el ejercicio del cargo y hasta doce (12) meses después de haber concluido el mismo.

e) Los titulares de instituciones o de organismos públicos del Poder Ejecutivo, los funcionarios públicos, empleados de confianza, servidores públicos con poder de dirección o decisión, según la ley especial de la materia, y los gerentes de las empresas del Estado. El impedimento se aplica para todo proceso de contratación durante el ejercicio del cargo; luego de culminado el mismo hasta doce (12) meses después sólo en la entidad a la que pertenecieron. Los directores de las empresas del Estado y los miembros de los Consejos Directivos de los organismos públicos del Poder Ejecutivo se encuentran impedidos en el ámbito de la Entidad a la que pertenecen, mientras ejercen el cargo y hasta doce (12) meses después de haber culminado el mismo.

f) Los servidores públicos no comprendidos en literal anterior, y los trabajadores de las empresas del Estado, en todo proceso de contratación en la Entidad a la que pertenecen, mientras ejercen su función. Luego de haber concluido su función y hasta doce (12) meses después, el impedimento se aplica para los procesos de contratación en la Entidad a la que pertenecieron, siempre que por la función desempeñada dichas personas hayan tenido influencia, poder de decisión, información privilegiada referida a tales procesos o conflicto de intereses.

g) En el proceso de contratación correspondiente, las personas naturales o jurídicas que tengan intervención directa en cualquiera de las siguientes actuaciones: i) determinación de las características técnicas y/o valor referencial o valor estimado, ii) elaboración de documentos del procedimiento de selección, iii) calificación y evaluación de ofertas, y iv) la conformidad de los contratos derivados de dicho procedimiento, salvo en el caso de los contratos de supervisión. Tratándose de personas jurídicas el impedimento le alcanza si la referida intervención se produce a través de personas que se vinculan a esta.

h) El cónyuge, conviviente o los parientes hasta el segundo grado de consanguinidad o afinidad de las personas señaladas en los literales precedentes, de acuerdo a los siguientes criterios:

(i) Cuando la relación existe con las personas comprendidas en los literales a) y b), el impedimento se configura respecto del mismo ámbito y por igual tiempo que los establecidos para cada una de estas;

(ii) Cuando la relación existe con las personas comprendidas en los literales c) y d), el impedimento se configura en el ámbito de competencia territorial mientras estas personas ejercen el cargo y hasta doce (12) meses después de concluido;

(iii) Cuando la relación existe con las personas comprendidas en el literal e), el impedimento se configura en la Entidad a la que pertenecen estas personas mientras ejercen el cargo y hasta doce (12) meses después de concluido;



(iv) Cuando la relación existe con las personas comprendidas en los literales f) y g), el impedimento tiene el mismo alcance al referido en los citados literales.

i) En el ámbito y tiempo establecidos para las personas señaladas en los literales precedentes, las personas jurídicas en las que aquellas tengan o hayan tenido una participación individual o conjunta superior al treinta por ciento (30%) del capital o patrimonio social, dentro de los doce (12) meses anteriores a la convocatoria del respectivo procedimiento de selección.

j) En el ámbito y tiempo establecido para las personas señaladas en los literales precedentes, las personas jurídicas sin fines de lucro en las que aquellas participen o hayan participado como asociados o miembros de sus consejos directivos, dentro de los doce (12) meses anteriores a la convocatoria del respectivo procedimiento de selección.

k) En el ámbito y tiempo establecidos para las personas señaladas en los literales precedentes, las personas jurídicas cuyos integrantes de los órganos de administración, apoderados o representantes legales sean las referidas personas. Idéntica prohibición se extiende a las personas naturales que tengan como apoderados o representantes a las citadas personas.

l) En todo proceso de contratación, las personas naturales o jurídicas inhabilitadas o suspendidas para contratar con el Estado.

m) En todo proceso de contratación, las personas condenadas, en el país o el extranjero, mediante sentencia consentida o ejecutoriada por delitos de concusión, peculado, corrupción de funcionarios, enriquecimiento ilícito, tráfico de influencias, delitos cometidos en remates o procedimientos de selección, o delitos equivalentes en caso estos hayan sido cometidos en otros países. El impedimento se extiende a las personas que, directamente o a través de sus representantes, hubiesen admitido y/o reconocido la comisión de cualquiera de los delitos antes descritos ante alguna autoridad nacional o extranjera competente.

n) En todo proceso de contratación, las personas jurídicas cuyos representantes legales o personas vinculadas que (i) hubiesen sido condenadas, en el país o el extranjero, mediante sentencia consentida o ejecutoriada por delitos de concusión, peculado, corrupción de funcionarios, enriquecimiento ilícito, tráfico de influencias, delitos cometidos en remates o procedimientos de selección, o delitos equivalentes en caso estos hayan sido cometidos en otros países; o, (ii) directamente o a través de sus representantes, hubiesen admitido y/o reconocido la comisión de cualquiera de los delitos antes descritos ante alguna autoridad nacional o extranjera competente. Tratándose de consorcios, el impedimento se extiende a los representantes legales o personas vinculadas a cualquiera de los integrantes del consorcio.

o) En todo proceso de contratación, las personas naturales o jurídicas a través de las cuales, por razón de las personas que las representan, las constituyen o participan en su accionariado o cualquier otra circunstancia comprobable se determine que son continuación, derivación, sucesión, o testafierro, de otra persona impedida o inhabilitada, o que de alguna manera esta posee su control efectivo, independientemente de la forma jurídica empleada para eludir dicha restricción, tales como fusión, escisión, reorganización, transformación o similares.

p) En un mismo procedimiento de selección las personas naturales o jurídicas que pertenezcan a un mismo grupo económico, conforme se define en el reglamento.

q) En todo proceso de contratación, las personas inscritas en el Registro de Deudores de Reparaciones Civiles (REDERECL), sea en nombre propio o a través de persona jurídica en la que sea accionista u otro similar, con excepción de las empresas que cotizan acciones en bolsa. Asimismo, las personas inscritas en el Registro Nacional de Abogados Sancionados por Mala Práctica Profesional y en el Registro Nacional de Sanciones de Destitución y Despido, por el tiempo que establezca la ley de la materia; así como en todos los otros registros creados por Ley que impidan contratar con el Estado.

r) Las personas jurídicas nacionales o extranjeras que hubiesen efectuado aportes a organizaciones políticas durante un proceso electoral, por todo el período de gobierno representativo y dentro de la circunscripción en la cual la organización política beneficiada con el aporte ganó el proceso electoral que corresponda.

s) En todo proceso de contratación y siempre que cuenten con el mismo objeto social, las personas jurídicas cuyos integrantes formen o hayan formado parte en la fecha en que se cometió la infracción, de personas jurídicas que se encuentren sancionadas administrativamente con inhabilitación temporal o permanente para participar en procedimientos de selección y para contratar con el Estado. El impedimento también es aplicable a la persona jurídica cuyos integrantes se encuentren sancionados administrativamente con inhabilitación temporal o permanente para participar en procedimientos de selección y para contratar con el Estado. Para estos efectos, por integrantes se entiende a los representantes legales, integrantes de los órganos de administración, socios, accionistas, participacionistas o titulares. Para el caso de socios, accionistas, participacionistas o titulares, el impedimento es aplicable siempre que su participación individual o conjunta sea superior al treinta por ciento (30%) del capital o patrimonio social y por el tiempo que la sanción se encuentre vigente.

t) En todo proceso de contratación, las personas naturales o jurídicas que se encuentren comprendidas en las Listas de Organismos Multilaterales de personas y empresas no elegibles para ser contratadas. (*)



(*) De conformidad con el Numeral 2 del Acuerdo de la Sala Plena N° 008-2020-TCE, publicado el 16 octubre 2020, cuando, por norma especial, el ejercicio de la docencia u otra actividad, adicional a su cargo, sea permitido a las personas (naturales) comprendidas en los literales a), b), c), d) y e) del numeral 11.1 del artículo 11 de la LCE, el perfeccionamiento de un contrato de naturaleza laboral o de un contrato administrativo de servicios, para dicho efecto, no configura la infracción tipificada en el literal c) del numeral 50.1 del artículo 50 de dicha Ley, consistente en Contratar con el Estado estando impedido.

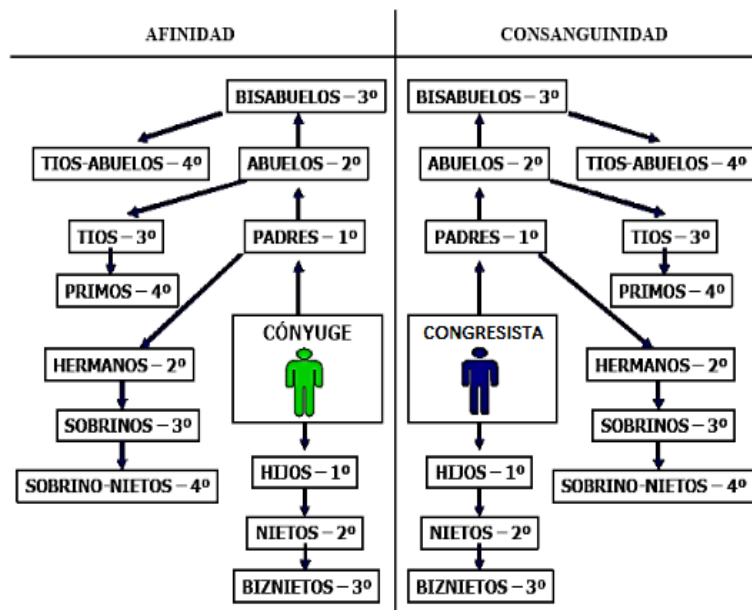
(*) De conformidad con el Numeral 1 del Acuerdo de la Sala Plena N° 003-2021-TCE, publicado el 07 abril 2021, los impedimentos para contratar con el Estado aplicables a los funcionarios o servidores públicos mencionados en los literales a), b), c), d) y e) del presente numeral, no son extensibles a su labor docente, tanto cuando ésta se ejerce bajo un régimen laboral como de locación de servicios.

(*) De conformidad con el Numeral 1 del Acuerdo de Sala Plena N° 006-2021/TCE, publicada el 27 octubre 2021, los Gobernadores, Vicegobernadores, Consejeros de los Gobiernos Regionales, Jueces de las Cortes Superiores de Justicia, Alcaldes y Regidores a los que se refieren los literales c) y d) del presente numeral, están impedidos de contratar con entidades públicas con sede en el ámbito de su competencia territorial, en los siguientes supuestos: i. En el caso de Gobernador, Vicegobernador, Alcalde y Juez de una Corte Superior de Justicia, luego de dejar el cargo y hasta por un periodo de doce (12) meses, el impedimento será con entidades públicas cuyas sedes se encuentren ubicadas en el espacio geográfico en el que han ejercido su competencia. Sin perjuicio del impedimento que se encuentre vigente durante el ejercicio del cargo, para todo proceso de contratación. ii. En el caso de Consejero de Gobierno Regional y Regidor de un gobierno local, el impedimento será durante el ejercicio del cargo y hasta por un periodo de doce (12) meses después de haber dejado el cargo con entidades públicas cuyas sedes se encuentren ubicadas en el espacio geográfico en el que ejercen o han ejercido su competencia. Los criterios desarrollados en el citado numeral son de aplicación a los impedimentos que vinculan a los parientes o a las personas jurídicas en las cuales los Gobernadores, Vicegobernadores, Consejeros de los Gobiernos Regionales, Jueces de las Cortes Superiores de Justicia, Alcaldes y Regidores, o sus parientes, tienen participación, conforme a lo dispuesto en los literales h), i), j) y k) del presente numeral.

11.2 El incumplimiento de lo establecido en el presente artículo conlleva las consecuencias y responsabilidades establecidas en la Ley.

(Texto modificado por la Segunda Disposición Complementaria Modificatoria de la Ley N° 30353, el artículo 1 del Decreto Legislativo N° 1341, el artículo 3 de la Ley N° 30689 y el artículo 2 del Decreto Legislativo N° 1444)

CÓMPUTO DE LOS GRADOS DE PARENTESCO



ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 001-2023/OSIPTEL

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 “Proyecto de Seguridad de Infraestructura Tecnológica”, 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° 001-2023/OSIPTEL

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 siguiente plazo:

Plazo de la Prestación Principal:

i. **Entrega, Implementación y Puesta en operación del Equipamiento**

1. Todo el equipamiento provisto por el contratista deberá ser entregado, instalado, configurado y/o afinado, y puesto en operación en las oficinas de la institución dentro de los 75 días calendarios contados a partir del día siguiente de la firma de contrato⁶⁹.
2. Dentro de este periodo deben considerarse las labores de configuración/reconfiguración/afinamiento que sea necesario realizar sobre el equipamiento propiedad de la institución a fin de garantizar un óptimo desempeño de la plataforma tecnológica institucional⁷⁰. Todas estas labores deberán ser ejecutadas por el contratista⁷¹ sin costo adicional para la institución.
3. Hitos
 - a. Inicio del periodo: al día siguiente de la firma del contrato
 - b. **Plan de Implementación:** se debe presentar como máximo a los 7 días siguientes de la firma del contrato.
 - c. **Acta de Aceptación de Plan de Implementación:** se debe firmar como máximo a los 14 días siguientes de la firma del contrato
 - d. **Acta de Entrega, Implementación y Puesta en Operación del Equipamiento** dentro de los 75 días del plazo de la prestación principal.

Plazo de la Prestación Accesoría:

iii. **Inicio del servicio**

El servicio dará inicio al día siguiente de la firma del "Acta de Entrega, Implementación y Puesta en Operación del Equipamiento"

A. Mantenimiento preventivo y correctivo por parte del contratista

36 meses

B. Soporte remoto e implementación de políticas de seguridad

6 meses

C. Transferencia de conocimiento y capacitación

Hasta 2 meses después de concluido el servicio de soporte remoto e implementación de políticas de seguridad

[CONSIGNAR CIUDAD Y FECHA]



.....
**Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda**

⁶⁹ Aplica también para equipamiento en nube pública.

⁷⁰ Esto incluye también las labores de retiro de operación y/o transferencia de configuraciones del equipamiento (propiedad de la institución) que la institución considere que ya no va a ser requerido luego de la implementación del presente servicio (ejemplo: cortafuegos, enrutadores, filtro de contenidos, entre otros).

⁷¹ El contratista es íntegramente responsable de las actividades que lleve a cabo su equipo humano y de las consecuencias que éstas pudiesen tener en la infraestructura de la institución, debiendo subsanar junto a la entidad ante cualquier incidente que se pudiese presentar como producto del accionar de éste (ejemplos: reconfiguración de equipos, reposición de cables y conectores, reposición de equipos, entre otros.).

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° 001-2023/OSIPTEL

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° 001-2023/OSIPTEL**.

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] [%]⁷²

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]⁷³

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%⁷⁴

[CONSIGNAR CIUDAD Y FECHA]

⁷² Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

⁷³ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

⁷⁴ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.



.....
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.



ANEXO N° 6

PRECIO DE LA OFERTA

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 001-2023/OSIPTEL

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
Ítem Paquete N° 01	Prestación Principal:	Seguridad Perimetral: Cortafuegos	
		Seguridad NDR (Network Detection and Response)	
	Prestación Accesorio:	Gestión del Servicio	
TOTAL			

El precio de la oferta en soles 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.

El postor debe detallar en el precio de su oferta, el monto correspondiente a la prestación principal y las prestaciones accesorias.

[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]"



ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 001-2023/OSIPTEL
Presente.-

Mediante el presente, el suscrito detalla la siguiente EXPERIENCIA EN LA ESPECIALIDAD:

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ⁷⁵	FECHA DE LA CONFORMIDAD DE SER EL CASO ⁷⁶	EXPERIENCIA PROVENIENTE ⁷⁷ DE:	MONEDA	IMPORTE ⁷⁸	TIPO DE CAMBIO VENTA ⁷⁹	MONTO FACTURADO ACUMULADO ⁸⁰
1										
2										
3										

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.

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.

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”.

Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

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.

⁸⁰ Consignar en la moneda establecida en las bases.

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ⁷⁵	FECHA DE LA CONFORMIDAD DE SER EL CASO ⁷⁶	EXPERIENCIA PROVENIENTE ⁷⁷ DE:	MONEDA	IMPORTE ⁷⁸	TIPO DE CAMBIO VENTA ⁷⁹	MONTO FACTURADO ACUMULADO ⁸⁰
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° 001-2023/OSIPTEL
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/rmp/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° 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° 001-2023/OSIPTEL

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.





INFORMACIÓN DEL CCI

FECHA - -

Por medio del presente, informo al OSIPTEL los datos de mi representada:

NOMBRE O RAZON SOCIAL DEL PROVEEDOR

RUC

Y solicito dispongan que los pagos sean abonados en la siguiente cuenta corriente en moneda nacional perteneciente a mi representada, apertura con el RUC antes indicado y con Código de Cuenta Interbancarios (CCI) N°:

BANCO

CCI

 - - - -

En caso de ser persona natural, confirmo que he realizado las afiliaciones correspondientes ante la entidad financiera a fin de que el Código de Cuenta Interbancario (CCI) antes indicado, se encuentre debidamente asociado al número de RUC que he expuesto, lo cual es requisito indispensable para la cancelación del comprobante de pago emitido.

CONFIRMO LO ANTES EXPUESTO

SI

☐

Las personas naturales marcar con una "X"

Así mismo, dejo constancia que la factura a ser emitida por mi representada, una vez cumplida o atendida la correspondiente Orden de Compra y/o de Servicio o las prestaciones en bienes y/o servicios materia del contrato quedará cancelada para todos sus efectos mediante la sola acreditación del importe de la referida factura a favor de la cuenta en la entidad bancaria a que se refiere en el presente documento.

De efectuarse cambios en el número de la cuenta corriente, mi representada es responsable de comunicar al OSIPTEL el nuevo número de CCI.

Finalmente, ante cualquier eventualidad en el proceso de pago, detallo los datos de la persona a contactar:

NOMBRE DEL CONTACTO

CORREO ELECTRÓNICO

TELEFONOS

Atentamente,

Datos del representante legal:

FIRMA

NOMBRE

DNI

