BASES ADMINISTRATIVAS DE CONCURSO PÚBLICO PARA LA CONTRATACIÓN DE SERVICIOS EN GENERAL

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

OSCE Organismo Supervisor de las Contrataciones del Estado

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	**Importante** • *Abc*	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	***Advertencia*** • *Abc*	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	**Importante para la Entidad** • *Xyz*	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

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

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:

1. *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.*

2. *La nota **IMPORTANTE** no puede ser modificada ni eliminada en la Sección General. En el caso de la Sección Específica debe seguirse la instrucción que se indica en dicha nota.*

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

BASES INTEGRADAS

BASES ADMINISTRATIVAS DE CONCURSO PÚBLICO PARA LA CONTRATACIÓN DE SERVICIOS EN GENERAL

CONCURSO PÚBLICO Nº 15-2024-GRP-ORA-CS-CP-1

CONTRATACIÓN DEL SERVICIO DE INTERNET – SEGURIDAD PERIMETRAL PARA LA SEDE CENTRAL DEL GOBIERNO REGIONAL PIURA.

DEBER DE COLABORACIÓN

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

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

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

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

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

Importante

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

Importante

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

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

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

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

Advertencia

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

Importante

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley Nº 27269, Ley de Firmas y Certificados Digitales[1]). 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*

[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

coincida con lo declarado a través del SEACE, prevalece la información declarada en los documentos escaneados.

- *No se tomarán en cuenta las ofertas que se presenten en físico a la Entidad.*

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

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

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

1.9. EVALUACIÓN DE LAS OFERTAS

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

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

1.10. CALIFICACIÓN DE OFERTAS

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

1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.12. RECHAZO DE LAS OFERTAS

Previo al otorgamiento de la buena pro, el comité de selección revisa las ofertas económicas

que cumplen los requisitos de calificación, de conformidad con lo establecido para el rechazo de ofertas, previsto en el artículo 68 del Reglamento, de ser el caso.

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

1.13. OTORGAMIENTO DE LA BUENA PRO

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

1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

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

CAPÍTULO II
SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

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

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

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

- *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

CAPÍTULO III
DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

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

- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establecen los numerales 149.4 y 149.5 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento.*

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

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

Advertencia
Los funcionarios de las Entidades no deben aceptar garantías emitidas bajo condiciones distintas a las establecidas en el presente numeral, debiendo tener en cuenta lo siguiente: *1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo).* *2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.* *3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.* *4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.* *En caso exista alguna duda sobre la clasificación de riesgo asignada a la empresa emisora de la garantía, se deberá consultar a la clasificadora de riesgos respectiva.* *De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza).* *Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.*

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

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

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

La Entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, 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	:	GOBIERNO REGIONAL PIURA – SEDE CENTRAL
RUC N°	:	20484004421
Domicilio legal	:	Av. Fortunato Chirichigno S/N San Eduardo el Chipe – Piura
Teléfono:	:	073 – 264800 - Anexo 4173
Correo electrónico:	:	procesos_oasa@regionpiura.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la CONTRATACIÓN DEL SERVICIO DE INTERNET – SEGURIDAD PERIMETRAL PARA LA SEDE CENTRAL DEL GOBIERNO REGIONAL PIURA

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante MEMORANDUM N° 789-2024/GRP-480000 el 05 de julio 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 **SUMA ALZADA**, de acuerdo con lo establecido en el expediente de contratación respectivo.

1.6. DISTRIBUCIÓN DE LA BUENA PRO

NO CORRESPONDE

1.7. ALCANCES DEL REQUERIMIENTO

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

1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

Los servicios materia de la presente convocatoria se prestarán en el plazo de **UN MIL NOVENTA Y CINCO (1095) DIAS CALENDARIO** contado a partir del Acta de Conformidad de activación del servicio en concordancia con lo establecido en el expediente de contratación.
El plazo para la activación del servicio no deberá exceder de 80 días calendario a partir del día siguiente de la suscripción de contrato.

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/ 5.00 (Cinco con 00/100 Soles) en Oficina de Tesorería y recabar las bases en la Oficina de Abastecimiento y Servicios Auxiliares del Gobierno Regional Piura, sito en Av. Fortunato Chirichigno S/N – Urb. San Eduardo-El Chipe-Piura.

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

1.10. BASE LEGAL

- Ley Nº 31953 Ley de Presupuesto del Sector Público para el Año Fiscal 2024.
- Ley Nº 31954 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2024.
- Texto Único Ordenado de la Ley N° 30225, Ley de Contrataciones del Estado. Aprobado mediante Decreto Supremo N° 082-2019-EF
- Ley Nº 30225, Ley de Contrataciones del Estado, modificada por el Decreto Legislativo N° 1341 y Decreto Legislativo N° 1444.
- Reglamento de la Ley N° 30225, aprobado mediante Decreto Supremo N° 344-2018-EF, modificado por Decreto Supremo N° 377-2019-EF, Decreto Supremo N° 168-2020-EF, Decreto Supremo N° 250-2020-EF, Decreto Supremo N° 162-2021-EF, Decreto Supremo N° 234-2022-EF y Decreto Supremo N° 308-2022-EF.
- DECRETO SUPREMO N° 004-2019-JUS, que aprueba la el Texto Único Ordenado de la Ley N° 27444 Ley del Procedimiento Administrativo General.
- Ley N° 27809, Ley de Transparencia y de Acceso a la Información Pública
- Decreto Supremo N° 008-2008-TR, Reglamento de la Ley Mype
- Directivas OSCE.
- Decreto Supremo Nº 011-79-VC.

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 documentos[2], la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

a) Declaración jurada de datos del postor. **(Anexo N° 1)**

b) Documento que acredite la representación de quien suscribe la oferta.

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

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

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

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

c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. **(Anexo N° 2)**

d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo N° 3**)

e) El postor deberá presentar documentos que acredite la **información de carácter técnico del equipamiento propuesto que sustente el servicio ofertado,**

[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/

incluirá como mínimo los detalles técnicos del equipo router, del equipo de seguridad perimetral, así como las especificaciones técnicas estándar del fabricante; los cuales son de su entero conocimiento, en los cuales se indiquen las características principales de los mismos. El postor será responsable de la exactitud y veracidad de dichos documentos, por ende, toda información entregada por el postor en su oferta tendrá carácter de declaración jurada.

f) Declaración jurada de plazo de prestación del servicio. **(Anexo N° 4)**[4]

g) 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**)

h) El precio de la oferta en SOLES. Adjuntar obligatoriamente el **Anexo N° 6.**

El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales. Los precios unitarios pueden ser expresados con más de dos (2) decimales.

Importante
• *El comité de selección verifica la presentación de los documentos requeridos. De no cumplir con lo requerido, la oferta se considera no admitida.*
• *En caso de requerir estructura de costos o análisis de precios, esta se presenta para el perfeccionamiento del contrato.*

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:

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

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

a) Garantía de fiel cumplimiento del contrato.
b) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes de ser el caso.
c) 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.
d) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
e) 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

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

medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE[5] 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).

f) Domicilio para efectos de la notificación durante la ejecución del contrato.
g) Detalle de los precios unitarios del precio ofertado[6].
h) Diagrama de red o topología donde se indique las direcciones o ubicaciones de los servidores DNS redundantes.
i) Declaración jurada indicando el número telefónico 0800 gratuito para la atención de las llamadas.
j) Declaración jurada indicando los números de celular de por lo menos tres (03) soportes para escalamiento de la atención que se requiera en temas de configuración inmediata de los diversos equipos de seguridad propuestos y ante alguna contingencia de intentos de violación de la seguridad.
k) Diagrama o topología de la arquitectura (Redes, interconexión, protocolos) de la solución propuesta, incluyendo todo lo que constituye la oferta del operador de comunicaciones, así como sus rutas alternas de respaldo.

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 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 periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link http://www2.trabajo.gob.pe/servicios-en-linea-2-2 opción consulta de empresas acreditadas en el REMYPE.*

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

Importante

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

- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y*

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

[6] Incluir solo en caso de la contratación bajo el sistema a suma alzada.

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[7].

- *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:

Lugar: Gobierno Regional de Piura – Sede Central Av. Fortunato Chirichigno s/n Urb. San Eduardo El Chipe-PIURA/PIURA/PIURA
Oficina: Tramite Documentario.

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

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en **PAGOS PERIÓDICOS.**

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

En el Primer Pago:
- Informe final con detalles técnicos de infraestructura de telecomunicaciones implementados en la Sede Central del Gobierno Regional Piura, así como información con respecto a la tecnología utilizada, equipos y accesorios, previa aprobación de la Oficina de Tecnologías de la Información.
- Acta de Conformidad de Activación del Servicio.
- Informe Mensual del Servicio realizado por el funcionario responsable de la Oficina de Tecnologías de la Información emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago (Recibo de servicios de acuerdo al formato debidamente aprobado por SUNAT y OSIPTEL).

Pagos Posteriores:
- Informe Mensual del servicio realizado por el funcionario responsable de la Oficina de Tecnologías de la Información emitiendo la conformidad de la prestación efectuada.

Se debe tener en cuenta, sin que afecte el valor del monto adjudicado, en caso que el inicio de la prestación del servicio no coincida con el ciclo de facturación del operador adjudicatario de la buena pro, la primera y la última facturación incluirá un cargo por el prorrateo del servicio brindado durante los días previos al inicio y culminación del correspondiente ciclo de facturación.

Dicha documentación se debe presentar en en TRAMITE DOCUMENTARIO, con atención a la Dirección de Obras, sito en Av. San Ramón N° 525 Urb. San Eduardo El Chipe – Piura.

[7] 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. TERMINOS DE REFERENCIA

SERVICIO DE INTERNET - SEGURIDAD PERIMETRAL E INFORMATICA PARA LA SEDE CENTRAL DEL GOBIERNO REGIONAL PIURA

1. **OBJETIVO**

   Proveer a la Sede Central del Gobierno Regional Piura del Servicio de Internet y Seguridad Perimetral.

2. **ASPECTOS GENERALES DE LOS SERVICIOS SOLICITADOS**

   - Los medios de transmisión que IMPLEMENTE el proveedor, deberán cumplir con las normas vigentes de cableado estructurado, respetando la planificación y el ornato de las sedes del Gobierno Regional Piura.
   - El Proveedor es responsable de la operatividad de los enlaces de comunicación y del buen funcionamiento, licencias, actualización de hardware (averia a cambios tecnológicos), firmware y software de sistema operativo de sus equipos de comunicación durante la duración del contrato.

3. **PLAZO DE ENTREGA DEL SERVICIO Y TIEMPO DE DURACION DEL SERVICIO**

   - El plazo para la activación del servicio no deberá exceder de 80 días calendarios a partir del día siguiente de la suscripción del contrato.
   - Tiempo de duración del Servicio a 36 meses a partir del acta de conformidad de activación del servicio, es decir por un periodo de 1095 días calendario

4. **CARACTERÍSTICAS DEL SERVICIO**

   - Enlace a internet dedicado con un ancho de banda de al menos 800 Mbps, deberá ser simétrico y con un Overbooking 1:1 en el enlace local y 1:1 hasta la puerta de enlace de su proveedor internacional.
   - El Overbooking solicitado de 1:1 corresponde desde la puerta de enlace del router de internet de la Sede Central del Gobierno Regional Piura hasta la puerta de enlace del proveedor conectado directamente al (los) proveedor(es) de Internet.
   - El medio físico de transporte deberá ser 100% fibra óptica tanto en el lado internacional, nacional, local y en la última milla será con fibra óptica propia 100% canalizada y/o subterránea y/o aérea(antiroedores), desde el Punto de presencia del Postor hasta el local de Gobierno Regional de Piura in situ en Av. Fortunato Chirichigno S/N URB. SAN EDUARDO - EL CHIPE - PIURA (Oficina de Tecnologías de la Información). Cuyas coordenadas geográficas son las siguientes:

69

2

Latitud Sur :5°10'49.33" S
Longitud Oeste :80°37'42.01"O

- La entidad brindará lo siguiente:
  - Espacio en gabinetes/racks para la instalación de los equipos
  - Energía estabilizada.
  - Sistema de aterramiento.
  - Switches y cableado LAN.

- Considerando que se solicita enlace de contingencia, el medio físico de transporte será de Fibra óptica y el tendido del mismo podrá ser de manera aérea o subterránea. El backbone del postor también deberá ser íntegramente de fibra óptica.

- Registro en sus DNS y asignación de mínimo 64 direcciones IPv4 y Ipv6 públicas de Internet que No se encuentren en Blacklist de reputación confiable, dentro de las cuales estarán el IP del router, el IP de la red y el IP del Broadcast, así como el respectivo acceso a Internet y la inscripción de los dominios en los servidores del ISP. El proveedor deberá proveer de una aplicación o plataforma web que permita administrar los registros DNS de los dominios y subdominios que el Gobierno Regional Piura administra. En casa el proveedor no permita administrar los registros DNS a través de una aplicación o plataforma web deberá garantizar una atención a las solicitudes de modificación o registro de dominio en un tiempo no mayor a 4 horas, y se deberá de ver reflejado en los DNS Raíz o de primer Nivel, como máximo en un plazo de 6 horas desde realizado los cambios en la herramienta o generado el ticket de atención por el proveedor en ambos casos. Dichas solicitudes deberán ingresar dentro del horario de trabajo de la entidad (8x5) y la programación de ejecución estará en base a lo requerido en dicha solicitud.
- También podrá aceptarse la atención de requerimientos del DNS vía NOC del proveedor

- Se podrán utilizar ips de diferente segmento para poder llegar al número de ips publicas solicitadas.

- El proveedor informará sobre cualquier mantenimiento físico o lógico que afecte el desempeño del servicio de internet proporcionado (equipos de última milla, routers y accesorios). Para ello, elaborará cronogramas, que serán entregados o comunicados a la Oficina de Tecnologías de la Información, con 48' horas de anticipación al mantenimiento.

- El Proveedor deberá proveer un Router acorde al servicio solicitado, que permita

3

configurar NAT y otras BGP, RIP, OSPF o las que se requieran para el correcto funcionamiento de las comunicaciones de acuerdo a los estándares internacionales establecido). Las interfaces deberán ser mínimo de tecnología Gigabit y el proveedor es responsable de la operación del equipo. Los equipos serán de tecnología vigente y que estén en garantía por el postor y por la marca.

- El proveedor deberá contar con salidas redundantes 100% fibra óptica al backbone Internacional de Internet como mínimo con dos (02) operadores que le proporciones 01 enlace de 100 Gbps c/u. Uno debe ser propio y el segundo rentado a un tercero o con dos salidas internacionales al backbone internacional propias

- Ambas salidas redundantes deberán conectarse hacia su(s) proveedor(es) tipo TIER-1 en puntos de interconexión (Pool) dentro del territorio nacional y deberá asegurar que estas interconexiones tienen independencia de operación y conexión. Estas salidas podrán estar en la Ciudad de Lima, o cualquier otra parte del país. Los Proveedores TIER-1, deberán estar conectados mediante. enlaces de fibra óptica y llegar a diferentes puntos de conexión.

- El proveedor debe de considerar el equipamiento necesario hasta el puerto RJ-45 Gigabit Ethernet del Switch de la Sede Central del Gobierno Regional Piura para iniciar el servicio.

- El proveedor debe incluir todo lo necesario para la puesta en marcha de sus servicios, la Entidad brindará las facilidades, espacio y condiciones para la instalación de los equipos. Se confirma que el contratista sólo será responsable de los equipos incluidos en su propuesta y que requiera para implementar la solución solicitada

- El protocolo de comunicación será TCP/IP, deberá tener disponibilidad de protocolo de ruteo IP V4/ IP V6 y el protocolo de transporte del Backbone del proveedor deberá ser MPLS, También podrá trabajar con el protocolo Metro Ethernet. Se hace mención que la tecnología Metro Ethernet soporta protocolos de calidad de servicio y protocolos de red IPV4 e IPV6,

- El Proveedor instalará y configurará todos los equipos, dispositivos y/o componentes necesarios para la puesta en funcionamiento del servicio sin que esto implique costo adicional para La Sede Central del Gobierno Regional Piura. La Entidad brindará las facilidades técnicas para la instalación de los equipos tales como: espacio en gabinetes, puntos de energía estabilizados, puertos disponibles en sus equipos, ambiente adecuado para la instalación de equipos, entre otros.

- El proveedor deberá poseer NOC (Network Operation Center) con soporte técnico las 24 horas del día, durante todo el plazo del contrato, este NOC debe de estar ubicado en el Perú de tal forma que permita a la institución hacer inspección de las

instalaciones.

- El proveedor asegurará que el servicio de Internet deberá ser brindado las veinticuatro (24) horas del día, los siete (7) días de la semana durante todo el tiempo de duración del contrato con una disponibilidad mínima del servicio al 99.50%, equivalente a un tiempo de respuesta de 4 horas y que será medido de manera mensual. La disponibilidad se aplica sobre el servicio de internet y no sobre los enlaces de internet, en caso de caída de uno de los enlaces se debe garantizar que el otro enlace continúe activo para garantizar la disponibilidad del servicio.

- El servicio debe ser acceso total a Internet. No deberá contener filtros de ninguna clase, restricción de protocolo, puertos o aplicativos con lo cual se asegurará el funcionamiento de cualquier tipo de aplicación que se ejecute sobre el protocolo TCP/IP.

- El proveedor deberá proporcionar una herramienta vía web que permita monitorear y supervisar en línea el enlace y consumo de ancho de banda para lo cual deberá entregar un usuario y su clave de acceso respectivo, durante la fase de implementación. Así mismo deberá proveer reportes de tráfico diario, semanal y mensual, en línea almacenando una bitácora mínima de las últimas 12 semanas, si el postor cuenta con más funcionalidades deberá de especificarlo en su oferta.

- El proveedor deberá poseer servidores DNS redundantes y distribuidos geográficamente en locales distintos en diferentes departamentos del Perú. Deberá demostrar mediante un diagrama de red o topología elaborada por el postor donde se indique las direcciones o ubicaciones de los servidores DNS redundantes. Su presentación será para el perfeccionamiento del contrato.

5. DEL ENLACE DE CONTINGENCIA DEL SERVICIO DE INTERNET

- El Proveedor deberá brindar el servicio de Enlace de Contingencia en caso el Enlace Principal por algún motivo quede interrumpido, el equipamiento a colocar deberá soportar el tráfico total ya que este enlace asumirá el servicio cuando el enlace principal tenga caída de servicio.

- El ancho de banda del Enlace de Contingencia será IGUAL que el ancho de banda del enlace principal, garantizando la totalidad (1:1) del canal.

- El acceso de última milla del enlace de contingencia podrá ingresar canalizado de manera aérea o subterránea a la Institución, deberá ser un cable de fibra óptica diferente del enlace principal el cual deberá partir de un nodo de acceso diferente al del enlace principal y a través de una ruta diferente y su recorrido desde el punto de presencia del postor puede ser subterráneo y/o aéreo o una combinación de ambos.

5

- El Proveedor deberá configurar el Enlace de Contingencia con los protocolos adecuados de tal manera que ante la caída del enlace principal el mismo se levante sin intervención externa y pueda ser utilizado inmediatamente suceda un problema con el Enlace Principal. (HA).

- El Enlace de Contingencia deberá ser distinto al Enlace Principal, no podrá ser el mismo enlace físico y deberá partir desde un punto de acceso diferente.

- Cuando ocurra un problema en el Enlace Principal, será comunicado por el proveedor al Gobierno Regional Piura vía correo electrónico y/o Llamada telefónica a un número gratuito brindando por el proveedor, indicando el motivo de la interrupción del Enlace Principal. El enlace de contingencia deberá de estar operativo. dicho informe pueda ser entregado en un plazo máximo de 5 días hábiles

- El Enlace de Contingencia deberá tener el mismo direccionamiento y cantidad de IPs Públicas fijas.

- El uso de este servicio será ACTIVO - PASIVO, el proveedor deberá considerar la logística necesaria para tal caso.

5. CARACTERÍSTICAS COMPLEMENTARIAS DEL SERVICIO

- El proveedor deberá tener acceso directo al backbone internacional y el backbone de la red local del postor deberá ser redundante.

- El proveedor del servicio indicará si pertenece al NAP (Network Access Point) Perú- Se considerarán miembros del NAP Perú a los postores que cuenten con enlace propio al NAP Perú de 2x 100 Gbps mínimo, activo y 100% operativo.

- El proveedor deberá reparar o disponer de equipos necesarios de contingencia en su almacén local y/o instalados en el Data Center del Gobierno Regional según lo requiera para el remplazo en el caso de presentarse alguna falla en su equipamiento, los equipos deben ser de iguales o mejores características no necesariamente nuevos o de primer uso siempre que estén en garantía por el postor y/o por la marca, el tiempo de cambio no deberá exceder a 04 horas y aplica para la solución de manera global, es decir a todos los equipos incluidos en la solución. Esto no debe de generar costo alguno, siempre y cuando la falla no sea imputable al Gobierno Regional Piura.

- Los medios de acceso de transporte físico de última milla del proveedor deberán ser 100% Fibra Óptica, el mismo que deberá ser canalizado y/o subterráneo y/o aéreo (Para el Enlace Principal) (el Enlace de Contingencia podrá llegar Aéreo a

Subterráneo) desde el nodo más cercano del proveedor hasta los ambientes donde se instalarán los equipos para la prestación del servicio (ambientes del Gobierno Regional Piura, donde se ubicarán routers y equipos de seguridad).

- Si para la instalación del servicio de Internet es necesario realizar obras civiles, trámites de permisos municipales y otros necesarios, los costos serán asumidos por el proveedor.

- Se debe considerar el registro en sus servidores de dominio (DNS) correspondientes el dominio regionpiura.gob.pe, subdominios, registros inversos y cualquier otro dominio que requiera registrar dentro de sus competencias la Oficina de Tecnologías de la Información del Gobierno regional Piura. Cualquier modificación o nuevo registro deberá ser atendido dentro del plazo máximo de 4 horas a partir de generada la solicitud en el formato de llenado de registro de manera correcta y el proveedor confirma dicha información., y se deberá de ver reflejado en su DNS como máximo en un plazo de 6 horas desde la generación del ticket

- Siendo fundamental evaluar y mejorar la capacidad de la entidad proteger sus activos digitales de amenazas cibernéticas provenientes del presente servicio de Internet, es necesario identificar y analizar los riesgos posibles que pueden afectar las operaciones, procesos y servicios de tecnologías de la información y comunicaciones en la Sede Central del Gobierno Regional Piura

  Por lo tanto, el proveedor debe realizar la medición de la *"Postura de Ciberseguridad"* de manera presencial , el análisis de la postura de ciberseguridad se deberá realizar al menos dos (02) veces durante el plazo de contrato: el primer análisis que se deberá realizar al inicio del contrato (mes 1), el segundo análisis se deberá brindar a los 12 meses de contrato (mes 12 o 13) .Con ello, se podrá revisar el estado general de la ciberseguridad, focalizándose en el proceso y tecnologías implementadas para detectar y gestionar incidentes para entornos empresariales, responder ante ellos y recuperarse, debiendo establecer la metodología y criterios de medición en los niveles de implementación según estándares como ISO 27001, NIST Cybersecurity Framework, GDPR. Para tal fin el profesional que realizará dicha actividad deberá ser por (01) especialista en seguridad de la Información.

6. ATENCIÓN DE AVERÍAS O FALLAS

- Se entenderá por avería a una interrupción parcial o total del servicio, así como a un decremento en la calidad del mismo, para lo cual el postor deberá aceptar el ticket de reclamo y tomar acción para corregir la afectación parcial o total del servicio, cuyo plazo de atención será 04 horas para avería total del servicio, y en caso de afectación parcial por degradación de servicio el tiempo de subsanación no se computará para el SLA. En caso de avería por rotura de fibra óptica por causas no imputables al

contratista y que no afecten al servicio (solo uno de los enlaces) se considerará un tiempo adicional de hasta 8 horas para la subsanación de la avería del enlace afectado.

- Toda actividad o provisión de bienes que tenga que ejecutar el proveedor para subsanar la avería serán sin costo alguno para La Sede Central del gobierno Regional de Piura, salvo el caso en que la avería sea imputable al Gobierno Regional Piura.

- Se entenderá por Tiempo de Atención at tiempo transcurrido desde que el Gobierno Regional Piura comunica la avería al Centro de Gestión del Postor hasta que este le genera el ticket de atención, este tiempo no deberá exceder de 01 hora. Se entenderá por Tiempo de Subsanación al tiempo transcurrido desde generado el ticket por el centro de gestión del postor hasta la subsanación de la avería (este tiempo no deberá exceder de 4 horas). En caso de avería por rotura de fibra óptica o avería de equipo por causas no imputables al contratista y que no afecten al servicio (solo uno de los enlaces) se considerará un tiempo de hasta 8 horas adicionales para la subsanación de la avería del enlace o equipo afectado, debiendo sustentar en el informe que la avería no fue atribuida al contratista.

- La Sede Central del Gobierno Regional Piura solamente reportará a un único número telefónico el cual será una ventanilla única que atenderá todas las averías del servicio contratado, permitiendo un adecuado control, gestión y seguimiento de la misma, debiendo indicar número telefónico. El proveedor del servicio deberá contar con un número 0800 gratuito para la atención de las llamadas. Y deberá ser proporcionado al Perfeccionamiento del Contrato.

- La Sede Central del Gobierno Regional Piura podrá efectuar llamadas de servicio de lunes a domingo incluyendo feriados desde las 00:00 hasta las 24:00 horas. El Proveedor deberá contar con un centro de atención de llamadas de reparación o asistencia técnica instalado de tal manera que le asegure al Gobierno Regional Piura que se encuentra en condiciones de cumplir con lo estipulado en las bases.

- El proveedor adjudicado deberá entregar al Gobierno Regional Piura culminada la fase de implementación una relación de las personas de contacto responsables de la Gestión de servicio; además del nivel de escalamiento.

7. DE LA SEGURIDAD PERIMETRAL GESTIONADA

El proveedor deberá incluir en la solución de seguridad perimetral gestionada, para lo cual deberá instalar dos equipos appliance de seguridad en HA en formato rack, con las funciones de Firewall Perimetral, IPS, Protección y Control Web, Protección y Control de Aplicaciones, funcionalidades de enrutamiento WAN/LAN y VPNs.

El equipamiento deberá de tener vigencia tecnológica (es decir que no estén anunciados como EoS o EoL al momento de la presentación de la oferta), soporte y garantía de fabrica vigentes durante la ejecución del contrato. Dicho equipamiento se deberá de registrar a nombre del Gobierno Regional Piura con la finalidad de que la Institución pueda renovar a futuro las actualizaciones, licencias y todo lo concerniente al mismo. A la culminación del contrato, dicho registro como opcional.
El proveedor es el responsable de la gestión de garantías en caso de averías del hardware, así como de la solicitud de ampliación de licencias y demás

las soluciones de seguridad perimetral gestionada, solución de protección de próxima generación XDR para estaciones de trabajo y servidores y protección de correo electrónico deben permitir la orquestación de dispositivos desde una misma consola de forma automatizada sin necesidad de salir a cada dispositivo individualmente.

Las soluciones de seguridad perimetral gestionada, solución de protección de próxima generación XDR para estaciones de trabajo y servidores deben permitir hablar entre si y permitir interacción mutua entre anti virus y equipos de protección perimetral a fin de poder tener información detallada entre el borde y el usuario final.
las soluciones de seguridad perimetral gestionada, solución de protección de próxima generación XDR para estaciones de trabajo y servidores deben permitir el paso de información e IOC del antivirus y cualquier tipo de protección de seguridad de terceros para nutrir la inteligencia de toma de acciones del firewall.

7.1 Características Generales Mínimas:

- El dispositivo debe tener acceso directo por el plazo de las licencias (por el plazo de duración del contrato), en forma ilimitada a la base de datos del fabricante para todas las actualizaciones de Firmware de los equipos.
- El equipo debe contar con el RMA de Fabrica, que en caso deba utilizarse el proveedor se encarga de realizar las gestiones respectivas hasta la llegada del equipo de remplazo.
- El proveedor deberá contar con un SOC (Security Operation Center) (propio o tercerizado), para el servicio de Soporte Técnico en 7x24 para lo cual debe contar con un procedimiento de atención para que La Sede Central del Gobierno Regional Piura pueda solicitar las atenciones que requiera en forma ilimitada las 24 horas del día y sin costos adicionales, este SOC debe de estar ubicado en el Perú de tal forma permita a la institución hacer inspección de las instalaciones.

- El proveedor debe encargarse en forma conjunta con el personal de la Oficina de Tecnologías de la Información, de todos los cambios de reglas y/o configuraciones que La Sede Central del Gobierno Regional Piura desee hacer en forma ilimitada, sin restricción de cantidad de solicitudes y sin costos adicionales. Además, se permitirá un mayor de acceso a los equipos appliance de seguridad a nivel de

escritura, con la finalidad de activar/desactivar features, interfaces, rutas internas, externas, configuración de los mensajes de alerta a los usuarios ante un acceso indebido, todo lo anterior de manera coordinada con el SOC.

- Cualquier cambio o configuración realizado por la Entidad, y que esto afecte circunstancialmente el servicio será de responsabilidad de la Entidad. En caso, de requerir el apoyo al contratista, para la subsanación de dichos efectos, la Entidad podrá asumir los gastos que ello implique, previa evaluación y determinación de responsabilidades

- El proveedor deberá realizar backup de la información cuando haya existido cambios en las configuraciones en el equipo durante el plazo del contrato.

- El proveedor se debe encargar de hacer todas las actualizaciones de Firmware y de Sistema operativo del dispositivo o dispositivos de seguridad por el plazo del contrato y sin costos adicionales.

- Si el/los equipos appliance de seguridad instalados fallan, el postor los debe cambiar por otro de iguales o superiores especificaciones a las requeridas en un plazo no mayor a 4 horas de detectado el hecho por el SOC del proveedor, lo cual está plenamente respaldado en los almacenes del postor o con el equipo raqueado en la sala de Servidores del Gobierno Regional Piura (de ser el caso).

- Debido a que la solución está orientada a incorporar equipos en Alta Disponibilidad (HA), solo en el caso de que uno de los equipos fallara, el tiempo de subsanación podrá ser según el RMA del fabricante toda vez que el servicio se mantenga activo mediante el equipo de contingencia. Cuando sea una avería total (caída de ambos equipos), el tiempo de subsanación será de 24 horas.

7.2 Características Específicas Mínimas de Appliance de Seguridad:

a) **Características del hardware**

- El postor deberá ofrecer una solución en Alta Disponibilidad.
- Deberá contar con arquitectura de Doble Procesador: Tecnología de procesamiento multinúcleo - x86 AMD CPU & Xstream Flow Processor (Marvell NPU)
- Almacenamiento Local: 240 GB
- Puertos Ethernet Incluidos:
  - 4 x GbE copper
  - 4 x 2.5 GbE copper
  - 4 x SFP+ 10 GbE fiber*
- Deberá contar con 2 puertos x USB 3.0
- Deberá contar con 2 Slots de Expansión
- Deberá contar con pantalla módulo LCD multifunción
- Fuente de alimentación: Internal auto-ranging AC-DC 100-240VAC, 3.7-7.4A@50-60 Hz
- Deberá contar con certificaciones de producto: CB, CE, UKCA, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, TEC, SDPPI

10

b) **Rendimiento del equipo de seguridad**

- Firewall Throughput: 75,000 Mbps
- Firewall IMIX: 33,000 Mbps
- IPS throughput: 29,500 Mbps
- Threat Protection throughput: 6,500 Mbps
- NGFW: 23,000 Mbps
- IPsec VPN throughput: 62,500 Mbps
- IPsec VPN Concurrent tunnels: 8,500
- SSL VPN Concurrent tunnels: 7,500
- Conexiones simultáneas: 16,600,000
- Nuevas conexiones/seg: 368,000
- SSL/TLS Inspection throughput: 8,000 Mbps

c) **Características de administración**

- Deberá contar con Interfaz de usuario optimizada y especialmente diseñada y administración de reglas de firewall para grandes conjuntos de reglas con agrupación con características de reglas de un vistazo e indicadores de aplicación
- Compatibilidad con autenticación de dos factores (contraseña de un solo uso) para acceso de administrador, portal de usuario, IPSec y SSL VPN
- Deberá contar con un Sistema de menú de autodocumentación / Ayuda
- Deberá contar con Herramientas avanzadas de resolución de problemas / Troubleshooting en GUI (por ejemplo, captura de paquetes)
- Deberá contar con Interfaz de línea de comandos (CLI) completa accesible desde GUI
- Deberá contar con Administración basada en roles
- Deberá contar con Notificación de actualización de firmware automatizada con un proceso de actualización automatizado sencillo y funciones de reversión.
- Definición de objetos reutilizables para redes, servicios, hosts, periodos de tiempo, usuarios y grupos, clientes y servidores.
- Portal de autoservicio
- Deberá poder realizar seguimiento de cambios de configuración
- Deberá poder realizar control flexible de acceso a dispositivos para servicios por zonas
- Deberá tener opciones de notificación de captura snmp o correo electrónico
- Deberá contar con soporte SNMP v3 y Netflow
- Deberá contar con soporte de administración central a través de la consola unificada basada en la nube
- Notificaciones automáticas por correo electrónico para cualquier evento importante
- Configuraciones de backup y restauración: localmente, a través de FTP, correo electrónico, desde la plataforma de administración Cloud; bajo demanda, diariamente, semanalmente o mensualmente
- Mejoras en el proceso de restauración de copias de Seguridad

11

- API para la integración con terceros
- Deberá contar con guias de administración en video integradas en Links en el FW
- Opción de acceso remoto al firewall de manera nativa del fabricante
- Soporte técnico de Syslog
- La consola de adminisitración Cloud debe tener capacidades de agrupar FWs, generar Backups y hacer deployments zero touch
- Desde la consola de administración cloud se debe poder generar reportes centralizados.
- La gestión de políticas de grupo permite que los objetos, la configuración y las políticas se modifiquen una vez y se sincronicen automáticamente en todos los Firewalls que pertenecen al mismo grupo.
- Contar con un Administrador de tareas proporciona una pista de auditoría histórica completa y una supervisión del estado de los cambios en las políticas de grupo
- La gestión de copias de seguridad de firmware desde la consola en nube debe tener la opción de almacenar los últimos cinco archivos de copia de seguridad de configuración de cada Firewall registrado con uno que se puede anclar para un almacenamiento permanente y un acceso sencillo.
- La programación de actualizaciones de firmware desde la consola en nube debe permitir aplicar fácilmente actualizaciones automatizadas en cualquier momento
- Gestión de firewalls de grupo a través del Partner Dashboard
- Informes de varios firewalls a través de grupos de firewalls

d) **Caracteristicas de Firewall, Networking y Routing**

- Deberá realizar inspección profunda de paquetes (Stateful deep Packet)
- Deberá contar con un modelo de políticas unificada que permite gestionar las directivas en una sola pantalla
- Deberá contar con una arquitectura de procesamiento de paquetes con niveles extremos de visibilidad, protección y rendimiento mediante el procesamiento de paquetes basado en flujos
- Deberá contar con una herramienta de simulador de pruebas de politicas para habilitar la regla de firewall y la web, simulación de políticas y pruebas por usuario, IP y hora del día.
- Deberá soportar TLS 1.3 sin degradación, puertos independientes, políticas de nivel empresarial, visibilidad única del panel y solución de problemas de compatibilidad.
- Deberá contar con un motor DPI que proporcione protección de escaneado de flujo para IPS, AV, Web, App Control e inspección TLS en un único motor de alto rendimiento.
- Deberá acelerar el tráfico SaaS, SD-WAN y en la nube, como VoIP, video y otras aplicaciones confiables a través de FastPath (Aceleración de tráfico)
- Deberá contar con aceleración inteligente y basada en políticas del tráfico de confianza
- Deberá ofrecer aceleración del tráfico cifrado TLS
- Deberá poder configurar políticas basadas en usuarios, grupos, tiempos o redes
- Deberá soportar políticas de acceso delimitadas por tiempo por usuario/grupo
- Deberá poder habilitar políticas por zonas, redes o por tipo de servicio
- Deberá poder realizar aislamiento de zonas y soporte de políticas basadas en zonas
- Deberá poder configurar zonas predeterminadas para LAN, WAN, DMZ, LOCAL, VPN y WiFi

- Deberá poder configurar Zonas personalizadas para LAN o DMZ
- Deberá poder configurar políticas NAT personalizables con enmascaramiento de IP
- Soporte completo de objetos para redirigir o reenviar múltiples servicios en una sola regla con un conveniente asistente de reglas NAT para crear rápida y fácilmente reglas NAT complejas con solo unos pocos clics
- Soporte completo de VLAN
- Nat de origen
- Nat de destino
- Renombrar Interfaces
- Protección contra inundaciones: DoS, DDoS y portscan blocking
- Bloqueo por geo-IP
- Deberá soportar enrutamiento avanzado: estático, multidifusión (PIM-SM) y dinámico (RIP, BGP, OSPF, OSPF v3) con soporte completo de VLAN 802.1Q y multicast (PIM-SM y IGMP)
- Deberá soportar enrutamiento de multidifusión independiente del protocolo con snooping IGMP
- Soporte de Bridging con STP y ARP broadcast forwarding
- Deberá soportar balanceo de enlaces WAN: Multiples conexiones a Internet, auto-link health check, failover automático, balanceo automático y por peso, reglas granulares multipath
- Compatibilidad con WAN inalámbrica
- Soporte de link aggregation 802.3ad
- Configuración completa de DNS, DHCP y NTP
- DNS dinámico (DDNS)
- Enrutamiento multicast independiente de protocolo con IGMP Snooping
- Compatibilidad con IPv6 con soporte de tunelización 6in4, 6to4, 4in6 e implementación rápida de IPv6 (6rd) a través de IPSec de acuerdo con el RFC 5969
- Soportar IPv6 DHCP Prefix Delegation
- Soportar BGPv6
- Compatibilidad con Wilcards para objetos host de nombre de dominio
- Soporte y etiquetado DHCP VLAN
- Soporte de Multiple bridge
- Soportar Inspección SSL sin comprometer el rendimiento de la red o la experiencia del usuario. Ofrecer soporte de alto rendimiento y alta capacidad para TLS 1.3 y todos los conjuntos de cifrados modernos que proporcionan un rendimiento de inspección SSL extremo en todos los puertos, protocolos y aplicaciones.

e) **Características de SD-WAN**

- Debe tener tecnología de conectividad SD-WAN
- Integración de SD-WAN de terceros con redes troncales de Cloudflare, Akamai y Azure
- La funcionalidad SD-WAN debe ser compatible con la conectividad a Secure SD-WAN que se ofrece en el servicio Microsoft Azure Virtual WAN
- Debe admitir perfiles SD-WAN para balancear la carga de las conexiones entre interfaces
- Debe tener métodos de Balanceo: round-robin y persistencia de sesiones con las siguientes opciones:
    - Por conexión
    - IP de Origen

13

- IP de destino
- IP de Origen y Destino

Los enlaces se pueden ponderar para determinar cómo se distribuye el tráfico entre ellos, y el SLA se puede usar para seleccionar qué enlaces serán incluidos para balancear carga.

- Debe soportar la configuración de nivel de calidad (SLA) mínimo (latencia, jitter y pérdida de paquetes) para que SDWAN elija un enlace determinado.
- Debe soportar el uso de al menos 4 (cuatro) enlaces de Internet / MPLS
- Soporte para múltiples opciones de enlace WAN, incluyendo VDSL, DSL, cable y celular 3G / 4G / LTE con monitoreo esencial, balanceo, conmutación por error
- Los perfiles SD-WAN admiten varias opciones de enlace WAN, como VDSL, DSL, cable, LTE/celular y MPLS.
- Debe soportar el uso de enlaces de interfaz física, subinterfaces VLAN lógicas y túneles IPSec
- Debe generar un Log de eventos que registre los cambios en el estado de los enlaces SD-WAN, monitoreados por el estado de salud de los enlaces
- La solución debe ser capaz de medir el estado de salud del enlace en base a criterios mínimos de: Latencia, Jitter y Pérdida de Paquetes, donde es posible configurar un valor Theshold para cada uno de estos ítems, el cual será utilizado como factor de decisión en las reglas SD-WAN
- La solución SD-WAN debe poder presentar gráficamente todos los datos de análisis del estado del enlace, que contenga gráficos que presenten al menos los criterios descritos anteriormente.
- Los gráficos deben presentarse en tiempo real y permitir una visualización histórica de al menos 24 horas, 48 horas, 1 semana y 1 mes
- La verificación del estado de salud debe admitir el marcado de paquetes con DSCP, para una evaluación más precisa de los enlaces que tienen QoS configurado
- La solución debe tener funcionalidad para crear la malla SD-WAN en varios firewalls en un solo concentrador
- Esta funcionalidad debería facilitar la configuración SD-WAN de múltiples firewalls, creando automáticamente toda la información necesaria para que SD-WAN suceda, como al menos, pero no limitado a: creación de rutas, reglas de firewall, objetos y túneles VPN necesarios.
- La misma consola del concentrador SD-WAN debe monitorear los enlaces de cada dispositivo implementado, lo que garantiza una vista única de todos los dispositivos implementados.
- Selección y enrutamiento de rutas de aplicaciones, que se utiliza para garantizar la calidad y minimizar la latencia para aplicaciones de misión crítica como VoIP
- SD-WAN sincronizada, una función de seguridad sincronizada que aprovecha la claridad y confiabilidad adicionales de la identificación de aplicaciones que viene con el intercambio de información de control de aplicaciones sincronizadas entre los puntos finales administrados y el firewall
- Enrutamiento sincronizado de aplicaciones SD-WAN a través de enlaces preferidos a través de reglas de firewall o enrutamiento basado en políticas
- Soporte VPN robusto que incluye IPSec y SSL VPN
- Orquestación VPN centralizada.
- El fabricante debe proveer una terminal que no contenga todas las capacidades del FW de nueva generación y que sea mucho más económica para levantar VPNs con

oficinas remotas de pocos usuarios que no necesiten tener un FW dedicado
- Gestión Central de todos los dispositivos RED
- Zero Trust: se conecta automáticamente a través de un servicio de aprovisionamiento basado en la nube
- Túnel cifrado seguro con certificados digitales X.509 y cifrado AES256-
- Interfaz Ethernet virtual para una transferencia fiable de todo el tráfico entre ubicaciones
- Administración de direcciones IP con configuración de servidor DHCP y DNS definida de forma centralizada
- Desautorizar remotamente los dispositivos después de un período selecto de inactividad
- Compresión del tráfico del túnel
- Opciones de configuración del puerto VLAN.

f) **Opciones VPN**

- La solución de Firewall deberá permitir crear túneles VPN IPSec y SSL, debe permitir una cantidad limitada de túneles VPN (IPSec VPN Concurrent Tunnels mínimo de 8000 y para SSL VPN Concurrent Tunnels mínimo de 7000.
- Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
- La VPN IPsec debe admitir: Autenticación DES, 3DES, GCM, Suite-B, MD5 y SHA-1, Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14; algoritmo de intercambio de claves de Internet (IKE); AES 128, 192 y 256 (Estándar de cifrado avanzado); SHA 256, 384 y 512; Autenticación mediante certificado PKI (X.509) y clave precompartida (PSK).
- L2TP y PPTP
- Deberá permitir las VPN basada en rutas
- Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Andriod VPN client
- Deberá brindar soporte al protocolo IKEv2 que se utiliza para negociar una asociación de seguridad al principio de una sesión
- La solución deberá permitir la aplicación de TLS 1.2 para túneles VPN de acceso remoto y sitio a sitio SSL
- Debe tener opción IPSEC VPN con cliente nativo del fabricante
- Cliente SSL para Windows & descarga de configuración a través del portal de usuarios
- Debe contar con un portal encriptado basado en HTML5 para soportar al menos: RDP, SSH, Telnet y VNC, sin necesidad de instalar clientes VPN en las estaciones de acceso
- Debe permitir la creación de políticas de control de aplicaciones, IPS, Antivirus, Anti-Malware y filtrado de URL para el tráfico de clientes remotos conectados a la VPN SSL.
- Debe soportar de forma nativa la integración con Amazon para establecer un túnel seguro entre los dispositivos y AWS VPN
- Permita establecer un túnel VPN SSL con una solución de autenticación a través de LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ y a través de una base de datos local.
- Autenticación: Pre-Shared Key (PSK), PKI (X.509), Smartcards, Token y XAUTH
- Cifrado: AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (up to 2048 Bit), Grupos DH 1/2/5/14, MD5 y SHA-256/384/512

56

15

- Soportar autentición via AD/LDAP, Token y base datos de usuários locales
- Split-tunneling inteligente para un enrutamiento de tráfico óptimo
- Soporte de NAT-transversal
- Monitor de cliente para una visión general gráfica del estado de la conexión
- Multilenguaje

g) Características de Autenticación

- Debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién usa qué aplicaciones a través de la integración con los servicios de directorio, la autenticación a través de LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ y a través de la base de datos local, para la identificación de usuarios y grupos que permiten granularidad de control/políticas basadas en usuarios y grupos de usuarios
- Debe soportar la identificación de múltiples usuarios conectados a la misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que se encuentran en estos servicios
- Debe permitir la autenticación en los modos: transparente, autenticación proxy (explícita, NTLM y Kerberos) y autenticación vía clientes en estaciones de trabajo con sistemas operativos Windows, macOS y Linux 32/64
- Al usar la opción de proxy explícito, se debe permitir la autenticación para cada conexión, a fin de garantizar que el Firewall identifique correctamente a los usuarios que iniciaron sesión en servidores multisesión, incluso cuando se usa solo 1 IP de origen
- Debe ser compatible con la configuración de inicio de sesión único para que los administradores inicien sesión en la consola web mediante Azure AD
- Debe tener autenticación de inicio de sesión único para al menos Active Directory, Azure AD y sistemas de directorio de eDirectory
- Autenticación vía: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
- Agentes de autenticación de servidor para SSO, STAS, SATC de Active Directory
- Tiempo de espera de radio con autenticación de dos factores (2FA)
- Agentes de autenticación de cliente para Windows, Mac OS X, Linux 32/64
- Certificados de autenticación para iOS y Android
- Single sign-on: Active directory, eDirectory
- Servicios de autenticación para IPSec, L2TP, PPTP, SSL
- Compatibilidad con la creación de usuarios con formato UPN para la autenticación RADIUS
- Debe permitir el control, sin necesidad de instalar un software cliente, de los dispositivos que soliciten salida a internet para que antes de iniciar la navegación se amplíe un portal de autenticación residente en el firewall (Portal Cautivo).

h) Características de Protección de red

- Motor de inspección profunda de paquetes IPS de próxima generación y alto rendimiento con patrones IPS selectivos que se pueden aplicar sobre la base de reglas de firewall para obtener el máximo rendimiento y protección
- Debe realizar una inspección profunda de paquetes para la prevención de intrusiones (IPS) y debe incluir firmas de prevención de intrusiones

16

- Las firmas de prevención de intrusiones (IPS) deben poder personalizarse
- Protección avanzada contra amenazas (Detectar y bloquear el tráfico de red con servidores de comando y control mediante DNS multicapa, AFC y firewall)
- Visibilidad instantánea sobre el estado de amenaza de los endpoints, con la opción de responder automáticamente a los incidentes de seguridad mediante el aislamiento de los sistemas infectados tanto para tráfico en el mismo dominio de broadcast como para otros segmentos de red sin que haya ningún tipo de intervención o cambios realizados por el administrador
- Proporcionar visibilidad de los usuarios de mayor riesgo, aplicaciones desconocidas, amenazas avanzadas y payloads sospechosos
- Los filtros inteligentes de directiva IPS habilitan directivas dinámicas que se actualizan automáticamente a medida que se agregan nuevos patrones
- Solicitar información de aplicaciones al Endpoint para el tráfico que no coincida con ninguna firma de control de aplicaciones.
- Capacidades forenses y de análisis profundas en usuarios, amenazas, aplicaciones, uso web y otras actividades en la red.
- Limitar el acceso a los recursos de red o aislar completamente los sistemas comprometidos hasta que se mitigue completamente el riesgo o se elimine la amenaza
- Tener la capacidad de compartir telemetría y el estado de salud entre el Endpoint Intercept X y el firewall para proporcionar una respuesta automática y adaptativa ente una amenaza de seguridad.

i) **Características de Protección de Web**

- Proxy totalmente transparente para antimalware y filtrado web
- Protección avanzada mejorada contra amenazas
- Debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién usa qué URL a través de la integración con servicios de directorio, autenticación a través de LDAP, Active Directory, Azure AD, Radius, E-directory y base de datos local.
- Permitir llenar todos los registros de URL con información de usuario como se describe en Integración de servicios de directorio
- La solución deberá proveer una base de datos de filtrado de URL con millones de sitios en 92 categorías respaldados por OEMLabs
- Debe poder categorizar URL desde la base o caché de URL locales o mediante consultas dinámicas en la nube del fabricante, independientemente del método de clasificación, la categorización no debe causar demoras en la comunicación visibles para el usuario.
- Debe soportar la creación de categorías de URL personalizadas
- Políticas de tiempo de cuota de navegación por usuario/grupo
- Políticas de acceso por tiempo para usuario/grupo
- Debe tener la capacidad para que algunos usuarios seleccionados previamente eludan temporalmente la política de bloqueo actual
- Análisis de malware: bloquee todas las formas de virus, malware web, troyanos y spyware en HTTP/S, FTP y correo electrónico basado en la web
- Protección avanzada contra malware web con emulación JavaScript
- Live Protection búsquedas en tiempo real en la nube para la última inteligencia de amenazas
- Segundo motor de detección de malware independiente para el doble análisis

54

17

- Escaneo en tiempo real o en modo por lotes
- Protección de Pharming
- Análisis HTTP y HTTPS por usuario o política de red con reglas y excepciones personalizables
- Detección y enforcement de túneles SSL
- Supervisión y aplicación de palabras claves en navegación para bloquear o permitir sitios que contengan dicho contenido.
- Validación de certificados
- Almacenamiento en caché de contenido web de alto rendimiento
- Filtrado de tipos de archivo por tipo de mimo, extensión y tipos de contenido activo (por ejemplo, Activex, applets, cookies, etc.)
- Soporte de SafeSearch (basada en DNS) para los principales motores de búsqueda por política (usuario/grupo)
- Monitoreo y aplicación de palabras clave web para registrar, informar o bloquear palabras clave coincidentes con contenido web listas con la opción de subir listas de aduanas
- Bloquear aplicaciones potencialmente no deseadas (PUAs)
- Debe permitir especificar la política de navegación Web por tiempo, es decir, definir reglas para un día de la semana determinado y hora de inicio y fin, permitiendo agregar múltiples días y horas en una misma definición de política por tiempo. Esta regla de tiempo puede ser recurrente o única.
- Opción de anulación de directivas web para que los profesores o el personal permitan temporalmente el acceso a sitios o categorías bloqueados que son totalmente personalizables y administrables por usuarios seleccionados
- Aplicación de políticas de usuario/grupo en Google Chromebooks
- Filtrado web automático de sitios identificados por Internet Watch Foundation (IWF) que contienen abuso sexual infantil

j) **Características de Protección y control de aplicaciones**

- Control mejorado de aplicaciones con firmas y patrones de Capa 7 para miles de aplicaciones
- Los dispositivos de protección de red deben tener la capacidad de reconocer aplicaciones por firmas y capa 7, utilizando puertos estándar (80 y 443), puertos no estándar, salto de puerto y tunelización a través de tráfico SSL encriptado.
- Debe ser posible inspeccionar paquetes cifrados con algoritmos SSL 2.0, SSL 3.0, TLS 1.2 y TLS 1.3
- El motor de análisis de tráfico cifrado debe reconocer, entre otros, al menos los siguientes algoritmos: curvas elípticas (ECDH, ECDHE, ECDSA), DH, DHE, Autenticación, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camelia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384
- El motor de inspección de paquetes cifrados debe ser configurable y permitir definir acciones como no descifrar, denegar el paquete y cifrar para determinadas conexiones cifradas
- Reconocer al menos 2300 aplicaciones diferentes clasificadas por nivel de riesgo, características y tecnología, incluido, entre otros, el tráfico relacionado con peer-to-peer, redes sociales, acceso remoto, actualización de software, servicios de red, VoIP, transmisión de medios, proxy y tunelización. mensajería instantánea, uso compartido de archivos, correo electrónico web y actualizaciones de software

53

18

- Reconocer al menos las siguientes aplicaciones: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, base de datos Oracle, descarga de archivos RAR, Redtube Streaming, RPC sobre HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing and File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer y WhatsApp Web
- Debe escanear y controlar la microaplicación que incluye, entre otros: Facebook (aplicaciones, chat, comentarios, eventos, juegos, complemento Me gusta, mensaje, descarga y carga de fotos, complemento, adjunto de publicación, publicación, preguntas, actualización de estado, chat de video, video reproducción, carga de video, sitio web), Freegate Proxy, Gmail (aplicación de Android, archivo adjunto), Google Drive (base, descarga de archivos, carga de archivos), aplicación de Google Earth, Google Plus, LinkedIN (búsqueda de empresa, redacción de correo web, búsqueda de empleo, correo Bandeja de entrada, actualización de estado), carga y descarga de archivos de SkyDrive, Twitter (mensaje, actualización de estado, carga, sitio web), Yahoo (correo web, archivo adjunto de correo web) y Youtube (búsqueda de video, transmisión de video, carga, sitio web)
- Para el tráfico cifrado SSL, debe descifrar los paquetes para poder leer la carga útil para verificar las firmas de las aplicaciones conocidas por el fabricante.
- Reconocimiento de Aplicaciones en IPv6
- Control de aplicaciones basado en categorías, características (por ejemplo, consumo de ancho de banda y productividad), tecnología (por ejemplo, P2P) y nivel de riesgo
- El medidor de riesgo de aplicaciones proporciona un factor de riesgo general basado en el nivel de riesgo de las aplicaciones de la red
- Identificar, clasificar y controlar aplicaciones previamente desconocidas activas en la red a través de integración Nativa con solución de Endpoint
- Identificar, clasificar y controlar automáticamente todas las aplicaciones en la red incluyendo las desconocidas o para las que no se tengan firmas a través de integración nativa con solución de XDR garantizando la identificación y control del 100% de las aplicaciones que generan tráfico dentro de la organización
- Debe permitir el uso individual de diferentes aplicaciones para usuarios pertenecientes a un mismo grupo de usuarios, sin necesidad de cambiar de grupo o crear uno nuevo. Otros usuarios de este mismo grupo que no tengan acceso a estas aplicaciones deberán tener bloqueado su uso
- Aplicación de directivas de control de aplicaciones por usuario o regla de red

k) Características de Protección de Sandboxing

- El appliance de seguridad ofertado debe poder habilitar el servicio de Sandboxing en la nube para análisis y detonación de malware potencial
- Inspeccionar ejecutables y documentos que contengan contenido ejecutable
- Inspecciona ejecutables y documentos que contienen contenido ejecutable (incluidos .exe, .com y .dll, .doc, .docx, docm y .rtf y PDF) y archivos que contienen cualquiera de los tipos de archivo enumerados anteriormente (incluidos ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)

- Inspeccionar documentos de Word (incluyendo .doc, .docx, docm and .rtf)
- Detonar PDF
- Informes de archivos maliciosos en profundidad y capacidad de liberación de archivos de panel
- El sanbox debe realizar analisis dinamico de comportamiento de malware y deep learning
- Analisis en menos de 120 segundos
- Reportes detallados conteniendo inteligencia de amenaza: Composición del archivo, patrones de ejecución, similitud con otros códigos, etc.

l) Protección Web Application Firewall

- Proxy Reverso
- Motor de endurecimiento de URL con enlace profundo y prevención de recorrido de directorios
- Motor de endurecimiento de formularios
- Protección contra la inyección SQL
- Protección contra Cross-site scripting
- Debe contar con un motor de antivirus Dual, tener dos diferentes fuentes de definiciones
- Offloading cifrado HTTPS (SSL)
- Firma de cookies con firmas digitales
- Enrutamiento Path-based
- Soporte de Outlook anywhere
- Autenticación inversa (descarga) para la autenticación básica y basada en formularios para el acceso al servidor
- Abstracción de servidores virtuales y servidores físicos
- Balanceador de carga integrado para distribuir a los visitantes entre varios servidores
- Omita los cheques individuales de manera granular según sea necesario
- Coincidir con las solicitudes de las redes de origen o las direcciones URL de destino especificadas
- Soporte para operadores lógicos y/o
- Ayudar a la compatibilidad con varias configuraciones e implementaciones no estándar
- Opciones para cambiar los parámetros de rendimiento de WAF
- Opción de límite de tamaño de escaneo
- Permitir/Bloquear rangos IP
- Soporte de Wildcards para paths de servidores
- Anexar automáticamente un prefijo/sufijo para la autenticación.

m) Caracteristicas de loggin y reportería

- Cientos de informes integrados con opciones de informe personalizados y flexibles
- Dashboards de tráfico, Seguridad y Amenazas de Usuario
- Informe de aplicaciones (riesgo de aplicaciones, aplicaciones bloqueadas, usos web, motores de búsqueda, servidores web, FTP),

- Informe de Amenazas de Red (IPS, ATP, Wireless, Respuesta a incidentes),
- Reportes de VPN
- Reportes de protección y uso de Correo Electrónico
- Informes de cumplimiento (HIPAA, GLBA, SOX, FISMA, PCI-DSS, NERC CIP v3 y CIPA)
- Supervisión de actividad actual: estado del sistema, usuarios activos, conexiones IPsec, usuarios remotos, conexiones en vivo, clientes inalámbricos, cuarentena y ataques DoS
- Reportar anonimización
- Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles
- Opciones de registro estándar y granular
- Exportar informes como HTML, PDF, Excel (XLS)
- Informe de auditoría de seguridad
- Informe de contenido de palabras clave web
- Almacenamiento en la nube de 7 días para informes de Central Firewall
- Reportar marcadores
- Visor de registro completo con personalización de retención por categoría.
- Informes agregados de múltiples firewalls
- Guardar plantillas de informe personalizadas
- Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles
- Exportar informes en formato PDF, CFV o HTML
- Posibilidad de tener desde 30 días hasta 1 año de almacenamiento de datos por firewall en la consola Centralizada - Sophos Central
- Contar con el conector XDR/MDR
- Búsqueda y visualización de Syslog
- Informes bajo demanda en Sophos Central.
- Cientos de informes en la caja con opciones de informes personalizados: paneles (tráfico, seguridad y cociente de amenazas del usuario), aplicaciones (riesgo de aplicaciones, aplicaciones bloqueadas, aplicaciones sincronizadas, motores de búsqueda, servidores web, coincidencia de palabras clave web, FTP), redes y amenazas (IPS, ATP, inalámbrico, security heartbeat, sandstorm), VPN, correo electrónico, cumplimiento (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)
- Almacenamiento integrado en la serie XGS para un almacenamiento ilimitado de datos de registro para informes históricos
- Monitoreo de actividad actual: estado del sistema, usuarios en vivo, conexiones IPSec, usuarios remotos, conexiones en vivo, clientes inalámbricos, cuarentena y ataques DoS
- Anonimización de informes
- Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles.
- Exportar informes como HTML, PDF, Excel (XLS)
- Personalización de la retención de registros por categoría
- Soporte de Syslog
- Visor de registros en vivo con todas las funciones con vista de columna y vista detallada con potentes opciones de filtro y búsqueda, ID de regla con hipervínculos y personalización de la vista de datos.

50

21

8. SOLUCIÓN DE PROTECCION DE PROXIMA GENERACION XDR PARA ESTACIONES DE TRABAJO Y SERVIDORES

La institución con la finalidad de mejorar la postura de seguridad a nivel de Endpoint, usuario final y servidores requiere contar con una solución de próxima generación XDR para un total de 1150 dispositivos distribuidos en 1100 estaciones y 50 Servidores por 36 meses, dicho despliegue deberá ser realizado por el proveedor, Así mismo la solución debe cumplir con las siguientes características:

8.1 CONSOLA DE ADMINISTRACION

- Todos los componentes que forman parte de la solución, de seguridad para servidores, estaciones de trabajo deben ser suministrados por un solo fabricante. No se aceptarán composiciones de productos de diferentes fabricantes;
- La consola de monitoreo y configuración deberá ser a través de una central única, basada en web y en nube, que deberá contener todas las componentes para el monitoreo y control de la protección de los dispositivos;
- La consola deberá presentar un Dashboard con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informacional;
- Debe poseer un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM;
- Este mecanismo de comunicación vía API deberá obtener los eventos y alertas asociados a la consola en al menos, los siguientes formatos: json, cef, or keyvalue.
- Este mecanismo de comunicación vía API deberá obtener la información correspondiente sin eliminarla ni borrarla de la consola primaria de administración.
- La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos.
- Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.
- Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales.
- La instalación debe poder realizarse de forma manual obtenido a través del cliente descargado de la consola central o también vía correo electrónico. El instalador debe permitir la distribución del cliente a través de Active Directory (AD) para múltiples máquinas.
- Proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos.
- Debe permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.
- La consola de administración debe permitir la definición de grupos de usuarios con diferentes niveles de acceso a la configuración, las políticas y los registros.

- Permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador.
- Utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.
- Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.
- Permitir la exportación de los informes gerenciales a los formatos CSV y PDF.
- Los recursos del informe y el monitoreo deben ser nativos de la propia consola central de administración.
- Posibilidad de mostrar información como nombre de la máquina, versión del antivirus, sistema operativo, dirección IP, versión del motor, fecha de la actualización, fecha de la última verificación, eventos recientes y estado.
- Capacidad de generación de informes, estadísticas o gráficos, tales como:
  - Detalle cuáles usuarios están activos, inactivos o desprotegidos, así como detalles de estos.
  - Detalle de los ordenadores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los ordenadores.
- La comunicación debe permitir limitar el ancho de banda utilizado por los agentes.
- La solución deberá permitir la selección de la versión del software de preferencia, permitiendo así la prueba de la actualización sobre un grupo de PC's piloto antes de implementarlo para toda la red. También debe permitir seleccionar un grupo de equipos para aplicar la actualización para controlar el ancho de banda de red. La actualización de la versión debe ser transparente para los usuarios finales.
- La herramienta de administración centralizada debe administrar todos los componentes de la protección para estaciones de trabajo y servidores y debe diseñarse para administrar, supervisar y elaborar informes de endpoint y servidores.
- La Consola de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad.
- Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención.
- Deberá mostrar los ordenadores administrados de acuerdo con los criterios de categoría (detalles del estado del equipo, detalles sobre la actualización, detalles de avisos y errores, detalles del antivirus, etc.), y ordenar los equipos en consecuencia.
- Una vez que se identifique un problema, debe permitir corregir los problemas de forma remota, con al menos las siguientes opciones:
- Proteger el dispositivo con la opción de inicio de una exploración;
- Forzar una actualización en ese momento;
- Ver los detalles de los eventos ocurridos;
- Ejecutar la comprobación completa del sistema;
- Forzar el cumplimiento de una nueva política de seguridad;
- Mover el equipo a otro grupo;
- Borrar el equipo de la lista;
- Aislarlo a demanda de la red corporativa.
- Ejecutar una interfaz de línea de comando sobre el dispositivo.

48

23

- Actualizar las directivas de seguridad cuando un equipo se mueve de un grupo a otro manualmente o automáticamente.
- Grabar un registro de auditoría seguro que supervise la actividad en la consola de administración para el cumplimiento de regulaciones, auditorías de seguridad, análisis y solución de problemas forenses.
- Deberá permitir exportar el informe de registros de auditoría en formatos CSV y PDF.
- Debe contener varios informes para el análisis y control de los usuarios y endpoints. Los informes se deben dividir, como mínimo, en informes de: eventos, usuarios, control de aplicaciones, periféricos y web, indicando todas las funciones solicitadas para los endpoints.
- Permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF.
- Deberá tener la posibilidad de implementar servidores de caché locales para utilizar de manera eficiente el uso del ancho de banda.
- Deberá tener la posibilidad de instalar un servidor para reenvío de eventos en caso de que el agente no pueda comunicarse con la consola en la nube.

8.2 Características básicas del agente de protección contra malware

- Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.
- Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque.
- Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA).
- Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing).
- Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.
- Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo las potencialmente no deseadas (PUA).
- Posee la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección.
- Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección.
- Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidad conocida.
- Ser capaz de aplicar un análisis adicional, inspeccionando el comportamiento del código durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.

- Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.

8.3 Funcionalidad de detección proactiva de reconocimiento de nuevas amenazas

- Protección de amenazas de día 0 a través de tecnología de deep learning (signature less).
- Funcionalidad de detección de amenazas desconocidas que están en memoria con tecnología de Deep learning.
- Capacidad de detección, y bloqueo proactivo de malware no conocido (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.
- Capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria.
- Debe detectar el malware en pre-ejecución un tiempo aproximado de no más de 20 milisegundos.
- Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.
- Análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.
- Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).
- Generación de excepciones ante falsos positivos.
- La solución debe tener capacidad de protección AMSI contra scripts maliciosos.
- La solución debe poseer un IPS Snort de Host.

8.4 Funcionalidad de protección contra ransomware:

- Disponer de capacidad de protección contra ransomware no basada exclusivamente en la detección por firmas.
- Disponer de capacidad de remediación de la acción de encriptación maliciosa de los ransomware.
- Debe poseer protección anti-ransomware para el sector de booteo.
- De restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.

8.5 Protección contra Vulnerabilidades y técnicas de explotación

- Debe brindar detección y protección de al menos las siguientes técnicas de explotación:
- Enforce Data Execution Prevention;
- Mandatory Address Space Layout Randomization;
- Bottom-up ASLR;

25

- Null Page (Null Deference Protection);
- Heap Spray Allocation;
- Dynamic Heap Spray;
- Stack Pivot;
- Stack Exec (MemProt);
- EStack-based ROP Mitigations (Caller);
- Branch-based ROP Mitigations (Hardware Assisted);
- Structured Exception Handler Overwrite (SEHOP);Import Address Table Filtering (IAF);
- Load Library;
- Reflective DLL Injection;
- Shellcode;
- VBScript God Mode;
- Wow64;
- Syscall;
- Hollow Process;
- DLL Hijacking;
- Squiblydoo Applocker Bypass;
- APC Protection (Double Pulsar / AtomBombing):
  - Mitigación de inyección de códigos en procesos.
  - Protección contra robo de credenciales.
  - Protección contra malware escondido en aplicaciones legitimas (code cave).
  - Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.
  - Evitar obtener escalada de privilegios y acceso elevado a recursos.
  - Modificación de las claves de registro para la ejecución de código arbitrario.

8.6 Capacidades de XDR

- El Analista debe poder identificar que atributos de código de un objeto son similares a archivos "known-good" y "known bad" con esto se puede determinar si se pueden permitir o bloquear.
- De tener un Sistema de registro por cada ataque o intento de ataque que se haya producido en los endpoints con información detallada del malware en sí y el origen de la infección (explorador de windows, correo electrónico, navegador, etc.).
- Debe permitir una investigación guiada entregando visibilidad de la dimensión del ataque cómo inicia, cómo impacta, cómo se responde.
- Detectar ataques que pueden haber pasado desapercibidos.
- Buscar de forma proactiva (Threat Hunting) indicadores de compromiso por nombre de archivo, SHA, direcciones IP.
- Priorizar eventos para investigación.
- Poder aislar una maquina comprometida de la red de forma automática mientras la investigación del incidente.
- Poder generar un Snapshot forense durante una investigación de una amenaza.

- Poder realizar queries de estandares de cumplimiento de seguridad.
- Poder realizar queries de tecnicas y tacticas de ataque mapeadas en MITRE ATT&CK.
- Poder realizar queries de conexiones de Red y transferencias de archivos.
- Poder realizar queries sobre información del SO, servicios, parches y más.
- Poder realizar queries de actividad de usuario y autenticación.
- Poder realizar queries de anomalias, actividad o conexiones de red inesperadas.
- Poder realizar queries de eventos en los logs del sistema.
- Poder realizar queries de actividad de procesos y reputación.
- Poder realizar queries de detalles de archivos y acceso a archivos
- Poder realizar queries de accesos y cambios a llaves de registro.

8.7 Despliegue Agente

- Soportar máquinas con arquitectura de 32 bits y 64 bits.
- Compatible con los sistemas operativos Mac MacOS12 en adelante; con los sistemas operativos Windows 7 (hasta 31/3/2025) y Windows 10 en adelante; con los sistemas operativos Windows Server 2008 (hasta 31/3/2025), Windows 2012/2012R2/8.1 (hasta 31/10/2026) y 2016 en adelante.

9. SERVICIO DE PROTECCIÓN DE CORREO ELECTRÓNICO

La institución con la finalidad de optimizar un adecuado uso del ancho de banda contratado requiere contar con una solución para 1500 usuarios de correo por 36 meses que cumpla con las siguientes características:

9.1 Aspectos Generales

- Gestionar la protección de la solución en grupos creados o en forma individual.
- Ver eventos agrupados por categorías de incidentes o amenazas, para permitir enfocar la atención en los compromisos detectados.
- Mostrar en forma gráfica el contexto y relacionamiento de los compromisos detectados.
- Integración con trazabilidad gráfica en la que pueda tener un contexto del incidente, y permita trazabilidad cruzada entre todos los componentes.
- Visibilidad de logs y estadísticas.
- Posibilidad de notificación al usuario final cuando un correo entrante (que lo tenga como usuario destino) ha sido retenido por la solución.
- Posibilidad de notificación al usuario final cuando un correo saliente (generado por el usuario) ha sido retenido por la solución.
- La solución debe tener la capacidad de almacenar datos de los últimos 90 días, y tenerlos disponibles para análisis en base a las caracteristicas del dashboard integral.

27

- Capacidad de exportación de logs a plataformas externas (SIEM/SOC) en formatos estándares del mercado.
- Capacidad de integración por medio de API´s abiertas a consolas externas centralizadas.
- Mostrar a nivel de reporte las direcciones de correo electrónico que recibieron la mayor cantidad de mensajes relacionados con Business Email Compromise (BEC).

9.2 Configuración y administración

- Debe ser compatible con Microsoft Exchange Online y Microsoft Office 365
- Debe ser compatible con Microsoft Exchange 2003 o posterior.
- En el caso de Microsoft office 365, debe tener la capacidad de integrarse vía API sin la necesidad de modificar registros DNS.
- Debe ser compatible con G Suite de Google Cloud
- Debe ser compatible con cualquier servicio de correo en el que sea propietario del dominio y controle los registros DNS asociados.
- Debe tener la capacidad de sincronizarse con Microsoft Active Directory
- Debe tener la capacidad de sincronizar con Microsoft Azure Active Directory
- Debe tener la capacidad de soportar múltiples dominios para la misma organización.
- Debe poder mantener a los usuarios sincronizados automáticamente con el producto mediante ADSync.
- Debe proporcionar al administrador la capacidad de agregar manualmente registros de alias de direcciones de correo electrónico cuando Active Directory no esté disponible.
- La solución debe tener la capacidad de crear diferentes tipos de roles para la gestión / administración de la plataforma.
- Debe proporcionar al administrador la capacidad de encontrar buzones de correo específicos.
- Debe tener un portal de autoservicio para usuarios finales.
- El portal de autoservicio debe permitir a los usuarios administrar correos electrónicos en cuarentena (aceptar / eliminar correos electrónicos)
- El portal de autoservicio debe permitir a los usuarios editar las reglas de permitir / bloquear
- El portal de autoservicio debe permitir a los usuarios ver los mensajes en caso de interrupción utilizando la bandeja de entrada de emergencia.
- Debe proporcionar a los usuarios la capacidad de agregar Smart Banners (un sistema de clasificación de colores simple) a cualquier correo electrónico recibido desde fuera de la organización, lo que ayuda a los destinatarios a identificar el riesgo de cada correo electrónico y les permite agregar remitentes a sus listas de permisos y bloqueos con un solo clic.

- Debe poder crear políticas de seguridad de correo electrónico únicas para individuos, grupos o todo el dominio.
- Debe cumplir con las regulaciones de cumplimiento de datos.
- Debe tener una opción de centros de datos globales al momento de la creación de la cuenta, como Reino Unido, EE. UU. Y Alemania.

9.3 Continuidad del negocio

- Debe tener la capacidad de manejar una cola de correo electrónico que garantice que no se pierda ningún correo.
- En caso de una interrupción de su servicio de correo electrónico de Microsoft o Google Cloud, el producto debe tener la capacidad de poner en cola automáticamente los correos electrónicos del destinatario y luego entregarlos una vez que se restablezca el servicio con un periodo de reintento de cinco días.
- Debe proporcionar al usuario acceso a una bandeja de entrada de emergencia 24 horas al día, 7 días a la semana.
- Debe tener la capacidad de enviar alertas cuando el correo no se pueda entregar a un servidor / servicio en caso de interrupciones de un proveedor de servicios de correo electrónico en la nube de terceros.

9.4 Seguridad

- Debe tener actualizaciones de amenazas en vivo para detener los últimos ataques.
- Debe tener detección antispam, antivirus y antiphishing.
- Debe tener un filtro de reputación que pueda bloquear al menos con un 90% del spam.
- Debe tener tecnología de filtrado de reputación de próxima generación que elimine el spam de botnet en el nivel de conexión IP al monitorear las solicitudes de conexión y rechace aquellas que muestren evidencia de conexiones de botnet.
- Debe proteger contra el spam tipo "Snowshoe Spamming"
- Debe tener un portal para el usuario final que luego permita a los usuarios publicar correos electrónicos bajo demanda y resúmenes de cuarentena en el mensaje que brinden un resumen diario del correo en cuarentena, con la opción de liberarlos directamente desde la bandeja de entrada.
- Debe tener técnicas de autenticación SPF, DKIM y DMARC para identificar y permitir correos electrónicos legítimos mientras bloquea a los impostores.
- Debe tener detección de anomalías en el encabezado que identifique si el nombre para mostrar del remitente es el mismo que un nombre de usuario interno.

9.5 Protección contra la suplantación de identidad

- Debe poder comparar el nombre para mostrar de los correos electrónicos entrantes con el nombre para mostrar de las marcas de servicios en la nube y tener la opción

42

29

de poder parametrizar usuarios con categoría VIP para evitar la suplantación de identidad dentro de la organización.
- Debe poder hacer un análisis de dominios similares para identificar nombres de dominio de uso corporativo.
- Los mensajes sospechosos se pueden bloquear, poner en cuarentena, etiquetar con una advertencia en la línea de asunto o agregar un banner con un enlace directo a la lista de bloqueo a nivel de usuario.

9.6 Protección de la información.

- Debe escanear automáticamente los cuerpos de los mensajes y los archivos adjuntos en busca de datos confidenciales para establecer fácilmente políticas para bloquear o cifrar los mensajes.
- Debe brindar a los usuarios la capacidad de cifrar correos electrónicos utilizando el complemento O365 del producto.
- Debe tener un cifrado basado en inserción que proteja todo el correo electrónico o solo los archivos adjuntos.
- Debe tener un cifrado TLS reforzado que evite las escuchas cuando los mensajes están en tránsito.
- Debe tener capacidades de control de contenido y prevención de pérdida de datos.

9.7 Protección activa contra amenazas

- Debe tener capacidad de reescritura de URL para verificar la reputación del sitio web de los enlaces de correo electrónico antes de la entrega y en el momento en que hace clic, bloqueando ataques furtivos y retardados.
- Debe contar con un laboratorio en nube que permita la clasificación de amenazas, protección de día cero, análisis exhaustivo de objetos limpios y maliciosos conocidos.

9.8 Informes completos

- Debe contar con un Panel de Control (Dashboard), en donde se ilustre de manera general el comportamiento del estado de los correos electrónicos analizados, así mismo deberá ilustrar que buzones de correo electrónico se encuentran en riesgo.
- Debe proporcionar informes de estadísticas dentro de la consola en forma de tablas y gráficos con rangos de fechas personalizados.
- Debe incluir un informe que proporcione información completa sobre el encabezado del mensaje y cualquier archivo adjunto.
- Debe incluir un informe que proporcione detalles de los pasos por los que pasó el mensaje en la infraestructura de análisis de correo electrónico.
- Debe incluir un reporte sobre detecciones asociadas a la política para prevención de Fuga de Información.

41

30

- Debe incluir un Informe de amenazas avanzado que proporcione un resumen de los mensajes entrantes que se detonaron en el entorno de la zona de pruebas, que se puede filtrar por fecha y el resultado del análisis durante el último año.

9.9 Seguridad avanzada

- Debe tener la capacidad de vincular la solución Email Security y Endpoint Protection para aislar automáticamente los buzones de correo comprometidos y limpiar las computadoras infectadas que envían spam y malware salientes.

10. SERVICIO DE RESPALDO DE INFORMACION

- Modalidad Software como Servicio (SaaS Software as a Servicie), la cual debe alojarse en un Centro de Datos con presencia global
- La interacción del servicio de respaldo será a través de servidor virtual privado (VPS) dedicado exclusivamente para almacenamiento e integrado con la infraestructura local del Gobierno Regional de Piura a través de una VPN privada, donde se podrá enviar información, carpetas y archivos de cualquier tipo hacia el servicio de almacenamiento con fines de trasladar la información sensible del Gobierno Regional de Piura, hacia un sitio externo. (opcional)
- Tamaño de almacenamiento mínimo de 4 TB en discos de estado sólido (SSD) (opcional)
- Debe ofrecer adicionalmente respaldo en RAID 6 en discos de clase empresarial para acceso SFTP como mínimo de 100GB FTP Storage. (opcional)
- Ancho de banda de mínimo 32TB de salida e ilimitado para tráfico entrante a una velocidad de 1 Gbit/s (opcional)
- Debe contar con un panel de monitoreo del uso de ancho de banda, rendimiento, tiempo de inactividad y configurar alertas por correo electrónico o mensajes de texto (opcional)
- Debe contar con certificados SSL firmados por una entidad certificadora (CA)
- Permitir crear redes privadas virtuales de alta velocidad, con tráfico interno ilimitado y no medido que permita mejorar la seguridad y el rendimiento.
- Direccionamiento IPv4 e IPv6 dedicadas, con opciones para configurar IP adicionales en caso de crecientes demandas de red. (opcional)
- Infraestructura equipada con mitigación DDoS siempre activa, que permita proteger los activos digitales contra ataques y garantizar operaciones ininterrumpidas. (opcional)
- Debe permitir automatizar y administrar los recursos en la nube de manera efectiva a través de API o directamente a través de la CLI de manera que simplifique las operaciones en la nube. (opcional)
- Debe permitir administrar la configuración de DNS fácilmente a través de un panel de control, con diversas opciones, lo que facilita una integración perfecta. (opcional)

- Debe permitir mejorar el proceso de implementación con imágenes personalizadas, cloud-init, claves SSH y canales de CI/CD, diseñados para operaciones de desarrollo rápidas y eficientes. (opcional)
- Tener disponibilidad global y contar con mínimo 10 centros de datos con latencia mínima y disponibilidad de servidores respaldada por SLA.
- Compatible con aplicaciones que no tienen altos requisitos de E/S y necesitan leer/escribir una gran cantidad de datos mientras realizan cálculos, aplicacioines compatibles serán como mínimo: SQL Server, Exchange Server, Active Directory, BD Oracle, Microsoft 365, Google Workspace, C Pannel, MySQL on Linux.
- Debe permitir realizar copias de seguridad, archivar datos y recuperarse ante desastres.
- Debe ofrecer servidores con equipamiento lideres del mercado como Intel, AMD, DELL y/o HP y/o Huawei (opcional)
- Debe permitir optimizar las copias de seguridad llevadas a la nube.
- Deben ser propietarios de sus Centros de datos y de todo su hardware. (opcional)
- Brindar soporte durante todo el periodo del servicio. (opcional)
- Manejar estrictas reglas de acceso basado en roles (RBAC) en sus centros de datos.
- Debe ser compatible con compatible con Archilinux, Sombrero, FreeBSD, AlmaLinux, RockyLinux
- El Proveedor es responsable de realizar todas las configuraciones para integrar la instancia en nube a la infraestructura tecnológica del Gobierno Regional de Piura.
- La solución de respaldo en la nube es por un periodo de 36 meses calendarios contados a partir del día siguiente de entregadas las credenciales de acceso al correo que determine la Jefatura de la Oficina de Tecnologías de la Información.

11. SERVICIO DE ANALISIS DE VULNERABILIDADES

Realizar una prueba de seguridad ofensiva que simula un ciber ataque real en un entorno controlado. El objetivo es identificar las debilidades que podrían ser aprovechadas por un atacante y completar así amenazas de tipo robo de información, acceso indebido, provocar caídas de servicios, la instalación de malware y otros.

Realizar el servicio de Pentesting a los a activos considerados en el alcance del servicio son los siguientes:

- Web Server: 5
- IP Hosts: 100
- Se deberá realizar al menos dos (02), Capacidad de Retake, pasados los 06 meses del escaneo inicial por la entidad bajo la misma plataforma o tenant, el cual permita contrastar los cambios y/o mejoras realizadas.

El postor debe presentar una metodología para el desarrollo del servicio que implique plataformas de Pentesting Licenciadas (No uso de Open Source), que contenga como

32

mínimo las siguientes características:

❖ **Simulación de ataques Programados**

Ataque externo: Lanzamiento de ataques desde fuera de la red empresarial hacia activos de acceso público, como sitios web de organizaciones, recursos compartidos de archivos o servicios alojados en la nube pública/CDN.

Ataque Interno: Despliegue ataques desde el interior de la red empresarial con el permiso del cliente, centrándose en explotar las vulnerabilidades descubiertas en la red y los sistemas locales.

❖ **Plataforma de Inteligencia de Amenazas**

- Debe contar con una base de datos extensa de más de 36,000 vulnerabilidades y una amplia colección de exploits. Al utilizar todas las técnicas y tácticas del framework MITRE ATT&CK
- Uso del CVSS score (Common Vulnerability Scoring System) para evaluar y calificar las vulnerabilidades presentes en sistemas y aplicaciones.
- Debe realizar un escaneo de vulnerabilidades.
- Debe realizar un escaneo de puertos, servicios y aplicaciones.
- Debe realizar tareas programadas de escaneo de vulnerabilidades en redes y aplicaciones.
- Debe realizar auditoria de configuración para el cumplimiento de políticas y estándares.
- Debe realizar escaneo de múltiples redes IPv4, IPv6 y redes híbridas.
- Debe realizar identificación de datos sensibles en objetivos a escanear.
- Debe realizar descubrimiento de activos en la red incluyendo cortafuegos de nueva generación, sistemas operativos, bases de datos, aplicaciones web, ambientes virtuales y servicios en la nube.
- Debe realizar escaneo con credenciales y sin credenciales.

  Dividida en dos categorías principales: escaneos sin credenciales en dispositivos de red interna y escaneos en páginas web, que pueden realizarse tanto con o sin credenciales

  - Escaneos sin credenciales en dispositivos de red interna (host):

    En el caso de los dispositivos de red interna, realizamos escaneos sin necesidad de autenticación o credenciales específicas. Esto significa que examinamos la infraestructura de red, incluidos los dispositivos como computadoras, servidores, enrutadores y otros dispositivos conectados a la red, sin requerir contraseñas o credenciales de acceso. Estos escaneos nos

permiten identificar posibles vulnerabilidades y problemas de configuración que puedan ser explotados por atacantes sin acceso directo a las credenciales.

- Escaneos en páginas web con o sin credenciales:

  En el caso de las páginas web, ofrecemos flexibilidad para realizar escaneos tanto con credenciales de acceso como sin ellas. Los escaneos sin credenciales, también conocidos como escaneos "externos" o "de caja negra", se realizan desde fuera de la red y simulan un enfoque de ataque desde el punto de vista de un atacante externo. Estos escaneos nos permiten identificar posibles vulnerabilidades que puedan ser aprovechadas por atacantes sin acceso a credenciales de usuario en la página web.
  Por otro lado, los escaneos con credenciales, también conocidos como escaneos "internos" o "de caja blanca y gris", se realizan con acceso autorizado y legítimo a la página web utilizando credenciales de usuario válidas. Estos escaneos nos brindan una visión más profunda y detallada de las vulnerabilidades internas y de las posibles debilidades que podrían ser explotadas por atacantes con acceso autenticado.

  - Debe realizar el escaneo selectivo.
  - Debe realizar análisis automático de escaneo.
  - Debe realizar la priorización de acciones de remediación y recomendaciones para su corrección.
  - Debe categorizar la vulnerabilidad encontrada por nivel de criticidad.
  - Debe realizar un escaneo basado en agentes.
  - Debe permitir gestionar y compartir recursos de escaneo desde una consola central.
  - Debe contar con actualizaciones de contenido como vulnerabilidades, amenazas avanzadas, día cero, y nuevos tipos de configuraciones de cumplimiento regulatorio.
  - Debe realizar la gestión de usuarios y grupos.
  - Debe realizar informes flexibles y personalizados para la clasificar por vulnerabilidad o servidor, creación de resumen ejecutivo o comparación de resultados.
  - Debe generar informes en formato HTML, PDF y CSV
  - Debe contar con tableros de control.
  - Debe brindar una interfaz gráfica para la modificación manual de la criticidad o categorización de las vulnerabilidades
  - Generación de reportes customizados de OWASP TOP 10, Sumario Ejecutivo, Mitre Att&ck, Raw Data (CSV) y Técnico con detalles de vulnerabilidades como sus respectivas remediaciones

❖ **Análisis de seguridad de las aplicaciones web.**

- Servicios de ejecución de pruebas de Análisis Dinámico la posibilidad de realizar Análisis Híbrido o Interactivo (IAST -Interactive Application Security Testing) en aplicaciones basadas en los lenguajes de programación Java y .NET

- Capacidades de pruebas de seguridad dinámica de aplicaciones (DAST) y pruebas de seguridad interactivas de aplicaciones (IAST) que fortalecen las posturas de seguridad de DevSecOps. DAST proporciona una perspectiva externa de la aplicación antes de que se publique, mientras que IAST analiza aplicaciones interactivas en las que los usuarios ingresan sus datos.
- El DAST analiza aplicaciones web antes de su lanzamiento en producción para encontrar vulnerabilidades utilizando ataques simulados tal como lo haría un actor malintencionado. El escáner DAST busca anomalías fuera del conjunto de resultados esperado para identificar vulnerabilidades de seguridad.
- Las capacidades de IAST ayudan a los equipos de DevSecOps a identificar y gestionar los riesgos de seguridad asociados con las vulnerabilidades descubiertas en las aplicaciones web en ejecución mediante técnicas de pruebas dinámicas.

❖ **Seguridad de DevSecOps:**

- Asegurar la aplicación antes de su implementación con DAST e IAST automatizados.
- Permitir a DevSecOps probar aplicaciones y gestionar riesgos a gran escala.
- Garantizar el cumplimiento de las regulaciones de datos y privacidad en las aplicaciones web.
- Permite a DevSecOps crear un programa de aplicaciones que respalde una postura de seguridad sólida.

  Dentro de un entorno de desarrollo dinámico, la prueba automatizada de seguridad de aplicaciones de la Plataforma encuentra vulnerabilidades que pueden permitir inyecciones de SQL, scripting entre sitios (Cross-Site Scripting) y otros ataques. Proporciona informes y envía alertas automatizadas para que el equipo de DevSecOps pueda remediar las vulnerabilidades de inmediato.

  Integración con los entornos de desarrollo de Jira y GitLab. Si RidgeBot detecta una vulnerabilidad, la reportará a Jira o GitLab como una tarea para que el desarrollador la solucione dentro del flujo de trabajo de la plataforma. Cuando DevSecOps cuenta con seguridad incorporada para respaldar aplicaciones existentes y emergentes, tienen la capacidad de innovar más rápido y con menos riesgo.

- El Servicio deberá ser realizado como mínimo por 2 especialistas con certificación nivel profesional oficial en la marca de la plataforma propuesta.

12. SERVICIO CONTRA ATAQUES DE NEGACIÓN DE SERVICIO ANTI-DDoS

El postor debe de ofertar una solución en nube (cloud) del servicio de Anti-DDoS, considerando que el ataque debe de quedar en la plataforma del operador y no afectar el ancho de banda de internet contratado por el Gobierno Regional.

Las características que debe de cumplir el servicio son:

- Deberá proteger el Tráfico saliente a Internet del Gobierno Regional de Piura (opcional)
- Detección y diferenciación entre tráfico malicioso y válido: mitiga los ataques maliciosos de tráfico y entrega el tráfico limpio.
- Protección contra ataques DDoS volumétricos y de aplicación en tiempo real.
- Protección DNS, identificación y bloqueo automático de los ataques que tratan de llegar a los servidores DNS.
- Protección general de infraestructuras para los protocolos conocidos y servicios (UDP/TCP, SMTP, FTP, SSH, VoIP, etc.)
- Reportería y notificación de eventos de manera mensual.
- Definir mecanismo (reporte) de gestión de incidencias de seguridad para ser comunicados al Gobierno Regional en el momento de la ocurrencia de las incidencias de seguridad, durante la fase de implementación del servicio en conjunto con el personal de TI se definirá dicho mecanismo.
- El ancho de banda que debe de soportar el equipamiento debe ser mínimo el doble del ancho de banda de Internet contratado por el Gobierno Regional, sin embargo, en caso de ataque de mayor volumetría el operador debe de garantizar la mitigación del mismo, sin que se afecte el servicio de internet contratado. para ello la plataforma del proveedor deberá tener la capacidad de throughput inspección y mitigación de 10 Gbps y/o 20 Gbps de tráfico.
- La solución debe incluir la protección contra ataques de denegación de servicio a nivel de aplicación sin estados (stateless), por lo que no deberá tener Límite de conexiones ni de sesiones concurrentes para el tráfico total (incluyendo tráfico atacante) y/o La solución de protección contra ataques de denegación de servicio deben ser dimensionadas de tal forma que la entidad no se vea comprometida ante este tipo de ataques cibernéticos, no debiendo tener límite de conexiones ni de sesiones concurrentes para el tráfico total (incluyendo tráfico atacante).

13. GESTIÓN DEL SERVICIO

- El tiempo de atención máximo para la subsanación de un problema, será de cuatro (04) horas, contadas desde que La Sede Central del Gobierno Regional Piura reporta el incidente al Centro de Servicio del postor y se le asigna un ticket de atención. Dicho reporte será vía llamada telefónica, para lo cual la empresa deberá dar la información sobre los puntos de contacto a La Sede Central del Gobierno Regional Piura.
- El proveedor deberá garantizar un eficiente sistema de gestión de sus redes de comunicación. El centro de gestión deberá estar en capacidad de realizar acciones de controles preventivos, correctivos y pruebas técnicas 7x24x365.
- El. proveedor deberá garantizar el profesionalismo, responsabilidad y conocimientos técnicos de su personal en los centros de llamadas de reportes de fallas, centros de gestión, y personal de reparación de averías. Así mismo, deberá

35

36

contar con el equipamiento necesario para solucionar los problemas técnicos que se presenten.

- Durante el periodo de prestación del servicio, se evaluarán los tiempos de respuesta y la calidad del servicio, a fin de que La Sede Central del Gobierno Regional Piura determine las correcciones necesarias si fuera el caso. La Sede Central del Gobierno Regional Piura se reserva la potestad de constatar la información presentada por el operador.
- El proveedor deberá de proporcionar los números celulares de por lo menos 3 soportes para escalamiento de la atención que se requiera en temas de configuración o reconfiguración inmediata de los diversos equipos de seguridad propuestos y ante alguna contingencia de intentos de violación de la seguridad. Siempre que no se tenga respuesta por parte del call center o no se cumplan con los tiempos de atención solicitados. Dicha información deberá ser proporcionada para el perfeccionamiento del contrato.

14. INSPECCIÓN Y PRUEBAS

- El proveedor y el personal de la Oficina de Tecnologías de la Información de La Sede Central del Gobierno Regional Piura, una vez terminada la instalación, realizarán en forma conjunta los procedimientos de inspección y pruebas sobre la infraestructura y equipos instalados, de tal forma que le permita, establecer que los servicios serán brindados de conformidad con lo requerido en las bases y en la propuesta del proveedor.
- Las pruebas se realizarán en los lugares de instalación. Los costos que demanden las mismas, no implicarán en ningún caso. reconocimiento de gastos por parte de La Sede Central del Gobierno Regional Piura y deberán ser provistos por el proveedor.
- La omisión en la oferta de algún producto que al momento de las pruebas resulte necesario para la provisión de los servicios, o para el cumplimiento de las especificaciones funcionales y/o técnicas ofrecidas, obligará al proveedor a brindarlo sin cargo alguno.
- Cualquier defecto notificado por La Sede Central del Gobierno Regional Piura al proveedor durante la realización de las pruebas de aceptación, será rectificado por este sin cargo alguno, teniendo como plazo máximo 5 (cinco) días calendario a partir de su notificación.
- Una vez realizados los procedimientos de inspección y pruebas a conformidad de La Sede Central del Gobierno Regional Piura, éste firmará el Acta de Conformidad de activación del servicio.

9 CONFORMIDAD DEL SERVICIO

La conformidad será otorgada por el responsable de la Oficina de Tecnologías de la Información, el mismo que emitirá un informe mensual del servicio realizado.

10 FORMA DE PAGO

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

En el primer pago:

- Informe Final con detalles técnicos y de infraestructura de telecomunicaciones implementados en la Sede Central del Gobierno Regional Piura, así como información con respecto a la tecnología utilizada, equipos y accesorios, previa aprobación de la Oficina de Tecnologías de la Información.
- Acta de Conformidad de Activación del Servicio.
- Informe Mensual del servicio realizado por el funcionario responsable de la Oficina de Tecnologías de la Información emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago (Recibo de Servicios de acuerdo al formato debidamente aprobado por SUNAT y OSIPTEL).

Pagos Posteriores:

- Informe Mensual del servicio realizado por el funcionario responsable de la Oficina de Tecnologías de la Información emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

Se debe tener en cuenta, sin que afecte el valor del monto adjudicado, en caso que el inicio de la prestación del servicio no coincida con el ciclo de facturación del operador adjudicatario de la buena pro, la primera y la última facturación incluiría un cargo por el prorrateo del servicio brindado durante los días previos al inicio y culminación del correspondiente ciclo de facturación, Este ultimo asignado por el proveedor.

11 DOCUMENTACIÓN Y CONSIDERACION ADICIONAL

- El proveedor deberá entregar un informe final de los detalles técnicos de cada equipo (Router, Equipo de Seguridad Perimetral así como la información técnica de los servicios ofertados donde se indique mínimamente el Nombre Comercial del Servicio Anti DDoS, las modalidades o tipos de licencias contratadas para estos servicios, y de la infraestructura de telecomunicaciones implementados en La Sede Central del Gobierno Regional Piura, así como información con respecto a la tecnología utilizada adjuntando certificados, constancias, datasheets, folletos y/o información pública del fabricante, pudiendo ser en idioma original. El Informe Final se entregará al finalizar la fase de implementación y previo a la suscripción del Acta de Conformidad de Activación del Servicio.

- Diagrama o topología de la arquitectura (Redes, interconexión, protocolos.) de la solución propuesta, incluyendo todo lo que constituye la oferta del operador de comunicaciones, así como sus rutas alternas de respaldo. El cual será presentado para el perfeccionamiento del contrato.

37

38

- El proveedor deberá tomar las previsiones del caso a fin de no perjudicar el inicio de las labores diarias en La Sede Central del Gobierno Regional Piura en el momento de la implementación del servicio.

12 CLAUSULA ANTICORRUPCION

- El Proveedor 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 248-A 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 servicio.

- Asimismo, el Proveedor se obliga a conducirse en todo momento, durante la ejecución del servicio, con honestidad, probidad, veracidad e integridad y a 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 248-A Reglamento de la Ley de Contrataciones del Estado.

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

13 CONFIDENCIALIDAD

El proveedor se compromete a mantener reserva, y no revelar a tercero alguno sin previa conformidad escrita en la Sede Central del Gobierno Regional Piura la información que le sea suministrada por esta. Se entiende que de acuerdo a lo dispuesto en el art. 147° del Reglamento de la Ley de contrataciones del Estado, No aplica la subcontratación por ser una prestación vinculadas a los aspectos que determinan la selección del contratista.

14 OTRAS PENALIDADES.

PENALIDAD POR FALTA DE SERVICIO:

- ✓ La Sede Central del Gobierno Regional Piura aplicará al proveedor una penalidad por las caídas del servicio de Internet registradas durante el periodo contractual, sólo deberá haber un máximo de 04 horas de pérdida del servicio mensual como máximo, caso contrario La Sede Central del Gobierno Regional Piura la siguiente penalidad:

OTRAS PENALIDADES			
Nº	Supuestos de aplicación de	Forma de cálculo	Procedimiento

	penalidad		
1	Falta de Servicio por mas de 4 horas al mes.	(P) = (0.19% x Mmv) Nhr P = Penalidad (por el tiempo sin servicio) NHr = Número de horas sin servicio (en exceso a las 4 horas máximas permitidas) MMmv = Monto Mensual Vigente	(*) Procedimiento de Validación en Línea siguiente

(*)
Se validará la falta de servicio con una prueba de conectividad hacia los DNS (remotos) de GOOGLE Y CLOUDFARE de la siguiente manera:

1ro. Validar si el GATEWAY de la red se encuentra operativo:
Esto se realiza desde una estación de trabajo local realizando un pineo a la IP del Gateway de no recibir respuesta verificar que los Gateways estén encendidos y operativos, conectados a la red local. Si aun así siguen sin responder y la red local se encuentra operativa, reportarlos como inoperativos ante el proveedor. De estar operativos ir al siguiente paso.

2do. Validar acceso hacia internet desde la LAN.
Desde la misma estación de trabajo local realizando un pineo a la ip de los DNS de Google (8.8.8.8 y 8.8.8.4), de no obtener respuesta realizar un pineo a los DNS de Cloudflare (1.1.1.1 y 1.0.0.1), si la respuesta sigue siendo negativa proceder al siguiente paso.

3ro. Validar acceso hacia internet desde el GATEWAY (FIREWALL)
Ingresar vía web a la interface del Gateway y verificar en el Dashboard del mismo la operatividad de los enlaces WAN. Si la gráfica muestra poco o nada de movimiento en el enlace WAN proceder a ejecutar la utilidad CLI consola del mismo firewall y ejecutar lo siguiente uno a la vez;

execute ping 8.8.8.8
execute ping 4.4.4.4
execute ping 1.1.1.1
execute ping 1.0.0.1 y validar si sigue sin haber respuesta de paquetes recibidos.

Si después de realizar este procedimiento sigue sin haber respuesta al envió de paquetes a los (hosts remotos) DNS de Google o Cloudfare, habremos determinado la inoperatividad de ambos enlaces pues al haberse requerido una configuración en alta disponibilidad (HA) si uno solo de los enlaces hubiera caído el otro debería de estar operativo y permitir la operatividad del servicio.

Corroborado lo anterior, la Oficina de Tecnologías de la Información emitirá el informe respectivo y lo hará de conocimiento de la Gerencia Regional de Administración quien a su vez ordenará al área de contrataciones las acciones a que hubiere lugar para la ejecución de las penalidades.

La sustentación, por parte de La Sede Central del Gobierno Regional Piura, de un acumulado de más del 10% del monto contractual vigente debido

15 DE LA GARANTÍA

- Duración 36 MESES
- La garantía incluirá el suministro de repuestos, componentes y piezas, en caso de emergencia, sin costo alguno para La Sede Central del Gobierno Regional Piura. Para esto, el proveedor cuenta con un plazo de 04 horas. Para casos extremadamente graves los cuales sea verificables de manera fehaciente por el Gobierno Regional Piura la imposibilidad de dar una solución dentro de este plazo, de manera excepcional se ampliará el mismo a 24 horas.
- Para la atención del servicio es indispensable que el PROVEEDOR cuente con soporte en la ciudad de Piura y si es en consorcio al menos una de las empresas que la conforman. Para una respuesta más rápida del servicio. Así mismo deberá contar con personal técnico capacitado como mínimo en routing a fin de dar una mejor solución al problema.

Importante

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

16 REQUISITOS DE CALIFICACIÓN

REQUISITOS DE CALIFICACIÓN

A	**CAPACIDAD LEGAL**
	HABILITACIÓN
	Requisitos: Autorización del Ministerio de Transportes y Comunicaciones (MTC) para la presentación del servicio en la modalidad de Internet Servís Provider o Proveedor (ISP). Acreditación: Copia de autorización del MTC para la prestación del servicio o el cuadro publicado en la página Web del Ministerio de Transportes donde se detalla las autorizaciones para brindar el servicio o las concesiones vigentes del postor para el servicio de valor añadido en el cual se puede verificar que se ofrece el servicio de Conmutación de Datos por paquetes (internet) o copia de la publicación en el diario oficial de la Resolución del Otorgamiento de Concesión

B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.1	CALIFICACIONES DEL PERSONAL CLAVE

B.1.1	FORMACIÓN ACADÉMICA
	Requisitos: **Un (01) jefe de Proyecto:** Ingeniero titulado y colegiado, habilitado en Electrónica y/o Telecomunicaciones y/o Sistemas y/o Redes y Comunicaciones y/o Computación y Sistemas y/o Informática. **Un (01) Especialista en Networking** Ingeniero titulado y colegiado, habilitado en Electrónica y/o Telecomunicaciones y/o Sistemas y/o Redes y/o Computación y Sistemas y/o Informática. **Un (01) Especialista en Seguridad de la Información** Ingeniero titulado y colegiado, habilitado en Electrónica y/o Telecomunicaciones y/o Sistemas y/o Redes y Comunicaciones y/o Computación y Sistemas y/o Informática. Acreditación: El TÍTULO PROFESIONAL será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: *https://enlinea.sunedu.gob.pe/* o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: *https://titulosinstitutos.minedu.gob.pe/*, según corresponda. En caso el título profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
B.1.2	CAPACITACIÓN
	Requisitos: **Un (01) jefe de Proyecto:** - Certificaciones/Capacitación: - Curso Especializado Gestión de Proyectos Basados en el PMBOK o certificación PMP - Curso en ITIL Foundation Certificate. - Curso y/o Especialización en la ISO 27001 como implementador líder mínimo de 40 horas. - Taller de especialización en tópicos de infraestructura en la marca de un fabricante de networking. (opcional) **Un (01) Especialista en Networking** - Certificación oficial y vigente a nivel asociado y/o profesional en la marca de los routers propuestos y/o certificaciones de networking independiente de la marca específica del router propuesto, como CCNA (Cisco Certified Network Associate) o HCNA (Huawei Certified Network Associate), **Un (01) Especialista en Seguridad de la Información** - Certificación Profesional como Implementador líder en ISO/IEC 27001. - Certificación Profesional como líder en CIBERSEGURIDAD (LCSPC) - Certificación Profesional Ridge Security Certified Professional (RSCP)

	- Curso Especializado Gestión de Proyectos Basados en el PMBOK mínimo 24 horas lectivas - Curso Especializado en Cobit 5 Foundation Level, como un mínimo de 20 horas Acreditación: Se acreditará CON CONSTANCIAS, CERTIFICADOS, U OTROS DOCUMENTOS, SEGÚN CORRESPONDA.
B.2	**PERIENCIA DEL PERSONAL CLAVE**
	Requisitos: **Un (01) jefe de Proyecto:** - Dos (02) años de experiencia como jefe de proyectos en TI en empresas de Telecomunicaciones realizando funciones ¡guales o similares al objeto de la convocatoria o la implementación de Servicios Fijos como transmisión de datos, Internet así como también Infraestructura de Data Center.. **Un (01) Especialista en Networking** - Dos (02) años de experiencia como Especialista de Networking realizando implementaciones de servicios de internet e interconexión de sedes en entidades públicas o privadas **Un (01) Especialista en Seguridad de la Información** - Experiencia de dos (2) años en sector públicos y/o privados, en implementación y/o ejecución de proyectos relacionados a Tecnologías de la Información y Comunicación, administración de data center, virtualización, seguridad en ambientes de alta criticidad, tecnología CLOUD y/o implementación de servidores y centro de datos y/o virtualización de servidores y/o redes y cableado estructurado para el sector público y/o privado y/o similares. - Profesional con experiencia en proyectos públicos en definición y/o implementación y/o ejecución de proyectos relacionados a Ciberseguridad, usando marcos de referencia como el NIST Cybersecurity Framework. Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

C	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 758,692.80 (Setecientos Cincuenta y ocho Mil Seiscientos Noventa y dos con 80/100 Soles), por la contratación de servicios 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. Se consideran servicios similares a los siguientes Internet dedicado y/o transmisión de datos y/o, Ciberseguridad y/o fibra oscura. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, 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 pago[1], correspondientes a un máximo de veinte (20) contrataciones. 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. En el caso de servicios de ejecución periódica o continuada, 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. 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. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. 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.

[1] 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 si se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".*

	Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**. Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

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	
Evaluación: Se evaluará considerando el precio ofertado por el postor. Acreditación: Se acreditará mediante el documento que contiene el precio de la oferta **(Anexo N° 6)**.	La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $Pi = \frac{Om \times PMP}{Oi}$ **i** = Oferta **Pi** = Puntaje de la oferta a evaluar **Oi** = Precio i **Om** = Precio de la oferta más baja **PMP** = Puntaje máximo del precio **90 puntos**
H. MEJORAS A LOS TERMIOS DE REFERENCIA	
Evaluación: Se evaluará considerando el ANCHO DE BANDA ADICIONAL OFERTADO POR EL POSTOR. Acreditación: Se acreditará únicamente mediante la prestación de una Declaración Jurada.	**(Máximo 10 puntos)** Mas de 800 Mbps **10 puntos** Menor de 700 a 800 Mbps **05 puntos**
PUNTAJE TOTAL	**100 puntos**[8]

Importante

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

[8] Es la suma de los puntajes de todos los factores de evaluación.

CAPÍTULO V
PROFORMA DEL CONTRATO

Importante

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

Conste por el presente documento, la CONTRATACIÓN DEL SERVICIO DE INTERNET – SEGURIDAD PERIMETRAL PARA LA SEDE CENTRAL DEL GOBIERNO REGIONAL PIURA., que celebra de una parte [CONSIGNAR EL NOMBRE DE LA ENTIDAD], en adelante LA ENTIDAD, con RUC Nº [.....], con domicilio legal en [.....], representada por [.....], identificado con DNI Nº [.....], y de otra parte [.....], con RUC Nº [.....], con domicilio legal en [.....], inscrita en la Ficha N° [.....] Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], debidamente representado por su Representante Legal, [.....], con DNI N° [.....], según poder inscrito en la Ficha N° [.....], Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [.....], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO Nº 15-2024-GRP-ORA-CS-CP-1 (Primera Convocatoria)** para la C CONTRATACIÓN DEL SERVICIO DE INTERNET – SEGURIDAD PERIMETRAL PARA LA SEDE CENTRAL DEL GOBIERNO REGIONAL PIURA, a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto la CONTRATACIÓN DEL SERVICIO DE INTERNET – SEGURIDAD PERIMETRAL PARA LA SEDE CENTRAL DEL GOBIERNO REGIONAL PIURA.

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 servicio, 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 del servicio materia del presente contrato.

CLÁUSULA CUARTA: DEL PAGO[9]

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en [INDICAR MONEDA], en [INDICAR SI SE TRATA DE PAGO ÚNICO, PAGOS PARCIALES O PAGOS PERIÓDICOS], 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 de las contraprestaciones pactadas a favor del CONTRATISTA dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios,

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

siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

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

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de [.....], el mismo que se computa desde [CONSIGNAR SI ES DEL DÍA SIGUIENTE DEL PERFECCIONAMIENTO DEL CONTRATO, DESDE LA FECHA QUE SE ESTABLEZCA EN EL CONTRATO O DESDE LA FECHA EN QUE SE CUMPLAN LAS CONDICIONES PREVISTAS EN EL CONTRATO PARA EL INICIO DE LA EJECUCIÓN, DEBIENDO INDICAR LAS MISMAS EN ESTE ULTIMO CASO].

CLÁUSULA SEXTA: 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 SÉTIMA: 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.

Importante
Al amparo de lo dispuesto en el numeral 149.4 del artículo 149 del Reglamento de la Ley de Contrataciones del Estado, en el caso de contratos periódicos de prestación de servicios en general, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato original como garantía de fiel cumplimiento de contrato, debe consignarse lo siguiente: *"De fiel cumplimiento del contrato:* [CONSIGNAR EL MONTO]*, a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo."*

CLÁUSULA OCTAVA: 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 por el literal a) del numeral 155.1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por [CONSIGNAR EL ÁREA O UNIDAD ORGÁNICA QUE OTORGARÁ LA CONFORMIDAD] en el plazo máximo de [CONSIGNAR SIETE (7) DÍAS O MÁXIMO QUINCE (15) DÍAS, EN CASO SE REQUIERA EFECTUAR PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LA OBLIGACIÓN] días de producida la recepción.

De 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 cumpliese 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 servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD no otorga la conformidad, 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 conformidad del servicio por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de UN (1) AÑO contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

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

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

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;
F = 0.40 para plazos menores o iguales a sesenta (60) días.

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

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

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 CONTROVERSIAS[10]

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

El arbitraje será institucional y resuelto por TRIBUNAL ARBITRAL CONFORMADO POR TRES (3) ÁRBITROS. LA ENTIDAD propone las siguientes instituciones arbitrales: COLEGIO DE INGENIEROS DEL PERU (FILIAL PIURA) Y CAMARA DE COMERCIO DE PIURA.

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.

[10] 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).

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 Digitales[11].

[11] 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 Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 15-2024-GRP-ORA-CS-CP-1
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 Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento Nº [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[12]		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 servicios[13]

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.

[12] 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 consideración, en caso el postor ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, en los contratos periódicos de prestación de servicios, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento.

[13] Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

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

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 15-2024-GRP-ORA-CS-CP-1

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[14]		Sí		No	
Correo electrónico :					

Datos del consorciado 2					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[15]		Sí		No	
Correo electrónico :					

Datos del consorciado …					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[16]		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.

[14] En los contratos periódicos de prestación de servicios, 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 consideración, en caso el consorcio ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

[15] Ibídem.

[16] Ibídem.

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 servicios[17]

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.

[17] Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

ANEXO N° 2

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 15-2024-GRP-ORA-CS-CP-1

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 Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 15-2024-GRP-ORA-CS-CP-1

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 servicio de [CONSIGNAR OBJETO DE LA CONVOCATORIA], de conformidad con los Términos de Referencia 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 los términos de referencia, conforme a lo indicado en el acápite relacionado al contenido de las ofertas de la presente sección de las bases.

ANEXO Nº 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 15-2024-GRP-ORA-CS-CP-1
Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a prestar el servicio objeto del presente procedimiento de selección en el plazo de [CONSIGNAR EL PLAZO OFERTADO].

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 5

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 15-2024-GRP-ORA-CS-CP-1
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 al **CONCURSO PÚBLICO Nº 15-2024/GRP-ORA-CS-CP-1**

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]	[%][18]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]	
2.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2]	[%][19]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]	
	TOTAL OBLIGACIONES	100%[20]

[CONSIGNAR CIUDAD Y FECHA]

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

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

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

.....
Consorciado 1
Nombres, apellidos y firma del Consorciado 1
o de su Representante Legal
Tipo y N° de Documento de Identidad

.....
Consorciado 2
Nombres, apellidos y firma del Consorciado 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
CONCURSO PÚBLICO Nº 15-2024-GRP-ORA-CS-CP-1
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
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 servicio 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 Nº 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 15-2024-GRP-ORA-CS-CP-1
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [21]	FECHA DE LA CONFORMIDAD DE SER EL CASO[22]	EXPERIENCIA PROVENIENTE[23] DE:	MONEDA	IMPORTE[24]	TIPO DE CAMBIO VENTA[25]	MONTO FACTURADO ACUMULADO [26]
1										
2										
3										
4										

[21] Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.

[22] Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho periodo.

[23] Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Al respecto, según la Opinión N° 216-2017/DTN *"Considerando que la sociedad matriz y la sucursal constituyen la misma persona jurídica, la sucursal puede acreditar como suya la experiencia de su matriz"*. Del mismo modo, según lo previsto en la Opinión N° 010-2013/DTN, *"... en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad incorporada o absorbida, que se extingue producto de la fusión; asimismo, si en virtud de la escisión se transfiere un bloque patrimonial consistente en una línea de negocio completa, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante podrá emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe"*.

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

[25] El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.

[26] Consignar en la moneda establecida en las bases.

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [21]	FECHA DE LA CONFORMIDAD DE SER EL CASO[22]	EXPERIENCIA PROVENIENTE[23] DE:	MONEDA	IMPORTE[24]	TIPO DE CAMBIO VENTA[25]	MONTO FACTURADO ACUMULADO [26]
5										
6										
7										
8										
9										
10										
	...									
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

.....

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

ANEXO Nº 9

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 15-2024-GRP-ORA-CS-CP-1
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.*