

BASES ESTÁNDAR DE ADJUDICACIÓN SIMPLIFICADA PARA LA CONTRATACIÓN DE BIENES

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



Firmado digitalmente por CABRERA
REATEGUI Juan Ramon FAU
20306484479 soft
Motivo: Soy el autor del documento
Fecha: 20.11.2024 11:19:22 -05:00



Firmado digitalmente por CORTEZ
CANAZAS Hector FAU 20306484479
soft
Motivo: Soy el autor del documento
Fecha: 20.11.2024 11:24:40 -05:00



Firmado digitalmente por ARAUJO
CERRUTTI Manuel Alejandro FAU
20306484479 soft
Motivo: Soy el autor del documento
Fecha: 20.11.2024 10:57:25 -05:00

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

SIMBOLOGÍA UTILIZADA:

N°	Símbolo	Descripción
1	[ABC] / [.....]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / [.....]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	<div>Importante</div> <ul style="list-style-type: none"> • Abc 	Se refiere a consideraciones importantes a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y por los proveedores.
4	<div>Advertencia</div> <ul style="list-style-type: none"> • Abc 	Se refiere a advertencias a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y por los proveedores.
5	<div>Importante para la Entidad</div> <ul style="list-style-type: none"> • Xyz 	Se refiere a consideraciones importantes a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda, y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

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

N°	Características	Parámetros
1	Márgenes	Superior : 2.5 cm Inferior: 2.5 cm Izquierda: 2.5 cm Derecha: 2.5 cm
2	Fuente	Arial
3	Estilo de Fuente	Normal: Para el contenido en general Cursiva: Para el encabezado y pie de página Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
4	Color de Fuente	Automático: Para el contenido en general Azul : Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
5	Tamaño de Letra	16 : Para las dos primeras hojas de las Secciones General y Específica 11 : Para el nombre de los Capítulos. 10 : Para el cuerpo del documento en general 9 : Para el encabezado y pie de página Para el contenido de los cuadros, pudiendo variar, según la necesidad 8 : Para las Notas al pie
6	Alineación	Justificada: Para el contenido en general y notas al pie. Centrada : Para la primera página, los títulos de las Secciones y nombres de los Capítulos)
7	Interlineado	Sencillo
8	Espaciado	Anterior : 0 Posterior : 0
9	Subrayado	Para los nombres de las Secciones y para resaltar o hacer hincapié en algún concepto

INSTRUCCIONES DE USO:

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

Elaboradas en enero de 2019

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

**BASES ESTÁNDAR DE ADJUDICACIÓN SIMPLIFICADA
PARA LA CONTRATACIÓN DE BIENES**

**ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI
PRIMERA CONVOCATORIA**

**CONTRATACIÓN DE BIENES
“ADQUISICIÓN DE UN SISTEMA DE PROTECCIÓN Y
SEGURIDAD PARA RED – FIREWALL”**

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, así como el literal a) del artículo 89 del Reglamento.

Importante

No pueden formularse consultas ni observaciones respecto del contenido de una ficha de homologación aprobada. 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 el numeral 72.4 del artículo 72 del Reglamento y el literal a) del artículo 89 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. FORMA DE PRESENTACIÓN DE OFERTAS

Las ofertas se presentan conforme lo establecido en el artículo 59 y en el artículo 90 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

- *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.*

1.7. 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.

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>

En la apertura electrónica de la oferta, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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, detallados en la sección específica de las bases. De no cumplir con lo requerido, la oferta se considera no admitida.

1.8. EVALUACIÓN DE LAS OFERTAS

La evaluación de las ofertas se realiza conforme a lo establecido en el numeral 74.1 y el literal a) del numeral 74.2 del artículo 74 del Reglamento.

En el supuesto de que dos (2) o más ofertas empaten, la determinación del orden de prelación de las ofertas empatadas se efectúa siguiendo estrictamente el orden establecido en el numeral 91.1 del artículo 91 del Reglamento.

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

1.9. 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.

1.10. 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.

1.11. RECHAZO DE LAS OFERTAS

Previo al otorgamiento de la buena pro, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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 órgano encargado de las contrataciones o el comité de selección, según corresponda, revisa el cumplimiento de los requisitos de calificación de los postores que siguen en el orden de prelación, en caso las hubiere.

1.12. OTORGAMIENTO DE LA BUENA PRO

Definida la oferta ganadora, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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.

1.13. CONSENTIMIENTO DE LA BUENA PRO

Cuando se hayan presentado dos (2) o más ofertas, el consentimiento de la buena pro se produce a los cinco (5) 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 la Entidad convocante, y es conocido y resuelto por su Titular, cuando el valor estimado sea igual o menor a cincuenta (50) UIT. Cuando el valor estimado sea mayor a dicho monto, el recurso de apelación se presenta ante y es resuelto por el Tribunal de Contrataciones del Estado.

En los procedimientos de selección según relación de ítems, el valor estimado total del procedimiento determina ante quién se presenta el recurso de apelación.

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 órgano encargado de las contrataciones o el comité de selección, según corresponda, 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 órgano encargado de las contrataciones o el comité de selección, según corresponda.

- *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, o en la Unidad de Trámite Documentario de la Entidad, según corresponda.*

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 cinco (5) 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 cinco (5) 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.

El contrato se perfecciona con la suscripción del documento que lo contiene, salvo en los contratos cuyo monto del valor estimado no supere los doscientos mil Soles (S/ 200,000.00), en los que se puede perfeccionar con la recepción de la orden de compra, conforme a lo previsto en la sección específica de las bases.

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 valor estimado del ítem corresponda al parámetro establecido en el párrafo anterior.

Importante

El órgano encargado de las contrataciones o el comité de selección, según corresponda, debe consignar en la sección específica de las bases la forma en que se perfeccionará el contrato, sea con la suscripción del contrato o la recepción de la orden de compra. En caso la Entidad perfeccione el contrato con la recepción de la orden de compra no debe incluir la proforma del contrato establecida en el Capítulo V de la sección específica de las bases.

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 accesoria, la misma que debe ser renovada periódicamente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

En los contratos cuyos montos sean iguales o menores 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. Dicha excepción también aplica a 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 no superen el monto señalado anteriormente, 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>).

Advertencia

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 DE FORMALIZACIÓN DE LA PROPIEDAD INFORMAL – COFOPRI

RUC N° : 20306484479

Domicilio legal : AV. PASEO DE LA REPÚBLICA N° 3135 – 3137 SAN ISIDRO

Teléfono: : 319 - 3838

Correo electrónico: : jcabrera@cofopri.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación de la ADQUISICIÓN DE UN SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED - FIREWALL

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante MEMORANDO N° D001834-2024-COFOPRI-OA el 31 de octubre del 2024.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios

Importante

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

1.5. SISTEMA DE CONTRATACIÓN

El presente procedimiento se rige por el sistema de 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 de Treinta (30) días calendarios, que incluyen su instalación y puesta en funcionamiento y serán contabilizados a partir del día siguiente de la suscripción del contrato, en concordancia con lo establecido en el expediente de contratación.

1.10. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases del procedimiento, el cual es SIN COSTO PARA SU REPRESENTADA, para cuyo efecto deberá solicitarlo al correo jcabrera@cofopri.gob.pe o puede descargarlo del Sistema Electrónico de las Contrataciones del Estado – SEACE.

Importante

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

1.11. BASE LEGAL

- Ley N° 31953 Ley de Presupuesto del Sector Público para el Año Fiscal 2024
- Ley N° 31954 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2024.
- Ley N° - Decreto Legislativo 1440 – Sistema Nacional de Presupuesto Público,
- Texto Único Ordenado de la Ley N° 30225 – Ley de Contrataciones del Estado, aprobado por Decreto Supremo N° 082-2019-EF (en adelante La Ley)
- Reglamento de la Ley N° 30225 – Ley de Contrataciones del Estado, aprobado por Decreto Supremo N° 344-2018-EF (en adelante El Reglamento).
- Texto Único Ordenado de la Ley N° 27444 – Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS.
- Ley N° 27806 – Ley de Transparencia y de Acceso a la Información Pública.
- Ley N° 27815 – Ley del Código de Ética de la Función Pública.

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

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

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

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

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

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

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

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

Advertencia

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

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

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

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

- e) El postor deberá acreditar en la presentación de la propuesta, el cumplimiento de las especificaciones técnicas de los bienes provistos, con folletos y/o manuales y/o catálogos y/o brochures u otros documentos técnicos similares emitidos por el fabricante, siendo las características y/o requisitos funcionales de las especificaciones técnicas que deberán ser acreditados por el postor, los que se incluyen en las siguientes secciones y literales⁴:

<p>NEXT GENERATION FIREWALL</p> <p>A. DESCRIPCION: A3, A4.</p> <p>B. REQUERIMIENTOS SOPORTE: B1.</p> <p>C. CAPACIDAD DE RENDIMIENTO C1, C2, C3, C7, C8.</p> <p>D. CAPACIDADES DE NETWORKING D1, D2, D6.</p> <p>E. ALTA DISPONIBILIDAD E1, E4.</p> <p>F. FUNCIONALIDADES DE FIREWALL: F2, F4.</p> <p>G. DESCIFRADO DE TRÁFICO SSL/TLS: G2, G3, G4, G7.</p> <p>H. PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (DoS): H1, H3, H5.</p> <p>I. VISIBILIDAD EN CAPA 7 Y CONTROL DE APLICACIONES: I1, I3, I5, I6.</p> <p>J. PREVENCIÓN DE AMENAZAS: J1, J3, J6, J7, J9, J10, J11, J13.</p> <p>K. PREVENCIÓN DE AMENAZAS AVANZADAS EN DNS: K1, K3, K5.</p> <p>L. SANDBOXING: L1, L2, L3, L6, L7, L9, L11, L13.</p> <p>M. FILTRO DE CONTENIDO WEB: M1, M3, M6, M7.</p> <p>N. IDENTIFICACION DE USUARIOS: N1, N2, N4, N5.</p> <p>O. QOS: O1, O2, O3, O5.</p> <p>P. FILTRO DE DATOS: P1, P2.</p> <p>Q. VPN: Q1, Q2, Q4, Q5, Q8, Q10, Q11.</p> <p>R. SD-WAN R1, R2, R3, R5, R7.</p> <p>S. CAPACIDADES DE OPTIMIZACIÓN: S1, S2, S3, S4, S6, S8.</p> <p>T. ADMINISTRACION Y MONITOREO: T2, T3, T4, T7, T9, T11, T14.</p>
<p>H5SOLUCIÓN DE SEGURIDAD DE ENDPOINT, DETECCIÓN Y RESPUESTA (EDR)</p> <p>A. GENERALIDADES: A2, A3, A4, A5, A6.</p> <p>B. PROTECCIÓN CONTRA EXPLOITS: B1, B2, B3, B5, B7, B8, B10.</p> <p>C. PROTECCIÓN CONTRA MALWARE: C1, C2, C3, C4, C5, C7, C10.</p> <p>D. PLATAFORMA DE SANDBOXING: D1, D2, D3, D4.</p> <p>E. CONTROL DE DISPOSITIVOS: E3, E4, E5.</p> <p>F. TELEMETRÍA Y COLECCIÓN DE DATOS Y EVENTOS: F3, F4, F6, F7, F12, F14, F15.</p> <p>G. CAPACIDADES DE INVESTIGACIÓN Y THREAT HUNTING: G1, G2, G3, G7, G8, G9.</p> <p>H. CAPACIDADES DE GESTIÓN DE INCIDENTES: H1, H2, H3, H5, H7.</p>

⁴ Artículo 59. Idioma de la documentación y otras formalidades 59.1. Los documentos que acompañan a las expresiones de interés, las ofertas y cotizaciones, según corresponda, se presentan en idioma español. Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado, según corresponda, salvo el caso de la información técnica complementaria contenida en folletos, instructivos, catálogos o similares, que puede ser presentada en el idioma original. El postor es responsable de la exactitud y veracidad de dichos documentos.

- I. CAPACIDADES DE THREAT INTELLIGENCE: I2, I3, I6, I7.
- J. CAPACIDADES DE USER ENTITY BEHAVIOR ANALYTICS (UEBA): J1, J2, J3, J6, J8.
- K. CAPACIDADES DE RESPUESTA: K1, K2, K4, K5, K6, K7, K11.
- L. DESCUBRIMIENTO DE ACTIVOS: L1, L2, L4.
- M. CARACTERÍSTICAS DEL AGENTE: M1, M2, M3, M4.
- N. CAPACIDADES DE GESTIÓN: N1, N2, N5, N7, N9, N10.

f) Se debe presentar en la oferta, como documento de admisibilidad, Carta y/o documento del fabricante y/o subsidiaria en el Perú del fabricante debidamente acreditado, que lo autorice o acredite al postor como: partner y/o comercializador y/o socio comercial y/o socio estratégico y/o distribuidor autorizado para la venta del equipamiento provisto⁵.

g) Declaración jurada de plazo de entrega. (**Anexo N° 4**)⁶

h) 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**)

i) 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 órgano encargado de las contrataciones o el comité de selección según corresponda, 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.

2.2.2. Documentación de presentación facultativa:

- a) En el caso de microempresas y pequeñas empresas integradas por personas con discapacidad, o en el caso de consorcios conformados en su totalidad por estas empresas, deben presentar la constancia o certificado con el cual acredite su inscripción en el Registro de Empresas Promocionales para Personas con Discapacidad⁷.
- b) Solicitud de bonificación del cinco por ciento (5%) por tener la condición de micro y pequeña empresa (**Anexo N° 10**).

⁵ Artículo 59. Idioma de la documentación y otras formalidades 59.1. Los documentos que acompañan a las expresiones de interés, las ofertas y cotizaciones, según corresponda, se presentan en idioma español. Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado, según corresponda, salvo el caso de la información técnica complementaria contenida en folletos, instructivos, catálogos o similares, que puede ser presentada en el idioma original. El postor es responsable de la exactitud y veracidad de dichos documentos.

⁶ 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.

⁷ Dicho documento se tendrá en consideración en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

Advertencia

El órgano encargado de las contrataciones o el comité de selección, según corresponda, no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápite “Documentos para la admisión de la oferta”, “Requisitos de calificación” y “Factores de evaluación”.

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

- a) Garantía de fiel cumplimiento del contrato
- b) Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso.
- 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.
- 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 siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) 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.

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 cuyos montos sean iguales o menores 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. Dicha excepción también aplica a 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 no supere el monto señalado anteriormente, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

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/>

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.

Importante para la Entidad

En caso se determine que adicionalmente se puede considerar otro tipo de documentación a ser presentada para el perfeccionamiento del contrato, consignar el siguiente literal:

- j) El postor adjudicado presentará como requisito para el perfeccionamiento del contrato el título profesional, el grado académico, el título técnico y capacitación solicitada.

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 Haya¹¹.*
- La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en Mesa de Partes de la Entidad, ubicada en la Av. Paseo de la República N° 3135 – 3137 - San Isidro o en Mesa de Partes Virtual de COFOPRI <https://mpv.cofopri.gob.pe/Management/FrmMesaPartesVirtual.aspx>.

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en ÚNICO PAGO, luego de emitida la conformidad por parte de la Oficina de Sistemas de la prestación principal.

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

- Recepción del responsable del Almacén o del que haga sus veces.
- Informe del funcionario responsable de la Oficina de Sistemas, emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Guía de remisión

Dicha documentación se debe presentar en Mesa de Partes de la Entidad, ubicada en la Av. Paseo de la República N° 3135 – 3137 - San Isidro o en Mesa de Partes Virtual de COFOPRI <https://mpv.cofopri.gob.pe/Management/FrmMesaPartesVirtual.aspx>.

¹¹ Según lo previsto en la Opinión N° 009-2016/DTN.

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

ESPECIFICACIONES TÉCNICAS ADQUISICIÓN DE UN SISTEMA DE PROTECCION Y SEGURIDAD PARA RED – FIREWALL

1. ÁREA USUARIA

Oficina de Sistemas.

2. OBJETIVO

El presente proceso tiene por objetivo la adquisición e instalación de un Sistema de Protección y Seguridad para Red – Firewall, que incluya una solución de seguridad de Endpoint, Detección y Respuesta (EDR), que permita fortalecer la seguridad digital en las sedes principales del COFOPRI.

3. FINALIDAD PÚBLICA

COFOPRI requiere asegurar la continuidad operativa de los servicios que brinda a la ciudadanía, a partir de un adecuado acceso y disponibilidad a los diversos servicios que brinda a sus usuarios internos y público en general, para ello cuenta con herramientas tecnológicas que permiten el cumplimiento eficiente de las funciones encomendadas, para realizar transacciones con los diversos sistemas de información de manera permanente y confiable, todo ello para brindar mayores y mejores servicios al ciudadano, logrando la eficiencia en la gestión interna e integrando la información en general.

En este sentido, se hace indispensable por renovación tecnológica adquirir un Sistema de Protección y Seguridad para Red – Firewall, para las sedes principales del COFOPRI que permitan fortalecer la seguridad digital en el uso de los servicios que provee la Oficina de Sistemas tanto a sus usuarios internos como externos.

Esta adquisición está alineado a la Actividad Operativa: C0242 "ATENCION DE LA CONTINUIDAD Y OPERATIVIDAD AL DATA CENTER".

4. ANTECEDENTES

El Organismo de Formalización de la Propiedad Informal – COFOPRI, cuenta con equipos Firewall los cuales se encuentran instalados en el Centro de Datos ubicado en la sede de La Molina, los que a la fecha requieren ser reemplazados por renovación tecnológica con soluciones modernas en materia de seguridad digital, asimismo se requiere una solución de detección y respuesta automática que protejan los equipos servidores alojados en el Centro de Datos, que permita mitigar los riesgos en los que se encuentran expuestos los activos críticos que albergan la información de la entidad, de vulnerabilidades de ataques tanto desde el interior como exterior a la red de datos corporativa, y que en la actualidad se han incrementado de forma significativa.

5. CARACTERÍSTICAS MINIMAS DEL BIEN

5.1. PRESTACION PRINCIPAL

El CONTRATISTA deberá proveer, instalar y poner en funcionamiento, un SISTEMA DE PROTECCION Y SEGURIDAD PARA RED – FIREWALL, en el Centro de Datos del COFOPRI sito en la sede de La Molina, ubicado en la Av. Raúl Ferrero esquina con Los Sauces - La Molina.

Los bienes a proveer por el CONTRATISTA deberán contar con las siguientes características técnicas mínimas:

NEXT GENERATION FIREWALL

A. DESCRIPCION

- A.1. Adquisición de una solución de Next Generation Firewall (NGFW) para la seguridad de la red institucional, debe ser ofrecida en alta disponibilidad, es decir por lo menos 2 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones técnicas.
- A.2. El Postor tiene la libertad de añadir consolas terceras para cumplir con los requerimientos técnicos solicitados, ya sea para capacidades de gestión, reportes y/o seguridad.
- A.3. El fabricante debe pertenecer al cuadrante de Líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 5 reportes.
- A.4. Deberá ser miembro del Cyber threat alliance.

B. REQUERIMIENTOS SOPORTE

- B.1. Ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life, end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.
- B.2. La solución propuesta deberá tener soporte vigente de fábrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware.
- B.3. El soporte deberá estar disponible 24x7x365, la apertura de casos deberá poder realizarse vía online o vía telefónica.
- B.4. Se deberá proporcionar accesos al portal de soporte del fabricante, donde se tenga la potestad de dar seguimiento a los mismos.

C. CAPACIDAD DE RENDIMIENTO

- C.1. Throughput de Prevención o Protección de Amenazas de 3 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Seguridad del tráfico DNS, Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido al habilitar los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242.
- C.2. Se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance de prevención o protección de amenazas.
- C.3. El equipo debe soportar como mínimo 250 000 sesiones/conexiones concurrentes y 40 000 nuevas sesiones/conexiones por segundo
- C.4. Debe contar con fuente de poder redundante.
- C.5. Disco interno para el almacenamiento de los eventos.
- C.6. Contar con una interfaz de cobre RJ45 dedicada para la gestión del equipo
- C.7. Contar con la siguiente cantidad de interfaces para el tráfico de datos: 8 interfaces RJ45
- C.8. Deberá tener CPU y memoria RAM dedicado para tareas de gestión del equipo, de manera independiente a los recursos para el procesamiento del tráfico. Esta arquitectura podrá estar integrada dentro del NGFW, o en caso no lo soporte, se podrán incluir consolas de gestión externas al NGFW.

D. CAPACIDADES DE NETWORKING

- D.1. El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- D.2. Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- D.3. Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.
- D.4. Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.
- D.5. Soportar diferentes características de networking operando en el protocolo IPv6, como mínimo: ruteo estático OSPFv3, MP-BGP, policy based routing o policy based forwarding, ECMP, dual-stack, QoS, DSCP, NAT64, LLDP, BFD, DHCPv6 Relay, SLAAC, SNMP.
- D.6. La plataforma debe contar con certificación USGv6-r1 para las pruebas de Firewall, IDS e IPS.

E. ALTA DISPONIBILIDAD

- E.1. Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).
- E.2. La configuración en alta disponibilidad debe sincronizar: sesiones, certificados de descifrado, configuraciones, incluyendo, más no limitado a políticas de seguridad, NAT, QoS y objetos de red.
- E.3. Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces.
- E.4. Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.

F. FUNCIONALIDADES DE FIREWALL

- F.1. Control de políticas puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos).
- F.2. Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
- F.3. El plano de gestión deberá realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
- F.4. Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.

G. DESCIFRADO DE TRÁFICO SSL/TLS

- G.1. Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en las estaciones de trabajo
- G.2. Permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el NGFW.
- G.3. Capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos y/o no fiables, a pesar de no descifrar el tráfico.
- G.4. Debe soportar certificados que utilicen Subject Alternative Name (SAN) y Server Name Indication (SNI).

- G.5. Permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar excluir del descifrado a páginas con contenido sensible y descifrar el resto de las páginas.
- G.6. Permitir excluir sitios a los cuales no se les aplicará la política de descifrado en base al Common Name del certificado.
- G.7. Debe contar con un dashboard que muestre gráficamente la proporción del tráfico descifrado, aplicaciones y dominios con descifrado correcto, errores de descifrado.
- H. PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (DoS)**
 - H.1. Debe ser posible definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood.
 - H.2. Debe ser posible utilizar SYN Cookies como medida de defensa.
 - H.3. La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor)
 - H.4. Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo
 - H.5. Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia dicho equipo.
- I. VISIBILIDAD EN CAPA 7 Y CONTROL DE APLICACIONES**
 - I.1. La solución propuesta deberá reconocer por lo menos 4000 aplicaciones, incluyendo, más no limitando a aplicaciones de tipo peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
 - I.2. Deberá ser posible definir grupos de aplicaciones en base a sus atributos, por ejemplo, un grupo de aplicaciones de riesgo alto que sea dinámicamente alimentado.
 - I.3. Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
 - I.4. Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. Debe ser capaz de determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.
 - I.5. Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.
 - I.6. Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación. Es decir, si 2 aplicaciones utilizan el mismo puerto y protocolo, se debe poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.
 - I.7. Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión.
- J. PREVENCIÓN DE AMENAZAS**
 - J.1. La solución propuesta deberá contar con capacidades de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.
 - J.2. Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar de forma permanente, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.

- J.3. El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
- J.4. La solución deberá identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que se pueda bloquear dichas consultas DNS.
- J.5. Deberá contar con un mecanismo que permita identificar los equipos potencialmente infectados en base al análisis de su tráfico DNS, inclusive si el tráfico entre la potencial víctima y su servidor DNS utilizado no pasa por el NGFW.
- J.6. Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH) o también DNS sobre TLS.
- J.7. El módulo de IPS debe ser capaz de bloquear ataques en base a firmas, heurística y anomalías en el protocolo.
- J.8. El módulo de IPS debe permitir personalizar firmas directamente desde la consola gráfica.
- J.9. La protección contra amenazas avanzadas indetectables por firmas, heurística o reputación del dominio o contenido deberá estar basado en mecanismos de inteligencia artificial, tales como deep learning y/o machine learning.
- J.10. Respecto a ataques de malware, las firmas deberán estar basadas en patrones y no únicamente en hashes, con el objetivo de identificar y bloquear el malware polimórfico que pertenezca a una misma familia.
- J.11. Con la finalidad de contar con una protección robusta contra amenazas emergentes a nivel mundial, la solución deberá ser capaz de actualizar su base de firmas de malware en tiempo real sin afectar el performance del equipo.
- J.12. Deberá contar con un mecanismo basado en aprendizaje de máquina que sea capaz de analizar en tiempo real los archivos desconocidos no identificables por firmas ni heurística; el análisis deberá identificar si los archivos son maliciosos, en cuyo caso el equipo deberá bloquear su ingreso para evitar la infección por amenazas de día cero.
- J.13. Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SFTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.

K. PREVENCIÓN DE AMENAZAS AVANZADAS EN DNS

- K.1. La plataforma deberá ser alimentada por un servicio de inteligencia global de amenazas capaz de identificar millones de dominios maliciosos con análisis en tiempo real.
- K.2. La identificación de amenazas avanzadas camufladas en tráfico DNS deberá contar con mecanismos avanzados de detección con el objetivo de identificar ataques imposibles de mitigar con firmas y/o reputación del dominio. Para ello se requiere que el tráfico DNS sea analizado con técnicas de inteligencia artificial.
- K.3. Deberá ser capaz de prevenir ataques como DGA (Domain Generation Algorithm) Random y de Diccionario, DNS Tunneling e infiltración de DNS.
- K.4. Deberá soportar el manejo excepciones para poder mitigar los falsos positivos.
- K.5. Deberá contar con dashboards y estadísticas sobre la cantidad, tipo de peticiones DNS, clasificación de la amenaza, generadas por los dispositivos internos de la Institución.

L. SANDBOXING

- L.1. La plataforma de Sandbox podrá ser ofrecido en Nube (Cloud), On-premise o ambos.
- L.2. Deberá ser capaz de emular el potencial malware en entornos Windows, Linux y MacOS.

- L.3. El sandbox deberá ser capaz de analizar 1000 archivos por hora realizando análisis dinámico del archivo (entiéndase por análisis dinámico aquel que no está basado en firmas, ni prefiltros, sino en emulación completa del potencial malware).
 - L.4. También se aceptará soluciones sandbox terceras de otro fabricante distinto al NGFW.
 - L.5. El análisis dinámico deberá realizarse de forma paralela para todos los archivos enviados y no deberá tomar más de 10 minutos en dar un veredicto.
 - L.6. En caso de tratarse de una plataforma de Sandbox Cloud, deberá cumplir con los siguientes requerimientos:
 - Deberá tener una disponibilidad de al menos 99.9% contabilizados mensualmente.
 - Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II Plus de AICPA.
 - L.7. En caso de tratarse de una plataforma de Sandbox On-premise, deberá cumplir con los siguientes requerimientos:
 - Deberá ser desplegado en Alta Disponibilidad (Activo-Pasivo) con el objetivo de mantener los controles de seguridad en caso de contingencia.
 - L.8. Debe proveer información forense sobre las acciones realizadas por el malware, tales como resumen del comportamiento visto, actividad sobre los archivos, peticiones DNS, conexiones de red, actividad de los archivos, procesos y registros. Esta información deberá poder extraída en un reporte PDF.
 - L.9. Deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
 - L.10. Debe permitir al administrador la descarga del archivo original analizado por el sandbox.
 - L.11. Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.
 - L.12. Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico.
 - L.13. Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
- M. FILTRO DE CONTENIDO WEB**
- M.1. Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.
 - M.2. Debe soportar un cache local de URLs en el dispositivo, evitando el delay de comunicación/validación de las URLs
 - M.3. Debe contar con medidas de antievasión como Cloaking, Captcha falsos, codificación de caracteres HTML o similares.
 - M.4. Debe permitir la creación de categorías personalizadas.
 - M.5. Debe permitir la personalización de la página de bloqueo.
 - M.6. Debe permitir notificar al usuario, mostrándole solo una página de alerta personalizable, pero permitiéndole continuar la navegación al site.
 - M.7. Debe ser capaz de registrar el User-agent, Referer, XFF de cada sesión hacia internet
 - M.8. Debe ser capaz de forzar la navegación de los usuarios en el modo Safe Search Enforcement.

N. IDENTIFICACION DE USUARIOS

- N.1. Debe permitir la creación de políticas de seguridad basadas en la identidad del usuario y grupo al cual pertenece, a través de la integración de servicios de autenticación como Active Directory, Novell eDirectory, Open LDAP y base de datos local.
- N.2. Debe contar con varios mecanismos para la identificación del usuario y la dirección IP del equipo en donde se encuentra autenticado. Como mínimo deberá poder integrarse a las siguientes plataformas para cubrir este requerimiento:
 - Eventos de login gestionados en Domain Controller y/o Microsoft Exchange.
 - Terminal Server de Microsoft o Citrix
 - Consultando directamente a cada estación de trabajo a través del protocolo WMI
- N.3. Deberá contar con un componente que permita integrarse a diversas plataformas de identidades tales como Azure LDAP, Google Directory, Okta, Cisco Duo, PingID.
- N.4. Debe contar con la funcionalidad de Portal Cautivo (Captive Portal), de tal manera que el NGFW muestre un portal al usuario para que se autentique manualmente. Las cuentas podrán ser definidas localmente en el NGFW o integradas con plataformas terceras.
- N.5. Debe tener integración con plataformas de MFA (Multi Factor Authentication), de tal forma que cuando un dispositivo requiera acceder a recurso, se le solicite el OTP.

O. QOS

- O.1. Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix), se requiere que la solución tenga la capacidad de controlarlas a través de políticas personalizables.
- O.2. Soportar la creación de políticas de QoS por: dirección de origen y destino, por grupo de usuario de LDAP, por aplicaciones, por puerto.
- O.3. El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.
- O.4. Soportar marcación de paquetes DSCP, inclusive por aplicaciones;
- O.5. Permitir el monitoreo en tiempo real del tráfico gestionado por el QoS.

P. FILTRO DE DATOS

- P.1. Los archivos deben ser identificados por extensión y firmas.
- P.2. Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos.
- P.3. Permitir, identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular.

Q. VPN

- Q.1. Soportar VPN Site-to-Site en protocolo IPSec
- Q.2. La VPN site to site debe soportar como mínimo:
 - 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
 - Autenticación MD5, SHA-1, SHA-2;
 - Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
 - Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
- Q.3. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
- Q.4. Permitir aplicar QoS dentro de los túneles VPN.

- Q.5. Soportar VPN client-to-site pudiendo operar usando el protocolo IPsec o SSL.
- Q.6. Permitir la conexión por medio de agente instalado en el sistema operativo.
- Q.7. Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS.
- Q.8. Capacidad de integrarse con plataformas de Doble Factor de Autenticación (2FA).
- Q.9. Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- Q.10. Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN, incluyendo el soporte de Split DNS.
- Q.11. Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
 - Antes del usuario se autentique en la estación.
 - Después de la autenticación del usuario en la estación usando Single Sign On (SSO).
 - A demanda, de forma manual por parte del usuario.
- Q.12. El agente de VPN client-to-site debe ser compatible al menos con: Windows y MacOS X.

R. SD-WAN

- R.1. La solución debe contar con una consola de monitoreo con la capacidad de poder identificar fácilmente las aplicaciones y enlaces sus estados dentro de la red de SD-WAN (aplicaciones con problemas de jitter, latencia, pérdida de paquetes y sus diferentes estados dentro de la red) pudiendo ver el estado de estas en por lo menos en los últimos 5 minutos, última hora, último día o bien haciendo filtros personalizados.
- R.2. La solución debe incluir la capacidad de poder monitorear la salud de los enlaces en términos de jitter, latencia y pérdida de paquetes, tomando decisiones inteligentes de enrutamiento basado en la condición de los enlaces de manera dinámica.
- R.3. La solución debe contar con la posibilidad de hacer reportes del estado de los enlaces y aplicaciones, indicando volúmenes de datos con respecto a las veces que fueron degradados o afectados.
- R.4. Capacidad de poder cambiar dinámicamente de camino al detectar alguna degradación del enlace sin afectar o cortar la sesión establecida de la aplicación, es decir, que el usuario no perciba corte en la aplicación, ni tener que reiniciar la sesión.
- R.5. Soportar de algoritmo de corrección de errores (FEC - Forward Error Correction) con el objetivo de poder garantizar una buena experiencia en el uso de aplicaciones de voz y video a través de la red de SD-WAN.
- R.6. Soportar la transmisión de paquetes duplicados por diferentes enlaces al utilizar la red de SD-WAN con el objetivo de mantener una calidad de experiencia alta al usar aplicaciones de misión crítica y prevenir la pérdida de paquetes, incremento de latencia, jitter, etc.
- R.7. Capacidad de monitorear la salud de los enlaces a través de aplicaciones de SaaS y aplicaciones de Cloud, para poder determinar si esas aplicaciones son enviadas a internet de manera directa o bien a través de algún camino de la red de SD-WAN.
- R.8. Capacidad de definir el tiempo de intercambio de heartbeats entre los puntos del túnel SD-WAN.
- R.9. Deberá ser posible activar la funcionalidad de SD-WAN en interfaces agregadas (IEEE 802.1AX) y en subinterfaces.
- R.10. Capacidad de realizar fail over a nivel de sub segundos

S. CAPACIDADES DE OPTIMIZACIÓN

- S.1. Como parte de la propuesta, se deberá proporcionar hasta 2 cuentas de acceso al portal oficial de educación del fabricante, para acceder, a cursos en línea sobre la solución ofertada.
- S.2. Se deberá incluir una herramienta integrada y/o externa que genere alertas si existen problemas de salud del equipo en materia de hardware y software, como mínimo: consumo de memoria, problemas de la alta disponibilidad (HA), problemas de disco duro, firmware vulnerable, firmware cerca a la obsolescencia, expiración de licencias.
- S.3. Con el objetivo de que la Institución cuente con autonomía para evaluar si el NGFW se encuentra configurado acorde a las buenas prácticas y evitar que el postor sea juez y parte del control de calidad de ésta, se deberá incluir una herramienta que permita evaluar automáticamente si el NGFW se encuentra configurado acorde a las buenas prácticas del fabricante en materia de los diferentes módulos de seguridad que se le haya activado.
- S.4. Esta herramienta deberá ser única y consolidar la información de todos los NGFW por adquirir en el presente proyecto.
- S.5. Debe contar con gráficos ejecutivos que permitan mostrar el nivel de adopción de los módulos de seguridad del NGFW en las políticas de seguridad.
- S.6. Debe contar con un módulo que permita filtrar y depurar las políticas de NGFW sin uso en la red.
- S.7. Debe identificar las reglas superpuestas (shadowed rules), los cuales representen un riesgo de seguridad al permitir mayores accesos que los autorizados.
- S.8. La herramienta podrá estar integrada al NGFW o externa, ya sea de la misma marca u otra que se puede integrar.
- S.9. La herramienta deberá ser dedicada para la Entidad, no se aceptarán plataformas compartidas con otras empresas o clientes del postor.
- S.10. La herramienta de evaluación de buenas prácticas deberá ser específica para la configuración del NGFW implementado, no se aceptarán portales con guías de usuarios genéricas.

T. ADMINISTRACION Y MONITOREO

- T.1. Con la finalidad de no degradar el performance de procesamiento de red y seguridad del NGFW, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante.
- T.2. En caso el postor haya incluido en su propuesta plataformas externas al NGFW, éstas también deberán tener su propia consola de gestión, ya sea de manera integrada, appliance independiente o basadas en nube.
- T.3. Permitir exportar las reglas de seguridad del NGFW en formato CSV y PDF
- T.4. Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.
- T.5. Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
- T.6. Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino)

- T.7. Ante escenarios donde existan dos o más administradores en el equipo, logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
- T.8. Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.
- T.9. Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.
- T.10. Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
- T.11. Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración.
- T.12. La gestión de NGFW debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.
- T.13. Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispymware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
- T.14. Debe permitir configurar reportes para ver el tiempo de navegación de los usuarios en internet, clasificado por tipo de página web y URL.
- T.15. Debe contar con reportes predeterminados que muestren información y diversas estadísticas sobre el uso de aplicaciones SaaS.
- T.16. La gestión de NGFW debe permitir realizar tareas de gestión a través del API basado en XML.

SOLUCIÓN DE SEGURIDAD DE ENDPOINT, DETECCIÓN Y RESPUESTA (EDR)

A. GENERALIDADES

- A.1. La solución debe consistir en una plataforma de Protección, Detección y Respuesta del endpoint (Endpoint Protection y EDR)
- A.2. Se deberán licenciar 200 agentes como mínimo.
- A.3. El almacenamiento de telemetría del endpoint deberá estar disponible durante al menos 30 días.
- A.4. Deberá contar con soporte del fabricante durante todo el tiempo de servicio.
- A.5. Se deberá otorgar acceso a un portal de e-learning donde la Entidad pueda llevar cursos en línea sobre la plataforma implementada.
- A.6. Deberá haber logrado una efectividad de protección de ataques de 100% según el último reporte de MITRE ATT&CK TURLA 2023
- A.7. El postor podrá integrar tecnologías de diferentes marcas para cumplir los requerimientos mínimos solicitados en las presentes especificaciones técnicas.

B. PROTECCIÓN CONTRA EXPLOITS

- B.1. Debe identificar y bloquear técnicas de explotación sin necesidad de utilizar firmas y/o heurísticas. La solución no deberá tener ningún componente que requiera actualizar una base de datos de firmas.
- B.2. El bloqueo de exploits deberá ser posible incluso en procesos desarrollados inhouse, la solución deberá permitir especificar los nombres de los procesos que serán protegidos contra exploits.

- B.3. Deberá proteger la explotación de vulnerabilidades de sistemas operativos y aplicaciones que incluso se encuentren sin el parche de seguridad instalado.
- B.4. La protección contra vulnerabilidades deberá ser independiente al CVE identificado, la solución deberá proteger cualquier intento de explotación incluyendo a vulnerabilidades de día cero que no tengan un CVE.
- B.5. Bloquear técnicas de explotación de vulnerabilidades, como mínimo Return Oriented Programming (ROP), Heap Spray, Jit Spray, Shell link, Structured Exception Handler, CPL Execution Process.
- B.6. Identificación y prevención de intentos de escalación de privilegios a nivel de Kernel.
- B.7. Deberá ser capaz de proteger contra ataques a vulnerabilidades conocidas y desconocidas (día cero).
- B.8. Capacidad de crear un snapshot (dump) de la memoria RAM al momento de prevenir la ejecución de una técnica de explotación, con la finalidad de proporcionar información forense sobre el evento.
- B.9. Prevención de técnicas de explotación que utilizan Java Deserialization, Kernel Integrity Monitor (KIM), Local Threat Evaluation Engine (LTEE), Reverse Shell Protection, Shellcode Protection, SO Hijacking Protection, Webshell.
- B.10. Todas las capacidades de prevención de exploits deberán estar disponibles de manera offline, sin necesidad de tener una conexión a la consola.

C. PROTECCIÓN CONTRA MALWARE

- C.1. Deberá contar con funcionalidades de antimalware de siguiente generación, entendiéndose antimalware de siguiente generación como plataformas que utilizan algoritmos de aprendizaje de máquina (machine learning) para detectar y bloquear el malware; no deberá tener ningún componente que requiera actualizar una base de datos de firmas de antivirus/antimalware.
- C.2. El algoritmo de machine learning deberá operar de manera local en el endpoint sin depender de una conexión permanente a la consola.
- C.3. Debe prevenir el robo de contraseña a partir de la lectura de la memoria RAM (mimikatz)
- C.4. Contar con un módulo de prevención contra ransomware que podrá ser configurado en modo normal y riguroso.
- C.5. Capacidad de prevenir ataques de Cryptomining a partir del comportamiento del objeto ejecutado.
- C.6. Adicionalmente a la protección basada en machine learning, deberá contar con la capacidad de identificar el comportamiento de la amenaza, de tal forma que la actividad maliciosa de un archivo se pueda detectar y bloquear en una fase temprana.
- C.7. Capacidad de prevenir contra shells reversos (reverse shell) para sistemas operativos Linux.
- C.8. Capacidad de poder colocar los malware en una carpeta de cuarentena
- C.9. Capacidad de colocar en lista permitida los archivos o directorios, para exceptuar la inspección.
- C.10. Capacidad de realizar escaneos a demanda y programados, con el objetivo de identificar malware dormido en los endpoints.
- C.11. El consumo de recursos al momento de realizar el escaneo debe de ser mínimo y no debe impactar en la experiencia del usuario.

D. PLATAFORMA DE SANDBOXING

- D.1. El agente deberá ser capaz de enviar automáticamente el archivo a un entorno de sandbox para ser emulado.
- D.2. El sandbox deberá estar basado en nube y debe tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.

D.3. El sandbox deberá soportar el análisis de 100 mil archivos por día. El sandbox deberá tener capacidad de analizar archivos de hasta 100 MB de peso.

D.4. Deberá garantizar la privacidad y seguridad del contenido de los archivos analizados, para lo cual se requiere que cuente como mínimo con las certificaciones SOC2 Tipo II Plus de AICPA.

D.5. Capacidad de realizar análisis de sandboxing en sistemas Windows, MacOS, Linux.

E. CONTROL DE DISPOSITIVOS

E.1. Debe permitir gestionar los puertos USB que permitan conectar dispositivos como: discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles, unidades lectoras de discos floppy externas con conexión USB.

E.2. Debe de permitir generar perfiles de excepciones para poder conectar dispositivos en puertos USB utilizando los siguientes parámetros: tipo de dispositivo, tipo de permiso a asignar (lectura/escritura o sólo lectura), fabricante (debe de contener una lista predeterminada), producto (debe de contener una lista predeterminada) y número de serie.

E.3. Las políticas generadas deben de poder asignarse a un endpoint en particular, a un grupo de endpoints.

E.4. Deberá ser capaz de integrarse a Active Directory para establecer políticas de control de USB en base a grupos de LDAP.

E.5. Debe de permitir la creación de excepciones temporales a partir de una alerta registrada, para permitir el dispositivo solo durante un tiempo configurable.

E.6. Capacidad de añadir nuevos tipos de dispositivos agregando el GUID de Windows correspondiente.

F. TELEMETRÍA Y COLECCIÓN DE DATOS Y EVENTOS

- El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Windows:

F.1. Proceso ejecutado, incluyendo el tiempo de inicio, el tamaño del archivo asociado.

F.2. Actividades de creación, escritura, renombre, eliminación, modificación de archivos.

F.3. Archivos DLL: ruta completa, dirección base, id del proceso, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL.

F.4. Creación y terminación de los procesos, incluyendo los siguientes atributos: nombre del proceso padre, ID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.

F.5. Inyecciones en hilos de procesos: ID del hilo padre, ID del hilo nuevo o que se ha terminado, proceso que inició el hilo (en caso de ser un proceso distinto).

F.6. Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP), resolución de dominio (hostname), tráfico entrante y saliente, país destino de la IP pública.

F.7. Estadísticas de red: volumen de tráfico en eventos de subida y descarga de tráfico TCP.

F.8. Acciones sobre los registros de Windows: Configuración o eliminación de valores del registro. Creación, modificación, eliminación, adición, restauración y guardar llaves del registro. Con los siguientes parámetros: ruta del registro del valor o llave que fue modificado. Nombre del valor o llave modificado. Datos del valor modificado.

F.9. Sesiones del sistema operativo: inicio de sesión, cierre de sesión, conexión y desconexión. Considerando los siguientes atributos: inicio de sesión interactivo, id de la sesión, estado de la sesión, y si la sesión es local o remota.

F.10. Logs de eventos de Windows.

- El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos MacOS:

F.11. Actividades de creación, escritura, renombre, eliminación, modificación de archivos.

F.12. Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.

F.13. Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).

F.14. Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.

F.15. Logs de eventos de autenticación

F.16. El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Linux:

- Para los archivos: las acciones de creación, apertura, escritura y eliminación, incluyendo la ruta completa del archivo y el hash del archivo (para ciertos archivos y sólo si el archivo fue escrito). Información del copiado o renombrado de los archivos, incluyendo las rutas completas tanto del archivo original como del modificado. Las acciones para cambiar el dueño (chown) y el modo (chmod) de los archivos, incluyendo la ruta completa del archivo, así como el nuevo dueño o nuevos atributos.
- Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.
- Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).
- Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.
- Logs de eventos de autenticación.

G. CAPACIDADES DE INVESTIGACIÓN Y THREAT HUNTING

G.1. Deberá mostrar una secuencia gráfica del incidente de seguridad que correlacione las alertas individuales con el objetivo de identificar la causa raíz. Esta secuencia gráfica deberá ser construida de manera automática a partir de la inteligencia artificial de la plataforma.

G.2. Deberá de mostrar información de los procesos correlacionados en la secuencia gráfica, entre los que se encuentran ruta de ejecución, nombre de usuario que ejecutó el proceso, entidad que firmó el proceso, valor SHA256 del ejecutable relacionado con el proceso, veredicto del análisis del sandbox y línea de comandos de la ejecución.

G.3. Por cada proceso correlacionado en la secuencia gráfica del incidente se deberá mostrar lo siguiente:

- Fecha, hora, hostname, dirección IP, nombre del usuario, sistema operativo del equipo que generó el proceso.

- Alertas relacionadas al proceso analizado con su respectiva descripción, acción tomada sobre la alerta, categoría de la amenaza, ejecutable que lo inicializó, táctica y técnica del ataque según el framework MITRE ATT&CK.
- Actividad de la red del proceso: IP y puerto origen, IP y puerto destino, resolución del DNS, país destino, indicar si la conexión fue exitosa o fallida.
- Creación, escritura, lectura, eliminación, renombre, cambio de atributos, hash en SHA256 y MD5 de los archivos relacionados al proceso analizado. En caso del renombre deberá mostrar el nombre anterior y actual para facilitar la investigación del analista.
- Creación, apertura, escritura, eliminación, renombre, cambio de atributos de los directorios relacionados al proceso analizado.
- Actividad sobre la clave y valores de registros, tales como creación, eliminación, carga, apertura, renombre, escritura, del proceso analizado.
- Mostrar los system calls, rpc calls y procesos inyectados sobre cada proceso analizado.
- Deberá contar con un mecanismo inteligente que separe de manera automática los binarios y DLLs no significados de la secuencia gráfica del incidente.

G.4. Deberá permitir realizar búsquedas avanzadas sobre la actividad de los endpoints:

- Actividad de los archivos, identificando las siguientes operaciones: creación, lectura, eliminación, escritura y renombrar.
- Actividad de red, identificando el tráfico saliente, entrante, IP origen e IP destino, Puerto origen y Puerto destino, protocolo de red.
- Actividad en el registro Windows, identificando la creación, eliminación, renombrado, definición de valores, eliminación de valores de las llaves de registro.
- Actividad de procesos, identificando si se trata de una ejecución o inyección, ruta desde donde se ejecuta, comando que inicializa el proceso, usuario, hash en SHA256 y MD5.
- Actividad en el Log de Eventos de Windows, identificando la descripción, ID del evento, nivel, mensaje, nombre del proveedor y usuario.
- Actividad de autenticación al endpoint
- Permitir realizar búsquedas en base a cualquier dato recopilado por la plataforma.
- Permitir seleccionar las columnas y orden de los datos mostrados como resultados de las búsquedas.
- Los resultados de las búsquedas deberán poder ser mostrados en una tabla o una gráfica de tipo pye, columnas, burbuja y área, con la finalidad de facilitar el análisis del investigador.
- Deberá contar con una librería predeterminada de búsquedas habituales realizadas en una labor de threat hunting. Esta librería podrá ser editada según la labor del investigador.

G.5. Las búsquedas deberán estar disponibles tanto para endpoints en línea y fuera de línea.

G.6. Las búsquedas deberán de poder programarse para ser ejecutadas en un día y hora determinados durante una sola ocasión y también de manera recurrente.

G.7. Todas las opciones de búsqueda anteriormente detalladas deberán poder ser utilizadas para configurar reglas personalizadas de seguridad, que permitan generar una alerta cuando un endpoint en particular genere ese comportamiento.

G.8. Deberá de contar con un dashboard que permita visualizar alertas generadas de distintas fuentes.

G.9. El timeline del ataque deberá mostrar el intento de ataque en diferentes fases de explotación acorde al Framework MITRE ATT&CK, tales como Ejecución,

Persistencia, Descubrimiento, Desplazamiento Lateral, Command & Control, Exfiltración.

- G.10. Deberá permitir la personalización de reglas de correlación que permitan configurar casos de uso utilizando los eventos recolectados de las diversas fuentes.

H. CAPACIDADES DE GESTIÓN DE INCIDENTES

- H.1. Deberá agrupar todas las alertas relacionadas a un incidente de seguridad de manera automática.
- H.2. Por cada incidente mostrado deberá mostrar los elementos relacionados como ejecutables, hashes, direcciones IP.
- H.3. Deberá mostrar los hosts y usuarios asociados al incidente.
- H.4. Deberá ser posible asignar la revisión del incidente a un investigador con acceso a la consola, con el objetivo de llevar un orden sobre la atención de incidentes.
- H.5. Capacidad de comentar los incidentes para detallar los avances realizados en la revisión.
- H.6. Capacidad de clasificar el estado del incidente como abierto, en revisión, gestionado, cerrado, etc.
- H.7. Capacidad de agrupar y desagrupar los incidentes de manera manual.
- H.8. Capacidad de modificar la severidad del incidente de manera manual.

I. CAPACIDADES DE THREAT INTELLIGENCE

- I.1. Capacidad de alimentar la plataforma de Indicadores de Compromiso (IOC) de manera manual o automática vía API
- I.2. Los IOC soportados deberán ser de tipo Hash, Ruta, Nombre de archivo, Dominio, Dirección IP.
- I.3. Capacidad de agregar IOC de manera individual o masiva (por ejemplo, subiendo un archivo CSV)
- I.4. Capacidad de colocar un nivel de reputación, confiabilidad del IOC y una fecha de expiración.
- I.5. Debe poder integrarse a una plataforma tercera de Threat Intelligence como Virus Total.
- I.6. Mostrar un mapa geográfico que permita analizar la dirección IP detectada como parte de incidente, como mínimo deberá mostrar lo siguiente: fecha de registro, ISP (Internet Service Provider), país. La información deberá poder ser mostrada en base al país, proceso, puerto e IP destino.
- I.7. Deberá contar con un dashboard que permita analizar el comportamiento del hash de un archivo en particular, mostrando su nivel de reputación y si dicho hash ha sido detectado en otras alertas e incidentes.

J. CAPACIDADES DE USER ENTITY BEHAVIOR ANALYTICS (UEBA)

- J.1. Deberá ser capaz de retener los eventos recolectados durante al menos 30 días y aprender una línea base o perfil de comportamiento de cada dispositivo.
- J.2. Los perfiles de comportamiento deberán de ser generados mediante el uso de algoritmos de aprendizaje de máquina no supervisado.
- J.3. El producto deberá de alertar las anomalías en el perfil de comportamiento generado
- J.4. La alerta deberá de formar parte de los incidentes que se hayan generado.
- J.5. A partir del comportamiento aprendido, la solución deberá ser capaz de alertar los siguientes comportamientos inusuales, que estén fuera del perfil base aprendido:
- User agent sospechoso
 - Cantidad de interacciones de red inusuales
 - Query LDAP inusual
 - Creación de reglas de firewall inusuales

- Sesión WinRM anómala
 - Servidor Python inicializado
 - Proceso raro ejecutado en la institución
 - Elevación de privilegios con usuario SYSTEM de manera anómala
 - Firewall de Linux desactivado de manera anómala
 - Tarea programada creada de forma inusual
 - Ejecución de arp.exe anómala
 - Cantidad inusual de screenshots tomados
 - Cantidad excesiva y anómala de información subida a internet
 - Conexión RDP inusual
 - Escaneo de puertos sospechoso
 - Creación de una máquina en el dominio
 - Creación de usuario con permisos de domain admin
 - Usuario imprime una cantidad inusual de archivos
- J.6. Deberá tener más de 200 casos de uso automáticos que puedan ser generados a partir del aprendizaje del comportamiento de la inteligencia artificial o machine learning no supervisados.
- J.7. Deberá ser posible alertar determinados comportamientos de los usuarios y hosts asociados a actividad en archivos, directorios, procesos red, cambios de registro.
- J.8. Deberá contar con integración al Active Directory para extraer información contextual del usuario, incluyendo el departamento en el cual labora, número de teléfono, última fecha de autenticación.

K. CAPACIDADES DE RESPUESTA

- K.1. Deberá ser posible colocar en lista bloqueada y/o lista permitida uno o más hashes.
- K.2. Deberá permitir colocar en cuarentena un archivo malicioso detectado y/o bloqueado. La colocación en cuarentena deberá poder realizarse de manera manual y automática.
- K.3. Capacidad de extraer el archivo dump de la memoria RAM del endpoint a partir de una alerta revisada.
- K.4. Capacidad de extraer el malware o archivo sospechoso del endpoint hacia la consola, para poder ser analizado por el investigador
- K.5. Debe ser posible aislar el endpoint de la red para que no tenga comunicación con ningún dispositivo de la red interna o externa.
- K.6. Capacidad de configurar reglas de automatización que permitan ejecutar una acción determinada en los endpoints en base condiciones de alertas de seguridad, como mínimo estas reglas deberán permitir las siguientes acciones de manera automática: aislar el endpoint, hacer un escaneo de malware, extraer el malware desde el endpoint.
- K.7. Deberá ser posible realizar una conexión remota a cada endpoint que forme parte de una investigación para ejecutar las siguientes acciones:
- Listar procesos y archivos
 - Ejecutar instrucciones por línea de comandos (CMD y Powershell para el caso de Windows; Bash para el caso de Linux).
 - Ejecutar scripts basados en Python
- K.8. Capacidad de ejecutar scripts remotamente a múltiples endpoints de manera concurrentes.
- K.9. Deberá contar con una librería de scripts predefinidos y deberá ser posible configurar scripts personalizados basados en Python.
- K.10. Capacidad de tareas remotas a múltiples endpoints, como mínimo cerrar procesos, eliminar archivos, eliminar y/o modificar claves de registro.
- K.11. Mostrar sugerencias para las remediaciones de un equipo comprometido.
- K.12. Capacidad de integración con un SIEM vía Syslog y plataformas SOAR.

L. DESCUBRIMIENTO DE ACTIVOS

- L.1. Deberá contar con un mecanismo para descubrir dispositivos de la red sin el agente instalado.
- L.2. El descubrimiento deberá tener la capacidad para identificar la dirección IP del equipo y el Sistema Operativo que no tienen el agente instalado.
- L.3. Permitir exceptuar los segmentos de red que no se desean escanear.
- L.4. Deberá contar con el licenciamiento adecuado para el descubrimiento de dispositivos en las diferentes sedes de la entidad.

M. CARACTERÍSTICAS DEL AGENTE

- M.1. Deberá ser un agente ligero que incluso pueda convivir con cualquier otro software instalado en el endpoint.
- M.2. Soporte para las siguientes versiones de sistemas operativos:
 - Windows 8.1 y superior, Windows Server 2012 y superior
 - MacOS 11.X y superior
 - Linux, distribuciones: CentOS 6.7 y superior, Debian 9 y superior, Red Hat Enterprise Linux 6.7 y superior, Suse for Enterprise 12 y superior, Ubuntu Server 12.04 y superior, Amazon Linux 8 y 9, Oracle Linux 6.7 y superior.
 - Android y iOS.
- M.3. No debe requerir el reinicio del equipo para que agente se encuentre operativo.
- M.4. Deberá estar protegido ante intentos de desinstalación o manipulación del agente.
- M.5. Deberá ser posible definir diferentes password de seguridad para diferentes grupos de endpoints.

N. CAPACIDADES DE GESTIÓN

- N.1. La consola deberá estar basada 100% en nube, con el objetivo de no depender ni administrar infraestructura física local. La nube del fabricante deberá contar con las siguientes características:
 - Contar con la certificación SOC2 Tipo II de AICPA.
 - Contar con doble factor de autenticación para el login.
 - Permitir el acceso solo desde un rango de IP pública de la Entidad.
- N.2. La consola debe permitir la gestión de usuarios mediante roles preconfigurados y debe ser capaz de crear roles personalizados.
- N.3. Permite utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente.
- N.4. Cuenta con la capacidad de crear grupos que pueden alimentarse de forma estática y dinámica.
- N.5. Capacidad de personalización del dashboard para mostrar los widgets según las necesidades de la Entidad.
- N.6. Capacidad de almacenar una auditoría de eventos sobre las acciones realizadas en la consola
- N.7. Deberá permitir el envío automático de alertas al correo electrónico cuando se identifica una actividad maliciosa. Podrán aplicarse filtros a dichas alertas para solo mostrar las de mayor relevancia.
- N.8. Deberá permitir la generación de reportes a través de plantillas preconfiguradas y también permitir definir reportes personalizados.
- N.9. Mantener un historial de los reportes que han sido generados para su posterior consulta.
- N.10. Los reportes podrán ser enviados de forma automática y programada a una o más direcciones de correos electrónicos.

CONDICIONES SOBRE LOS EQUIPOS:

- Todos los componentes de la solución requerida deberán ser nuevos y de primer uso.
- El proveedor debe considerar en su oferta todos los componentes (hardware y/o software), partes y/o piezas, cables y cualquier otro accesorio necesario para la instalación y buen funcionamiento de los bienes solicitados, los mismos que deben ser originales de fábrica y nuevos.
- No se aceptarán equipos reciclados, reensamblados o reacondicionados, tampoco se aceptarán aquellos que tengan la denominación "refurbished", "remarketing" o su equivalente comercial.

El postor deberá acreditar en la presentación de la propuesta, el cumplimiento de las especificaciones técnicas de los bienes provistos, con folletos y/o manuales y/o catálogos y/o brochures u otros documentos técnicos similares emitidos por el fabricante, siendo las características y/o requisitos funcionales de las especificaciones técnicas que deberán ser acreditados por el postor, los que se incluyen en las siguientes secciones y literales:

NEXT GENERATION FIREWALL
A. DESCRIPCION: A3, A4. B. REQUERIMIENTOS SOPORTE: B1. C. CAPACIDAD DE RENDIMIENTO C1, C2, C3, C7, C8. D. CAPACIDADES DE NETWORKING D1, D2, D6. E. ALTA DISPONIBILIDAD E1, E4. F. FUNCIONALIDADES DE FIREWALL: F2, F4. G. DESCIFRADO DE TRÁFICO SSL/TLS: G2, G3, G4, G7. H. PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (DoS): H1, H3, H5. I. VISIBILIDAD EN CAPA 7 Y CONTROL DE APLICACIONES: I1, I3, I5, I6. J. PREVENCIÓN DE AMENAZAS: J1, J3, J6, J7, J9, J10, J11, J13. K. PREVENCIÓN DE AMENAZAS AVANZADAS EN DNS: K1, K3, K5. L. SANDBOXING: L1, L2, L3, L6, L7, L9, L11, L13. M. FILTRO DE CONTENIDO WEB: M1, M3, M6, M7. N. IDENTIFICACIÓN DE USUARIOS: N1, N2, N4, N5. O. QOS: O1, O2, O3, O5. P. FILTRO DE DATOS: P1, P2. Q. VPN: Q1, Q2, Q4, Q5, Q8, Q10, Q11. R. SD-WAN R1, R2, R3, R5, R7. S. CAPACIDADES DE OPTIMIZACIÓN: S1, S2, S3, S4, S6, S8. T. ADMINISTRACIÓN Y MONITOREO: T2, T3, T4, T7, T9, T11, T14.
H5 SOLUCIÓN DE SEGURIDAD DE ENDPOINT, DETECCIÓN Y RESPUESTA (EDR)
A. GENERALIDADES: A2, A3, A4, A5, A6. B. PROTECCIÓN CONTRA EXPLOITS: B1, B2, B3, B5, B7, B8, B10. C. PROTECCIÓN CONTRA MALWARE: C1, C2, C3, C4, C5, C7, C10. D. PLATAFORMA DE SANDBOXING: D1, D2, D3, D4. E. CONTROL DE DISPOSITIVOS: E3, E4, E5. F. TELEMETRÍA Y COLECCIÓN DE DATOS Y EVENTOS: F3, F4, F6, F7, F12, F14, F15. G. CAPACIDADES DE INVESTIGACIÓN Y THREAT HUNTING: G1, G2, G3, G7, G8, G9. H. CAPACIDADES DE GESTIÓN DE INCIDENTES: H1, H2, H3, H5, H7.

- I. CAPACIDADES DE THREAT INTELLIGENCE: I2, I3, I6, I7.
- J. CAPACIDADES DE USER ENTITY BEHAVIOR ANALYTICS (UEBA): J1, J2, J3, J6, J8.
- K. CAPACIDADES DE RESPUESTA: K1, K2, K4, K5, K6, K7, K11.
- L. DESCUBRIMIENTO DE ACTIVOS: L1, L2, L4.
- M. CARACTERÍSTICAS DEL AGENTE: M1, M2, M3, M4.
- N. CAPACIDADES DE GESTIÓN: N1, N2, N5, N7, N9, N10.

5.2. PRESTACIONES ACCESORIAS

5.2.1. SOPORTE TECNICO

- Se entiende por servicio de soporte técnico, que el Contratista deberá asegurar el soporte técnico especializado, actualizaciones y asesoramientos a la adquisición de la solución implementada, cuando se produzca alguna falla y/o avería en el equipamiento provisto.
- Deberá contar con un centro de atención de servicios, de tal manera que le asegure a la Entidad que se encuentra en condiciones de cumplir con los servicios estipulados en las bases durante todo el tiempo de la garantía este servicio debe estar disponible 24x7x365 y deberá indicar número de atención 0800 o número de Call Center.

Dicho soporte deberá estar a disposición en los siguientes términos:

- La cobertura de atención del soporte técnico deberá ser de lunes a domingo, las 24 horas, los 7 días de la semana y los 365 días del año por dos (02) años.
- Deberá proveerse un número telefónico de contacto (teléfono fijo y/o 0800 o una línea móvil, siempre y cuando esté disponible las 24x7x365 durante los dos (02) años), así como un correo electrónico de contacto, para la atención sobre cualquier avería, incidencia o requerimiento de la solución y hacer cumplir la garantía de la Solución, y ante una incidencia y/o requerimiento de soporte técnico, este será reportado por el personal designado por la Oficina de Sistemas de la entidad, de acuerdo a los tiempos de atención y reparación; esta documentación se acreditará con declaración jurada como documentación requerida para suscripción del contrato.
- El contratista deberá llevar un registro de las solicitudes del servicio (reportes de problemas), para el control y estadísticas de la entidad, lo que debe permitirle periódicamente ser utilizado como herramienta de seguimiento.
- El contratista a partir del día siguiente de emitida la conformidad de la Prestación Principal, debe emitir informes de la prestación accesoria en un plazo máximo de cinco (05) días calendario al término de la ejecución del soporte trimestral, donde se evidencie el cumplimiento de todo lo solicitado para la emisión de la conformidad respectiva.

5.2.2. MANTENIMIENTO PREVENTIVO

El contratista deberá realizar mantenimiento preventivo a la solución ofertada, de todo lo que forma parte de la prestación principal a nivel hardware y software, este servicio debe contemplar como mínimo dos (02) mantenimientos por año, por el periodo de dos (02) años, con el objetivo de garantizar el correcto funcionamiento de toda la solución implementada.

Este tendrá inicio, a partir del día siguiente de emitida la conformidad de la Prestación Principal.

Se deberá considerar las siguientes actividades como parte del Mantenimiento:

- La limpieza durante el mantenimiento preventivo será externa de todos los equipos físicos que se mencionan en la prestación principal y solo interna en caso sea necesario por alguna incidencia o recomendación del fabricante, teniendo en cuenta que el contratista deberá asegurar que dichas actividades no afecten la garantía.
- Revisión/Evaluación para diagnosticar el estado del equipo indicado, a nivel de Hardware y Software.
- Aplicación de actualizaciones de firmware (nuevas versiones y parches), de acuerdo a las recomendaciones del fabricante de la solución ofertada.
- Pruebas de funcionamiento del equipo, luego del mantenimiento realizado.
- La fecha y hora de los mantenimientos preventivos serán acordados con la Oficina de Sistemas a fin de minimizar el impacto en los servicios que brinda COFOPRI.
- El CONTRATISTA deberá adjuntar un cronograma de mantenimiento preventivo, como parte de su Plan de Trabajo y deberá ser aprobado por la Oficina de Sistemas.
- El CONTRATISTA debe emitir un informe de la prestación en un plazo máximo de cinco (05) días calendario al término de la ejecución de cada mantenimiento preventivo donde se evidencia el cumplimiento de todo lo solicitado para la emisión de la conformidad respectiva.

5.2.3. CAPACITACION

- El CONTRATISTA deberá brindar una transferencia de conocimiento teórica práctica para tres (03) personas de la Oficina de Sistemas.
- El contratista deberá incluir una capacitación para tres (03) personas con una duración mínima de veinte (20) horas, correspondiente a la solución implementada, debiendo considerar al menos los siguientes puntos en el temario:
 - Introducción
 - Funcionalidades, tecnologías y características.
 - Transferencia de conocimiento (Instalación, configuración y administración de la solución ofertada).
 - Administración/operación, mantenimiento y troubleshooting.
- La fecha de inicio y horario de la capacitación serán coordinados con la Oficina de Sistemas y el CONTRATISTA y se dictará dentro de los 30 días contabilizados a partir del día siguiente de emitida la conformidad de la Prestación Principal.
- La capacitación se realizará de manera remota (virtual) y/o presencial en las instalaciones del CONTRATISTA o centro de capacitación que este designe.
- Al finalizar la capacitación, se debe entregar las constancias de participación, donde se debe incluir: el nombre del participante, el día y duración de la capacitación.
- La capacitación deberá ser impartida por uno de los especialistas propuestos como personal clave.
- El CONTRATISTA debe emitir un informe de la capacitación al término de la capacitación para la emisión de la conformidad respectiva.

6. GARANTÍA COMERCIAL

Periodo de la Garantía

- EL CONTRATISTA deberá brindar una garantía por el periodo de dos (02) años contados a partir del día siguiente de la emisión de la conformidad de la Prestación Principal.
- La garantía deberá tener modalidad 24x7 ante cualquier avería de la infraestructura instalada, por el mal funcionamiento del equipo y/o desperfectos de fabricación, garantía integral sobre toda la solución.

Alcance de la Garantía

- El CONTRATISTA debe de garantizar que todos los bienes suministrados en virtud del contrato son nuevos, sin uso y de la versión más reciente.
- Garantía de buen funcionamiento de la solución (hardware y software), contra defectos de diseño y/o fabricación y averías.
- La garantía incluye para el hardware que comprende la solución, el reemplazo de las partes (por repuestos originales) o de todo el equipo de ser necesario, con instalación incluida.
- Todos los bienes y/o servicios a los que está obligado EL CONTRATISTA para cumplir con la garantía serán sin costo adicional para la entidad.

Condiciones de la Garantía

- COFOPRI notificará al CONTRATISTA sobre cualquier defecto o mal funcionamiento del producto inmediatamente después de haberlo descubierto, de acuerdo con el procedimiento de reporte de averías o solicitud de garantía de EL CONTRATISTA.
- EL CONTRATISTA reparará o reemplazará la totalidad de los componentes o productos defectuosos, instalará y dejará en funcionamiento, sin costo alguno para la entidad, en un plazo máximo de veinticuatro (24) horas contabilizadas a partir de la notificación de COFOPRI al Contratista.
- Los trabajos derivados de la aplicación de la garantía no tendrán ningún costo para COFOPRI, salvo el caso en que la falla sea imputable a COFOPRI.
- Asegurar y proveer todo lo necesario para garantizar un máximo nivel de mantenimiento y operatividad del equipo a adquirir y restaurar a éstos su funcionamiento normal cuando una falla se produzca.
-

7. PERFIL DEL PROVEEDOR Y DEL PERSONAL CLAVE

Proveedor:

- Tener Registro Único de Contribuyente habilitado.
- Se debe presentar en la oferta, como documento de admisibilidad, Carta y/o documento del fabricante y/o subsidiaria en el Perú del fabricante debidamente acreditado, que lo autorice o acredite al postor como: partner y/o comercializador y/o socio comercial y/o socio estratégico y/o distribuidor autorizado para la venta del equipamiento provisto.

Personal Clave:

• **Un (01) Jefe de Proyectos:**

Título Profesional	Profesional Titulado en Ingeniería de Sistemas o electrónica o industrial o Informático(a) o de Comunicaciones o Sistemas de Información o Sistemas Computacionales o de Telecomunicaciones o Redes y Comunicaciones de Datos o de Software.
Experiencia	Mínima de cinco (05) años en entidad pública o privada, como líder y/o gerente y/o supervisor y/o coordinador y/o gestor de proyectos y/o gerente de proyecto, en soluciones de TI y/o implementación de equipamiento de seguridad perimetral y/o desarrollo, implementación y operación de proyectos de integración de soluciones de TI y/o proyectos de gestión de servicios de TI.
Capacitación	○ Certificación PMP (Project Management Professional) emitida por el PMI (Project Management Institute) y/o Certificación en Scrum Master.
Actividades a desarrollar	Será el responsable de la definición, planificación y ejecución del proyecto, para lo cual deberá encargarse de coordinar las tareas y los equipos de trabajo. Se requiere que este personal deberá estar dedicado al 100% en la ejecución del proyecto.

• **Un (01) Especialista en Implementación de Firewall de Próxima Generación:**

Grado Académico o Técnico titulado	Bachiller en Ingeniería de Sistemas o electrónica o Informático (a) o de Comunicaciones o Sistemas de Información o Sistemas Computacionales o de Telecomunicaciones o Redes y Comunicaciones, o Técnico Titulado en sistemas y/o electrónica y/o telecomunicaciones y/o Informático y/o redes y comunicaciones.
Experiencia	Experiencia mínima de un (01) año en funciones de implementación y/o configuración y/o administración de la solución propuesta.
Capacitación	○ Capacitación mínima de 08 horas lectivas en administración y troubleshooting en soluciones de seguridad perimetral. ○ Certificación nivel administrador y/o profesional y/o experto y/o ingeniero, de soluciones de la marca propuesta.
Actividades a desarrollar	Se encargará de realizar las labores de instalación, configuración y puesta en funcionamiento del equipamiento de seguridad provisto.

- Un (01) Especialista en Implementación de Seguridad para EndPoint Detección y Respuesta:

Grado Académico o Técnico titulado	Bachiller en Ingeniería de Sistemas o electrónica o Informático (a) o de Comunicaciones o Sistemas de Información o Sistemas Computacionales o de Telecomunicaciones o Redes y Comunicaciones, o Técnico Titulado en Computación o Sistemas o Electrónica o Informático (a) o De Telecomunicaciones o Redes y Comunicaciones.
Experiencia	Experiencia mínima de un (01) año en funciones de implementación y/o configuración y/o administración de la solución propuesta.
Capacitación	<ul style="list-style-type: none"> ○ Capacitación mínima de 08 horas lectivas en administración y troubleshooting en soluciones de seguridad perimetral. ○ Certificación nivel administrador y/o profesional y/o experto y/o ingeniero, de soluciones de la marca propuesta.
Actividades a desarrollar	Se encargará de realizar las labores de configuración y despliegue de la solución de Seguridad para EndPoint Detección y Respuesta provista.

El personal clave propuesto por el Postor, no podrán asumir más de un Rol.

El postor adjudicado presentará como requisito para el perfeccionamiento de contrato el título profesional, el grado académico, el título técnico y capacitación solicitada.

En el caso el postor ganador de la buena pro haya presentado en su oferta documentos que provengan del extranjero, deberá presentar los documentos que acrediten surtir efectos legales en el Perú, conforme a lo señalado en la siguiente nota.

Nota: "Para que los documentos públicos o privados que provengan del extranjero puedan surtir efectos legales 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 Haya. Sin perjuicio de ello, además, los interesados deberán cumplir con los requisitos adicionales que contemple la normativa especial de la materia para la validez en el Perú de los documentos extendidos en el exterior.

De esta manera, una vez que los documentos públicos o privados extendidos en el extranjero hubiesen cumplido con todos los requisitos necesarios para dotarlos de validez en el Perú, estos pueden utilizarse en el marco de los procesos de contratación que desarrollen las Entidades"

8. LUGAR Y PLAZO DE ENTREGA

Lugar:

La entrega de los bienes deberá efectuarse en el almacén de COFOPRI, ubicada en la Av. Paseo de la Republica N° 3135 - 3137, San Isidro, en horario de atención: de lunes a viernes de 08:30 a.m. a 1:00 p.m. y de 2:00 p.m. a 4:30 p.m.

Asimismo, se menciona que la instalación debe ser realizada en el centro de datos, ubicado en la Av. Raúl Ferrero esquina con Los Sauces - La Molina, para lo cual el Contratista trasladará el equipo a la Sede de La Molina en coordinación con Almacén y la Oficina de Sistemas.

Plazo:

Las prestaciones se deberán entregar en el plazo establecido en el siguiente cuadro, en concordancia con lo establecido en el expediente de contratación.

PRESTACIÓN	ENTREGABLE	PLAZO
PRESTACIÓN PRINCIPAL	- Plan de Trabajo.	El CONTRATISTA deberá remitir el Plan de Trabajo en un plazo máximo de tres (3) días calendarios contabilizados a partir del día siguiente de la suscripción del contrato. La Entidad contará con un plazo máximo de cinco (5) días calendarios para la revisión y/o aprobación del Plan de Trabajo (de corresponder), contados a partir del día siguiente de la entrega del Plan de Trabajo por parte del Contratista. En caso de presentarse observaciones al Plan de Trabajo, el Contratista deberá levantarlas en un plazo máximo de tres (3) días calendarios contabilizados a partir del día siguiente de notificado por la Entidad.
	- Equipamiento. - Acta de instalación, configuración, pruebas y puesta en funcionamiento. - Informe Final.	El CONTRATISTA realizará la entrega del Equipamiento, instalación, configuración, pruebas y puesta en funcionamiento (incluye el acta) e Informe Final de la prestación principal, en un plazo máximo de treinta (30) días calendarios contabilizados a partir del día siguiente de la suscripción del contrato.
PRESTACIONES ACCESORIAS	- Soporte Técnico. - Informes de Soporte Técnico Trimestrales.	El CONTRATISTA realizará el servicio de Soporte Técnico, el cual debe ser brindado con una frecuencia de 7x24x365 durante dos (02) años contabilizados a partir del día siguiente de brindada la Conformidad de la prestación principal. El Informe de Soporte Técnico Trimestral deberá ser presentado en un plazo máximo de cinco (5) días calendarios de culminado el soporte técnico realizado durante el trimestre respectivo.
	- Mantenimiento Preventivo - Informes de Mantenimiento Preventivo semestral.	El CONTRATISTA deberá realizar dos (2) mantenimientos preventivos al año, por el periodo de dos (02) años, contabilizados a partir del día siguiente a la conformidad de la prestación principal, previa coordinación con la Oficina de Sistemas.
		El CONTRATISTA deberá realizar

	<p>- Capacitación.</p> <p>- Informe de Capacitación.</p>	<p>la capacitación en un plazo máximo de treinta (30) días calendarios, contabilizados a partir del día siguiente de la suscripción del contrato; asimismo deberá emitir un informe de la capacitación realizada, en un plazo no mayor de tres (3) días calendarios a partir del día siguiente del término de la capacitación.</p>
--	--	--

9. ENTREGABLES

El Contratista debe entregar toda la documentación dirigida a la Oficina de Sistemas de COFOPRI con copia a la Unidad de Abastecimiento, ubicada en la Av. Raúl Ferrero esquina con Los Sauces – La Molina, provincia y departamento de Lima, en horario de atención: de lunes a viernes de 09:00 hrs. a 12:00 hrs. y de 14:00 hrs. a 16:30 hr, o a través de la Mesa de Partes Virtual de COFOPRI (<http://mpv.cofopri.gob.pe>).

PRESTACIÓN PRINCIPAL:

▪ **Plan de Trabajo:**

El Contratista deberá entregar un Plan de Trabajo, para la aprobación por parte de la Oficina de Sistemas, dicho plan debe contener como mínimo:

- Diseño y arquitectura de solución a instalar
- Datos del equipo de trabajo
- Cronograma de Actividades
- Cronograma de Mantenimientos Preventivos.
- Cronograma y temario de capacitación.
- El contratista deberá entregar copia de los Seguro Complementario de Trabajo de Riesgo – Salud, para el personal destacado dichas coberturas deberán cubrir los daños contra, el cuerpo o la salud, por accidente de trabajo o enfermedad profesional que pudiera sufrir el personal a consecuencia de las prestaciones, y se incluye pensión de sobrevivencia, pensión de invalidez, muerte accidental y gastos de curación.

▪ **Acta e Informe Final de instalación, configuración y pruebas y puesta en funcionamiento:**

El Contratista deberá entregar un Informe final de la instalación y puesta en funcionamiento del sistema provisto, deberá incluir fotos, asimismo deberá evidenciar la configuración realizada.

En dicho informe se deberá adjuntar el Acta de la instalación, configuración y pruebas y puesta en funcionamiento respectivo, suscrito entre el Contratista y el responsable técnico designado por la Oficina de Sistemas.

PRESTACIONES ACCESORIAS:

▪ **Soporte Técnico:**

El CONTRATISTA debe emitir informes parciales de la prestación (en lapsos de noventa días calendarios) en el cual deberá evidenciarse el cumplimiento de todo lo solicitado y ejecutado, así como el tiempo empleado para la solución del incidente o avería y las horas consumidas correspondientes, a fin de emitir la conformidad respectiva por parte del área usuaria.

▪ **Mantenimiento preventivo:**

El CONTRATISTA debe emitir informes de la prestación en un plazo máximo de cinco (05) días calendario al término de la ejecución de cada mantenimiento preventivo semestral, el cual deberá evidenciarse el cumplimiento de todo lo solicitado y ejecutado, a fin de emitir la conformidad respectiva por parte del área usuaria.

▪ **Capacitación:**

El CONTRATISTA debe entregar un (01) informe a la Oficina de Sistemas adjuntando los certificados y/o constancias de participación por cada participante de la capacitación brindada, indicando fecha de inicio y fin, horas lectivas y firmada por el instructor o capacitador.

10. CONFORMIDAD

La conformidad será otorgada por la Oficina de Sistemas, previa recepción y revisión de los entregables.

De existir observaciones, se le otorgará al Contratista un plazo no menor a dos (02) días, ni mayor ocho (08) días calendario, dependiendo de la complejidad de la observación.

11. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del Contratista según el siguiente detalle:

Prestación	Descripción	Forma de Pago
PRESTACION PRINCIPAL	<ul style="list-style-type: none"> Entrega del equipamiento Instalación, configuración, pruebas y puesta en Funcionamiento. 	En un único pago, luego de emitida la conformidad por parte de la Oficina de Sistemas de la Prestación Principal.
PRESTACIONES ACCESORIAS	SOPORTE TECNICO	Los pagos se realizarán de forma parcial y proporcional a un octavo del monto total de la prestación, previa conformidad por parte de la Oficina de Sistemas, al servicio de Soporte Técnico trimestral efectuado.
	MANTENIMIENTO PREVENTIVO	Los pagos se realizarán de forma parcial y proporcional a un cuarto del monto total de la prestación, previa conformidad por parte de la Oficina de Sistemas, a cada mantenimiento preventivo efectuado.
	CAPACITACION	En un único pago, luego de emitida la conformidad por parte de la Oficina de Sistemas a la capacitación efectuada.

12. NIVELES DE SERVICIO SLA

El Contratista debe cumplir con los siguientes niveles de servicios (SLA):

ATENCIONES	TIEMPO DE SOLUCIÓN
Soporte técnico y atención de Incidentes por falla de hardware y/o software.	Cuatro (4) horas como máximo, contabilizados desde comunicado el incidente por parte de la entidad.

En caso superen los tiempos máximos indicados se aplicarán las penalidades indicadas en el Numeral 14. (OTRAS PENALIDADES).

13. PENALIDADES

Penalidad por Mora en la ejecución de la prestación del bien adquirido:

En caso de retraso injustificado en la ejecución de las prestaciones, el COFOPRI aplicará al contratista una penalidad por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto total de la orden de compra y/o contrato, de ser el caso del ítem que debió ejecutarse.

Esta penalidad será deducida del pago a realizarse.

La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

Penalidad diaria = $(0.10 \times \text{Monto vigente}) / (F \times \text{Plazo vigente en días})$ Donde F tendrá los siguientes valores:

Para plazos menores o iguales a sesenta (60) días, para bienes : $F = 0.40$.

Se considera justificado el retraso, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. Esta calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.

14. OTRAS PENALIDADES

El cálculo de otras penalidades se realizará de acuerdo con lo siguiente:

- **Supuesto de aplicación de penalidad:** El nivel del servicio (SLA) brindado por el Contratista en el Soporte técnico y atención de Incidentes, por cada periodo trimestral, no es el mínimo esperado de 99.75%.
- **Forma de cálculo:**

El UPTIME es un coeficiente que mide el nivel de servicio brindado por el Contratista en un periodo mensual.

Se calcula el UPTIME de la siguiente forma:

$$\text{UPTIME} = \frac{\text{THM} - \text{THE}}{\text{THM}}$$

Siendo:

- THM: igual a la cantidad de horas brindada por el Contratista en un periodo de noventa días.
- THE: es la sumatoria de la cantidad de horas de exceso (respecto al tiempo máximo establecido para solucionar un incidente o avería reportado,

acorde a lo indicado en el numeral 12. NIVELES DE SERVICIO SLA, en que incurrió el Contratista en el periodo de noventa días, para solucionar dichos incidentes o averías.

Ejemplo:

Si el tiempo máximo para solucionar una atención de un incidente o avería es de 04 horas, y se reportaron 04 incidentes o averías en un periodo de noventa días, dos se reportaron dentro del tiempo de solución de problemas establecido (04 horas) y dos fueron resueltos excediendo los tiempos de respuesta establecidos, con 4 y 3 horas de retraso respectivamente.

El UPTIME será:

THM = $24 \times 90 = 2,160$ horas.

THE = $4 + 3 = 7$ horas de exceso.

UPTIME = $\frac{2160 - 7}{2160} = 99.68\%$

La penalidad por periodo de noventa días estará en función al UPTIME, según la siguiente tabla:

Rango de UPTIME	Penalidad (1)
> 99.50%, <= 99.75%	1.00% de UIT
> 98.99%, <= 99.50%	1.50% de UIT
> 98.50%, <= 98.99%	2.00% de UIT
> 97.99%, <= 98.50%	2.50% de UIT
> 97.50%, <= 97.99%	3.00% de UIT
> 96.99%, <= 97.50%	3.50% de UIT
> 96.50%, <= 96.99%	4.00% de UIT
> 95.99%, <= 96.50%	4.50% de UIT
> 95.50%, <= 95.99%	5.00% de UIT
> 94.99%, <= 95.50%	5.50% de UIT
> 94.50%, <= 94.99%	6.00% de UIT
> 93.99%, <= 94.50%	6.50% de UIT
> 93.50%, <= 93.99%	7.00% de UIT
> 92.99%, <= 93.50%	7.50% de UIT
> 92.50%, <= 92.99%	8.00% de UIT
> 91.99%, <= 92.50%	8.50% de UIT
> 91.50%, <= 91.99%	9.00% de UIT
> 90.99%, <= 91.50%	9.50% de UIT
Menor o igual a 90.99%	10% de UIT

Nota: El monto de la UIT es el vigente al momento de aplicar la penalidad. Para el caso del ejemplo arriba mencionado, el Contratista tendrá una penalidad en dicho periodo, equivalente al 1.0% UIT. Este porcentaje se descontará del pago a realizar para dicho periodo.

- **Procedimiento mediante el cual se verifica el supuesto a penalizar:**

Se realizará a través de los registros de solicitudes de servicio, que deben ser generados por el Contratista, indicado en el numeral 12. NIVELES DE SERVICIO SLA de las Especificaciones Técnicas, en el cual se debe indicar el tiempo de solución de cada incidente o avería, de acuerdo con lo establecido en la sección Tiempo de Solución de dicho numeral.

15. MODALIDAD DE EJECUCION

Llave en mano.

16. SISTEMA DE CONTRATACION

A Suma alzada

17. RESPONSABILIDADES DEL CONTRATISTA – VICIOS OCULTOS

El Contratista será responsable por la calidad ofrecida y por vicios ocultos del bien ofertado por un plazo de dos (02) años, contabilizados a partir del día siguiente de emitida la conformidad de la prestación principal.

18. CONFIDENCIALIDAD

El Contratista se compromete a no revelar ni permitir la revelación de cualquier información y a no usar el nombre de El COFOPRI en cualquier situación.

En caso de infringir lo indicado en el acuerdo de confidencialidad, LA ENTIDAD se reserva el derecho de iniciar los procedimientos legales correspondientes.

19. CLAUSULA ANTICORRUPCION

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 que se suscriba.

Asimismo, el Contratista se obliga a conducirse en todo momento, durante la ejecución del servicio, 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 RLCE.

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.

20. SECUENCIA FUNCIONAL DE META

Meta: 0138.

3.2. REQUISITOS DE CALIFICACIÓN

B.	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/. 400,000.00 (Cuatrocientos mil con 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>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/. 50,000.00 (Cincuenta mil con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los 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. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.</p> <p>Se consideran bienes similares a los siguientes:</p> <ul style="list-style-type: none"> • Venta de Firewall • Venta e instalación de equipo s firewalls • Venta de sistemas seguridad perimetral para centro de datos y/o data centers • Venta de sistemas de firewall para centro de datos y/o data centers. • Venta de Firewalls de Siguiete generación o Next Generación Firewalls (NGFW) • Venta de solución de seguridad perimetral • Venta de Seguridad Firewall. <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 pago¹² 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</p>

¹² 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".

	<p>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 sustentatoria correspondiente.</p> <p>Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.</p> <p>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.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <div data-bbox="293 663 1382 824"> <p>Importante</p> <p><i>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”.</i></p> </div>
--	--

C.	CAPACIDAD TÉCNICA Y PROFESIONAL
C.1	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>01 Jefe de Proyectos Mínima de cinco (05) años en entidad pública o privada, como líder y/o gerente y/o supervisor y/o coordinador y/o gestor de proyectos y/o gerente de proyecto, en soluciones de TI y/o implementación de equipamiento de seguridad perimetral y/o desarrollo, implementación y operación de proyectos de integración de soluciones de TI y/o proyectos de gestión de servicios de TI.</p> <p><u>Un (01) Especialista en Implementación de Firewall de Próxima Generación:</u> Experiencia mínima de un (01) año en funciones de implementación y/o configuración y/o administración de soluciones de seguridad perimetral.</p> <p><u>Un (01) Especialista en Implementación de Seguridad para EndPoint Detección y Respuesta:</u> Experiencia mínima de un (01) año en funciones de implementación y/o configuración y/o administración de soluciones de seguridad perimetral.</p> <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="293 1581 1422 2047"> <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 y 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> </div>

- *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*

Importante

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

CAPÍTULO IV
FACTORES DE EVALUACIÓN

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

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

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
<p><u>Evaluación:</u> Se evaluará considerando el precio ofertado por el postor.</p> <p><u>Acreditación:</u> 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 P_i = Puntaje de la oferta a evaluar O_i = Precio <i>i</i> O_m = Precio de la oferta más baja PMP = Puntaje máximo del precio </p> <p style="text-align: right;">100 puntos</p>

CAPÍTULO V PROFORMA DEL CONTRATO

Importante

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

Conste por el presente documento, la contratación de la ADQUISICIÓN DE UN SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED - FIREWALL, que celebra de una parte el ORGANISMO DE FORMALIZACIÓN DE LA PROPIEDAD INFORMAL - COFOPRI, en adelante LA ENTIDAD, con RUC N° 20306484479, con domicilio legal en Av. Paseo de la República N° 3135 – 3137 San Isidro, 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 órgano encargado de las contrataciones o el comité de selección, según corresponda, adjudicó la buena pro de la **ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – Primera Convocatoria** para la contratación de la ADQUISICIÓN DE UN SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED - FIREWALL, 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 ADQUISICIÓN DE UN SISTEMA DE PROTECCIÓN Y SEGURIDAD PARA RED - FIREWALL.

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 PAGO¹³

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en SOLES, en PAGO ÚNICO, 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 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.

¹³ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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 treinta (30) días calendarios, el mismo que se computa desde el día siguiente de la suscripción del contrato.

CLÁUSULA SEXTA: PRESTACIONES ACCESORIAS¹⁴

“Las prestaciones accesorias tienen por objeto suministrar los servicios de Soporte Técnico, Mantenimiento Preventivo y Capacitación para el Sistema materia de adquisición.

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 dos (02) años (Soporte técnico y Mantenimiento preventivo) y de treinta (30) días calendarios (Capacitación), el mismo que se computa desde el día siguiente de brindada la conformidad de la prestación principal (Soporte técnico y Mantenimiento preventivo) y treinta (30) días calendarios que se computan a partir del día siguiente de la suscripción del contrato (Capacitación).

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

En el caso que corresponda, consignar lo siguiente:

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

Importante

De conformidad con el artículo 152 del Reglamento, no se constituirá garantía de fiel cumplimiento del contrato ni garantía de fiel cumplimiento por prestaciones accesorias, en contratos cuyos montos sean iguales o menores a doscientos mil Soles (S/ 200,000.00). Dicha excepción también aplica a 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 no supere el monto señalado anteriormente.

¹⁴ 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) accesorias, 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.

CLÁUSULA NOVENA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

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

CLÁUSULA DÉCIMA: RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La recepción será otorgada por EL ALMACÉN O LA QUE HAGA SUS VECES y la conformidad será otorgada por la Oficina de Sistemas en el plazo máximo de SIETE (7) DÍAS de producida la recepción o máximo quince (15) días, en caso se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación.

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 dos (02) años contados 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

El cálculo de otras penalidades se realizará de acuerdo con lo siguiente:

- **Supuesto de aplicación de penalidad:** El nivel del servicio (SLA) brindado por el Contratista en el Soporte técnico y atención de Incidentes, por cada periodo trimestral, no es el mínimo esperado de 99.75%.

- **Forma de cálculo:**

El UPTIME es un coeficiente que mide el nivel de servicio brindado por el Contratista en un periodo mensual.

Se calcula el UPTIME de la siguiente forma:

$$\text{UPTIME} = \frac{\text{THM} - \text{THE}}{\text{THM}}$$

Siendo:

- THM: igual a la cantidad de horas brindada por el Contratista en un periodo de noventa días.
- THE: es la sumatoria de la cantidad de horas de exceso (respecto al tiempo máximo establecido para solucionar un incidente o avería reportado,

acorde a lo indicado en el numeral 12. NIVELES DE SERVICIO SLA, en que incurrió el Contratista en el periodo de noventa días, para solucionar dichos incidentes o averías.

Ejemplo:

Si el tiempo máximo para solucionar una atención de un incidente o avería es de 04 horas, y se reportaron 04 incidentes o averías en un periodo de noventa días, dos se reportaron dentro del tiempo de solución de problemas establecido (04 horas) y dos fueron resueltos excediendo los tiempos de respuesta establecidos, con 4 y 3 horas de retraso respectivamente.

El UPTIME será:

$$\text{THM} = 24 \times 90 = 2,160 \text{ horas.}$$

$$\text{THE} = 4 + 3 = 7 \text{ horas de exceso.}$$

$$\text{UPTIME} = \frac{2160 - 7}{2160} = 99.68\%$$

La penalidad por periodo de noventa días estará en función al UPTIME, según la siguiente tabla:

Rango de UPTIME	Penalidad (1)
> 99.50%, <= 99.75%	1.00% de UIT
> 98.99%, <= 99.50%	1.50% de UIT
> 98.50%, <= 98.99%	2.00% de UIT
> 97.99%, <= 98.50%	2.50% de UIT
> 97.50%, <= 97.99%	3.00% de UIT
> 96.99%, <= 97.50%	3.50% de UIT
> 96.50%, <= 96.99%	4.00% de UIT
> 95.99%, <= 96.50%	4.50% de UIT
> 95.50%, <= 95.99%	5.00% de UIT
> 94.99%, <= 95.50%	5.50% de UIT
> 94.50%, <= 94.99%	6.00% de UIT
> 93.99%, <= 94.50%	6.50% de UIT
> 93.50%, <= 93.99%	7.00% de UIT
> 92.99%, <= 93.50%	7.50% de UIT
> 92.50%, <= 92.99%	8.00% de UIT
> 91.99%, <= 92.50%	8.50% de UIT
> 91.50%, <= 91.99%	9.00% de UIT
> 90.99%, <= 91.50%	9.50% de UIT
Menor o igual a 90.99%	10% de UIT

Nota: El monto de la UIT es el vigente al momento de aplicar la penalidad. Para el caso del ejemplo arriba mencionado, el Contratista tendrá una penalidad en dicho periodo, equivalente al 1.0% UIT. Este porcentaje se descontará del pago a realizar para dicho periodo.

Procedimiento mediante el cual se verifica el supuesto a penalizar:

Se realizará a través de los registros de solicitudes de servicio, que deben ser generados por el Contratista, indicado en el numeral 12. NIVELES DE SERVICIO SLA de las Especificaciones Técnicas, en el cual se debe indicar el tiempo de solución de cada incidente o avería, de acuerdo con lo establecido en la sección Tiempo de Solución de dicho numeral.

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

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

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

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

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

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

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

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

Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

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

CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO

Sólo en lo no previsto en este contrato, en la Ley de Contrataciones del Estado y su Reglamento, en las directivas que emita el OSCE y demás normativa especial que resulte aplicable, serán de

aplicación supletoria las disposiciones pertinentes del Código Civil vigente, cuando corresponda, y demás normas de derecho privado.

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS¹⁵

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

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

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

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 45.21 del artículo 45 de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

Cualquiera de las partes puede elevar el presente contrato a Escritura Pública corriendo con todos los gastos que demande esta formalidad.

CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución del presente contrato:

DOMICILIO DE LA ENTIDAD: [.....]

DOMICILIO DEL CONTRATISTA: [CONSIGNAR EL DOMICILIO SEÑALADO POR EL POSTOR GANADOR DE LA BUENA PRO AL PRESENTAR LOS REQUISITOS PARA EL PERFECCIONAMIENTO DEL CONTRATO]

La variación del domicilio aquí declarado de alguna de las partes debe ser comunicada a la otra parte, formalmente y por escrito, con una anticipación no menor de quince (15) días calendario.

De acuerdo con las bases integradas, la oferta y las disposiciones del presente contrato, las partes lo firman por duplicado en señal de conformidad en la ciudad de [.....] al [CONSIGNAR FECHA].

“LA ENTIDAD”

“EL CONTRATISTA”

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹⁶.

¹⁵ 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).

¹⁶ 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

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – PRIMERA CONVOCATORIA

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):		
MYPE ¹⁷		Sí	No
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 compra¹⁸

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.

¹⁷ Esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

¹⁸ Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso 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

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – PRIMERA CONVOCATORIA

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) :			
MYPE ¹⁹		Sí		No	
Correo electrónico:					

Datos del consorciado 2					
Nombre, Denominación o Razón Social :					
Domicilio Legal:					
RUC :		Teléfono(s) :			
MYPE ²⁰		Sí		No	
Correo electrónico:					

Datos del consorciado ...					
Nombre, Denominación o Razón Social :					
Domicilio Legal:					
RUC :		Teléfono(s) :			
MYPE ²¹		Sí		No	
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.

¹⁹ Esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

²⁰ Ibidem.

²¹ Ibidem.

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 compra²²

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del representante
común del consorcio**

Importante

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

²² Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso se haya optado por perfeccionar el contrato con una orden de compra.

ANEXO N° 2

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

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – PRIMERA CONVOCATORIA

Presente. -

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento:

- i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.
- ii. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.
- iii. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- iv. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo N° 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.
- v. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.
- vi. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.
- vii. Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

En el caso de consorcios, cada integrante debe presentar esta declaración jurada, salvo que sea presentada por el representante común del consorcio.

ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – PRIMERA CONVOCATORIA

Presente. -

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el [CONSIGNAR EL OBJETO DE LA CONVOCATORIA], de conformidad con las Especificaciones Técnicas que se indican en el numeral 3.1 del Capítulo III de la sección específica de las bases y los documentos del procedimiento.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

Adicionalmente, puede requerirse la presentación de documentación que acredite el cumplimiento de las especificaciones técnicas, conforme a lo indicado en el acápite relacionado al contenido de las ofertas de la presente sección de las bases.

ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE ENTREGA

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – PRIMERA CONVOCATORIA

Presente. -

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a entregar los bienes objeto del presente procedimiento de selección en el plazo de [CONSIGNAR EL PLAZO OFERTADO. EN CASO DE LA MODALIDAD DE LLAVE EN MANO DETALLAR EL PLAZO DE ENTREGA, SU INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO].

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 5

PROMESA DE CONSORCIO

(Sólo para el caso en que un consorcio se presente como postor)

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – PRIMERA CONVOCATORIA

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 **ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – PRIMERA CONVOCATORIA**

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] [%]²³

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²⁴

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES 100%²⁵

[CONSIGNAR CIUDAD Y FECHA]

²³ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²⁴ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²⁵ 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

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – PRIMERA CONVOCATORIA

Presente. -

Es grato dirigirme a usted, para hacer de su conocimiento que, de acuerdo con las bases, mi oferta es la siguiente:

CONCEPTO	PRECIO TOTAL
PRESTACIÓN PRINCIPAL	
PRESTACIÓN ACCESORIA	
TOTAL	

El precio de la oferta [CONSIGNAR LA MONEDA DE LA CONVOCATORIA] incluye todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre el costo del bien a contratar; excepto la de aquellos postores que gocen de alguna exoneración legal, no incluirán en el precio de su oferta los tributos respectivos.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

- El postor debe consignar el precio total de la oferta, sin perjuicio que, de resultar favorecido con la buena pro, presente el detalle de precios unitarios para el perfeccionamiento del contrato.*
- El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:*

“Mi oferta no incluye [CONSIGNAR EL TRIBUTO MATERIA DE LA EXONERACIÓN]”.

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – PRIMERA CONVOCATORIA
Presente. -

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

Nº	CLIENTE	OBJETO DEL CONTRATO	Nº CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²⁶	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁷	EXPERIENCIA PROVENIENTE ²⁸ DE:	MONEDA	IMPORTE ²⁹	TIPO DE CAMBIO VENTA ³⁰	MONTO FACTURADO ACUMULADO ³¹
1										
2										
3										
4										

²⁶ 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.

²⁷ 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.

²⁸ 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”.

²⁹ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

³⁰ 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.

³¹ 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 ²⁶	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁷	EXPERIENCIA PROVENIENTE ²⁸ DE:	MONEDA	IMPORTE ²⁹	TIPO DE CAMBIO VENTA ³⁰	MONTO FACTURADO ACUMULADO ³¹
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

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – PRIMERA CONVOCATORIA

Presente. -

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro que la experiencia que acredito de la empresa [CONSIGNAR LA DENOMINACIÓN DE LA PERSONA JURÍDICA] como consecuencia de una reorganización societaria, no se encuentra en el supuesto establecido en el numeral 49.4 del artículo 49 del Reglamento.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

A efectos de cautelar la veracidad de esta declaración, el postor puede verificar la información de la Relación de Proveedores Sancionados por el Tribunal de Contrataciones del Estado con Sanción Vigente en <http://portal.osce.gob.pe/rnp/content/relación-de-proveedores-sancionados>.

También le asiste dicha facultad al órgano encargado de las contrataciones o al órgano de la Entidad al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.

ANEXO N° 10

SOLICITUD DE BONIFICACIÓN DEL CINCO POR CIENTO (5%) POR TENER LA CONDICIÓN DE MICRO Y PEQUEÑA EMPRESA

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – PRIMERA CONVOCATORIA

Presente. -

Mediante el presente el suscrito, postor y/o Representante legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], solicito la asignación de la bonificación del cinco por ciento (5%) sobre el puntaje total obtenido, debido a que mi representada cuenta con la condición de micro y pequeña empresa.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

- Para asignar la bonificación, el órgano encargado de las contrataciones o comité de selección, según corresponda, verifica la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/>.
- Para que un consorcio pueda acceder a la bonificación, cada uno de sus integrantes debe cumplir con la condición de micro y pequeña empresa.

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

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-COFOPRI – PRIMERA CONVOCATORIA

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.