

MINISTERIO DEL INTERIOR

CONCURSO PUBLICO N° 005-2022-IN-OGAF-OAB-PRIMERA CONVOCATORIA

SERVICIO DE INTERCONEXION, SEGURIDAD, ACCESO A INTERNET Y SERVICIO DE TELEFONIA FIJA
PARA EL MININTER

**BASES ESTÁNDAR DE CONCURSO PÚBLICO PARA LA
CONTRATACIÓN DE SERVICIOS EN GENERAL**

CONCURSO PÚBLICO N° 005-2022-IN-OGAF-OAB

PRIMERA CONVOCATORIA

**CONTRATACIÓN DE SERVICIO DE INTERCONEXION,
SEGURIDAD, ACCESO A INTERNET Y SERVICIO DE
TELEFONIA FIJA PARA EL MININTER**



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.

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

Importante

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

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

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

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

Advertencia

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

Importante

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

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

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>

Importante

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

1.8. 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 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.



Handwritten signature and stamp, possibly indicating approval or verification.

CAPÍTULO II SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

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

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

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

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

CAPÍTULO III DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

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

Handwritten signature and initials in the bottom left corner.

CAPÍTULO I GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre : MINISTERIO DEL INTERIOR
RUC N° : 20131366966
Domicilio legal : PLAZA 30 DE AGOSTO N° 150 – URB. CORPAC – SAN ISIDRO
Teléfono: : 225-3059
Correo electrónico: : Ogaf377@mininter.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del servicio de Interconexión, Seguridad, Acceso a Internet y Servicio de Telefonía Fija para el MININTER.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Formato N° 053-2022-APROB EXP de fecha 16 de agosto de 2022.

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 Mil Noventa y Seis (1096) días calendario contabilizados a partir del día siguiente de suscrito el **acta de implementación del servicio**, la cual será emitida por la Oficina de Servicios de Tecnologías y Comunicaciones (OSTC – OGTIC) en concordancia con lo establecido en el expediente de contratación.

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases de forma gratuita en la Oficina de Abastecimiento de la Dirección General de Administración y Finanzas del Ministerio del Interior, sito en Plaza 30 de Agosto N° 150 – Urb. Córpac – San Isidro.

Importante

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

1.10. BASE LEGAL

- Ley N° 31365– Ley de Presupuesto del Sector Público Para el Año Fiscal 2022.
- Ley N° 31366 - Ley de Equilibrio Financiero del Presupuesto del Sector Público para el Año Fiscal 2022
- Ley N° 31367 - Ley de Endeudamiento del Sector Público para el Año Fiscal 2022.
- Decreto Supremo N° 082-2019-EF, que aprueba el TÚO de la Ley N° 30225 Ley de Contrataciones del Estado, en adelante TÚO la Ley.
- Decreto Legislativo N° 1444 que modifica la Ley N° 30225.
- Decreto Supremo N° 344-2018-EF, que aprueba el Reglamento de la Ley de Contrataciones del Estado.
- Decreto Supremo N° 377-2019-EF, que modifica el Reglamento de la Ley de Contrataciones del Estado.
- Directiva N° 001-2019-OSCE/CD
- Decreto Supremo N° 004-2019-JUS, que aprueba el TÚO de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- Decreto Supremo N° 043-2003-PCM, que aprueba el TÚO de la Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública.
- Directivas del OSCE.
- Código Civil.

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

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

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

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

- 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 – PIDE³ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.

- 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**)

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

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

- e) Se deberá adjuntar la relación de equipos a utilizar indicando la marca, modelo y URL del fabricante.
- 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.

Incorporar a las bases o eliminar, según corresponda.

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

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.

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁵ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
 h) Detalle de los precios unitarios del precio ofertado⁶.
 i) Estructura de costos⁷.
 j) Presentación de otros documentos:

- El PROVEEDOR, debe entregar la estructura de costos desagregada por Componente, Sub Componente y Sede para la suscripción del contrato.
- Para el caso del servicio de Telefonía Fija, el PROVEEDOR, debe entregar la estructura de costos por tipo de llamada para la suscripción del contrato.
- EL PROVEEDOR debe presentar los números telefónicos de su Centro de Atención de Llamadas y/o Atención al Cliente.
- EL PROVEEDOR deberá presentar los documentos que acrediten el perfil profesional del personal indicado en el numeral VII.
- EL PROVEEDOR deberá presentar su estructura de costos en el siguiente formato:

COMPONENTE	SUB COMPONENTE	DESCRIPCIÓN	Costo por MB	Costo Mensual (S/)	Costo Anual (S/)	Costo Total 3 años (S/)
1 SERVICIO DE ACCESO A INTERNET EN LA SEDE PRINCIPAL	1	SERVICIO DE ACCESO A INTERNET EN LA SEDE PRINCIPAL				
		- Sede Central (Enlace Internet Principal)				
		- Sede Central (Enlace Internet Respaldo)				
	2	ADMINISTRADOR DE ANCHO DE BANDA				
2 SERVICIO DE SEGURIDAD GESTIONADA DE EQUIPOS PERIMETRALES.	1	SWITCH CORE EN ALTA DISPONIBILIDAD				
		NEXT GENERATION FIREWALL (NGFW) EN ALTA DISPONIBILIDAD				
	2	SOLUCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIOS SIMPLES Y DISTRIBUIDOS.				
		SISTEMA FIREWALL DE APLICACIONES WEB				
3 SERVICIO DE INTERCONEXIÓN PARA LAS SEDES DEL MININTER	1	SOLUCIÓN DE PROTECCIÓN DE AMENAZAS AVANZADAS EN ALTA DISPONIBILIDAD.				
		SERVICIO DE ACCESO A LA VPN-MININTER para la Sede Principal				
	2	- Sede Central (Enlace IPVPN Principal)				
		- Sede Central (Enlace IPVPN Respaldo)				
4 SERVICIO DE TELEFONÍA FIJA.	2	SERVICIO DE ACCESO A LA VPN-MININTER para las Sedes Remotas:				
		- Sede Remota 1 (Nombre de la Sede)				
	3	- Sede Remota 2 (Nombre de la Sede)				
		- Sede Remota 3 (Nombre de la Sede)				
		- Sede Remota N (Nombre de la Sede)				
		PLATAFORMA DE MONITOREO				
		TIPO DE LLAMADA		Costo por Segundo		
		Discado Directo Local				
		Discado Directo Nacional				
		Discado Directo Celular (Todos los operadores de telefonía móvil)				
		Discado Directo Internacional (Fijo Celular)				
		TOTAL				

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.

⁷ Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.

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 refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya⁸.*
- *La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en Mesa de partes del MININTER, sito en Plaza 30 de Agosto N° 150 – Urb. Córpac – San Isidro.

Importante

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

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 mensuales por 36 meses, siendo un pago fijo mensual correspondiente a 1/36 del monto del contrato original, para lo cual se empleará la siguiente fórmula:

$$\text{Pago Mensual} = (1/36) \times 100\% \times M$$

Donde:

M = Monto del Contrato Original

El pago se ejecutará una vez validada la conformidad del servicio y firmada el Acta de Implementación del Servicio.

Para efectos del pago de las contraprestaciones ejecutadas por el PROVEEDOR, este deberá presentar la documentación durante los primeros cinco (05) días posteriores al mes del servicio para de efectos de conformidad, para tal efecto la Entidad deberá contar con la siguiente documentación:

- Informe mensual (Entregables durante la vigencia del servicio), el mismo que se encuentra indicado en el numeral X. ENTREGABLES, del presente documento.
- Factura.

El MININTER realizará el pago de las contraprestaciones pactadas a favor del PROVEEDOR dentro de los diez (10) días calendarios siguientes de la conformidad dada por el área usuaria, siempre que se verifiquen las condiciones establecidas en la orden de servicio y/o contrato.

Dicha documentación se debe presentar en Mesa de partes del MININTER, sito en Plaza 30 de Agosto N° 150 – Urb. Córpac – San Isidro.

CAPITULO 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



PERU Ministerio del Interior

REQUERIMIENTO

A. TÉRMINOS DE REFERENCIA N° 003-2022-IN-OGTIC-OSTC

I. DENOMINACIÓN DE LA CONTRATACIÓN (Obligatorio)

Servicio de interconexión, seguridad, acceso a internet y servicio de telefonía fija para el MININTER.

II. OBJETIVO DE LA CONTRATACIÓN (Obligatorio)

Objetivo General:

Contratar un servicio integral de comunicaciones mediante una plataforma tecnológica segura, que utilice protocolos compatibles, para la transmisión de datos, voz, video e internet entre las distintas sedes del Ministerio del Interior a nivel nacional; permitiendo incorporar nuevas tecnologías para optimizar y elevar los niveles de eficiencia, y así contar con una red de alta calidad, segura y confiable.

Objetivos Específicos:

- Contar con un servicio dedicado de acceso a Internet para el MININTER
- Contar con un servicio de seguridad gestionada de equipos perimetrales para el MININTER
- Contar con un servicio de interconexión para las sedes del MININTER
- Contar con un servicio de Telefonía Fija para el MININTER

III. FINALIDAD PÚBLICA (Obligatorio)

La presente contratación tiene como finalidad proveer al Ministerio del Interior de una plataforma de comunicación oportuna y segura para optimizar sus labores asignadas en materia de orden interno y orden público, coadyuvando de esta forma a la mejor atención al ciudadano.

IV. ACTIVIDAD DEL POI (Obligatorio)

La presente contratación del servicio se encuentra enmarcada dentro del POI 2021 del Ministerio del Interior - Objetivo Estratégico Sectorial N° 4 – Mejorar la atención de los servicios que la ciudadanía demanda, Objetivo Estratégico Institucional N° 8: Fortalecer el Sistema Administrativo de Modernización de la Gestión Pública en el Ministerio del Interior, Acción Estratégica Institucional N° 8.1: Plataforma de interoperabilidad electrónica implementada a favor del ciudadano.

V. DESCRIPCIÓN DE LA CONTRATACIÓN (Obligatorio)

El servicio constará de los siguientes componentes

ÍTEM	COMPONENTE	SERVICIO
1	1	SERVICIO DE ACCESO A INTERNET EN LA SEDE PRINCIPAL (ANEXO A)
	2	SERVICIO DE SEGURIDAD GESTIONADA DE EQUIPOS PERIMETRALES.
	3	SERVICIO DE INTERCONEXIÓN PARA LAS SEDES DEL MININTER (ANEXO A Y B)
	4	SERVICIO DE TELEFONÍA FIJA.



Los equipos que requiera instalar el PROVEEDOR para la prestación del servicio, deben ser del tipo "appliance" - hardware dedicado específicamente diseñado para un propósito, en el que los fabricantes instalan sus softwares (firmware) y realizan la comercialización en una única solución. Así mismo, dichos equipos deben tener una antigüedad de fabricación no mayor de 12 meses contados a partir de la fecha de suscripción del contrato y deberán funcionar con la última versión de su software (firmware) vigente, debiendo el hardware tener un buen estado de conservación, no presentando partes con raspadura, rajadura, rotura, abolladura, perforación, ni óxido. Se precisa que todos los equipos del presente proyecto deberán ser nuevos y de primer uso. El estado de conservación de los equipos



Firmado digitalmente por:
MORAN REBATA Armando
Andres FAU 20131300000 soft
Motivo: Day V° 8°
Fecha: 20/07/2022 10:30:13-0500



Firmado digitalmente por:
REYES CAWPOS Marco
Aurelio FAU 20131300000 hard
Motivo: Day V° 8°
Fecha: 20/07/2022 10:34:45-0500



Firmado digitalmente por:
PARRA LEBRAN Miguel Joffre
FAU 20131300000 soft
Motivo: Day V° 8°
Fecha: 20/07/2022 10:47:54-0500



PERU Ministerio del Interior

será validado al momento de la instalación de cada equipo en el Centro de Datos del MININTER.

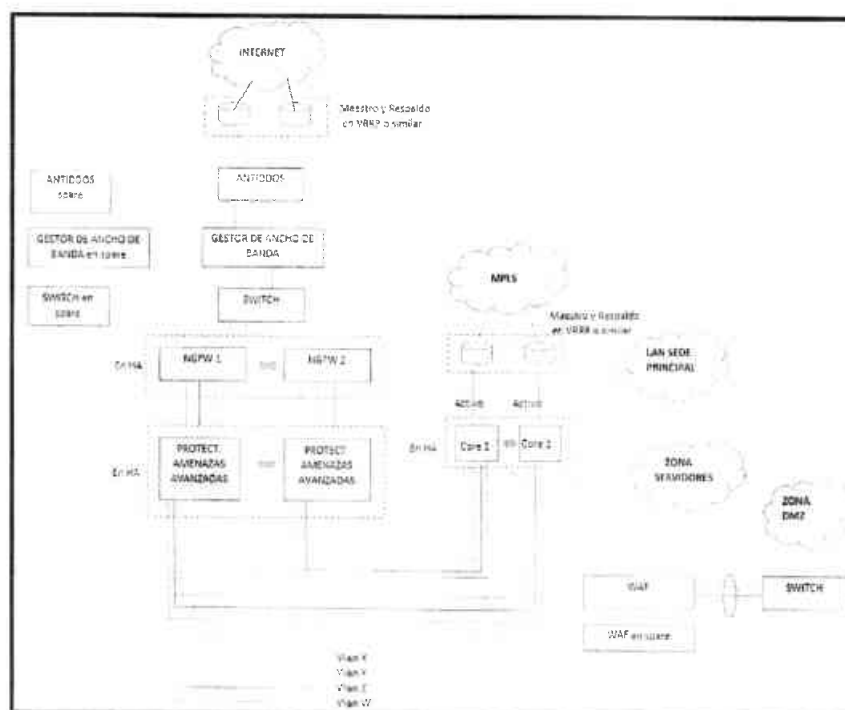
- ✓ Se precisa que: El Proveedor debe adjuntar en su propuesta, la relación de equipos a utilizar indicando la marca, modelo y url del fabricante, desde donde se validará que el equipo corresponde a un "appliance". La antigüedad de los equipos será validada durante la etapa de implementación del servicio, para lo cual el Proveedor deberá remitir a la Entidad, la documentación que permita acreditar fehacientemente la antigüedad de fabricación de cada equipo. Dicha validación también podrá realizarse a través de algún link o url del fabricante. La versión del software (firmware) instalado en cada equipo será validada durante el proceso de implementación mediante línea de comando o interfaz gráfica.
- ✓ La condición de nuevo y de primer uso deberá ser acreditada mediante DJ del Proveedor, carta del fabricante o cualquier otro documento que acredite fehacientemente tal condición. Dicha acreditación se realizará hasta antes de la suscripción del acta de implementación del servicio.
- ✓ En ningún caso, el PROVEEDOR entregará equipamiento cuya producción esté descontinuada por el fabricante, es decir, no deben estar en estado de fin de venta (EOS, End of Sale), ni en estado de fin de ciclo de vida (EOL, End of Live) por parte del fabricante, de los equipos necesarios para su operatividad hasta que finalice el servicio materia de la presente contratación. Se precisa que el cumplimiento de este requisito deberá ser acreditado mediante link o url o carta del fabricante, lo cual deberá ser presentada por el Proveedor hasta antes de culminar el plazo de implementación del servicio.
- ✓ En el caso que el fabricante de algún equipo provisto por el Proveedor, programe el EOS y/o EOL de dicho equipo, y dicha fecha de EOS y/o EOL se encuentre dentro del periodo de ejecución del servicio, el proveedor deberá garantizar el correspondiente soporte del fabricante, pudiendo facultativamente, efectuar el reemplazo del equipo por otro de igual o mejores características técnicas.
- ✓ El PROVEEDOR deberá proporcionar los recursos necesarios y ejecutar las actividades y tareas necesarias, a fin de brindar su operatividad en las diferentes sedes del MININTER. El servicio incluye la provisión, despliegue, habilitación, acondicionamiento, instalación, implementación, pruebas de la operatividad, y puesta en funcionamiento del servicio, el cual debe incluir todo concepto de gastos y tributos (a todo costo). Se precisa que el término "acondicionamiento" hace referencia a preparativos o arreglos necesarios para la implementación del servicio.
- ✓ Si al momento de la implementación del servicio, los equipos ofertados por el PROVEEDOR no se encuentran disponibles en el mercado, deberá reemplazarlos con equipos de iguales o mayores características técnicas, adjuntando el correspondiente sustento técnico documentado, con las validaciones técnicas del área usuaria.
- ✓ El PROVEEDOR será responsable de la operatividad de todos los componentes y sub componentes del servicio requerido, los cuales deberán estar disponibles y operativos las 24 horas del día, los 7 días a la semana y 365 días del año.
- ✓ El PROVEEDOR deberá trabajar de manera conjunta con el personal técnico de la Oficina de Servicios de Tecnología y Comunicaciones (En adelante OSTC), de la Oficina General de Tecnologías de Información y Comunicaciones (En adelante OGTIC) del MININTER, quienes supervisarán la implementación de los servicios correspondientes en los requerimientos. La OGTIC nombrará un responsable técnico del proyecto, quien será el encargado de las coordinaciones con el jefe de proyecto del PROVEEDOR, de modo que la implementación se ejecute en forma coordinada.
- ✓ Para los Servicios de los Componentes 1 y 3, los routers que el PROVEEDOR instale deben ser configurados con control de acceso centralizado mediante protocolo AAA (Autenticación, Autorización y Auditoría); y la configuración y gestión estará a cargo del



PERÚ Ministerio del Interior

PROVEEDOR, debiendo asignar al personal designado de la OGTC - MININTER una cuenta de usuario con nivel de lectura para fines de supervisión y monitoreo.

- ✓ Para el Servicio del Componente 2, la configuración y gestión estará a cargo del PROVEEDOR, debiendo asignar una cuenta de usuario con nivel Administrador para una gestión compartida al personal designado por el MININTER y una cuenta de usuario a nivel de lectura para fines de supervisión y monitoreo. Se precisa que, de comprobarse que una incidencia ha sido provocada por una configuración aplicada, con la cuenta de nivel de Administrador asignada a la Entidad, dicha incidencia no será atribuida al proveedor y por lo tanto, no generará penalidad para los supuestos de "exceso de tiempo de subsanación" y "nivel de disponibilidad de servicio".
- ✓ El PROVEEDOR para la firma del contrato, deberá presentar documentación técnica (brochures y/o datasheet y/o manuales y/o folletos, dichos documentos podrán ser presentados en su idioma original) en cumplimiento al artículo 59 del reglamento de contrataciones, donde evidencie el cumplimiento de las características técnicas mínimas de los equipos ofertados, para lo cual deberá adjuntar un cuadro comparativo de las características solicitadas versus las ofertadas y el número de folio donde se evidencia el cumplimiento. Adicionalmente y facultativamente, podrá presentar la carta emitida por el fabricante donde se confirme el cumplimiento de las características técnicas mínimas, que no pudieran ser evidenciadas en la documentación técnica, la misma que deberá estar acompañada de su debida traducción por traductor público juramentado o traductor colegiado, certificado, según corresponda.
- ✓ La topología de la solución requerida deberá estar basada en el siguiente diagrama referencial:



Cuadro N° 01: Topología de Red Requerida (Referencial)



PERU Ministerio del Interior

- ✓ El PROVEEDOR deberá proporcionar los equipos de comunicaciones, sus componentes y/o accesorios que resulten necesarios para establecer la topología propuesta, la misma que finalmente se debe conectar a los Switches Core provistos por EL PROVEEDOR.
- ✓ El PROVEEDOR asegurará que existan la cantidad de puertos disponibles necesarios en los Switches Core para la conexión de la solución propuesta. El PROVEEDOR deberá considerar la provisión de los transceiver y/o path cord que resulten necesarios. De acuerdo al diagrama propuesto (cuadro N° 01), toda la solución a implementar por parte del Proveedor deberá utilizar seis (06) puertos de red por cada Switch Core, sin embargo, deberá habilitar dos (02) puertos adicionales en cada Switch Core como reserva. El Proveedor, facultativamente podrá provisionar transceiver de cobre de 1 Gbps, en la medida que no afecte la conectividad con el resto de los equipos de la solución propuesta por el Proveedor, de acuerdo a la topología de red requerida e indicada en el cuadro N° 01.
- ✓ Para los componentes 1 y 3, el PROVEEDOR deberá disponer de un NOC (Centro de Operación de Red), propio o tercerizado, el cual se encargará del monitoreo, atención de incidencias y/o requerimientos de la solución instalada en la modalidad 7x24x365. En tal sentido, el NOC deberá generar de forma proactiva (sin necesidad de ser reportado por la Entidad) los correspondientes tickets de atención ante la ocurrencia de incidencias.
- ✓ Para el componente 2, el PROVEEDOR deberá disponer de un SOC (Centros de Operaciones de Seguridad), propio o tercerizado, el cual se encargará del monitoreo, gestión de eventos de seguridad, atención de incidencias y/o requerimientos en la modalidad 7x24x365. Los especialistas del SOC, analizarán e informarán a la Entidad las alertas de los equipos de seguridad descartando falsos positivos, los cuales se incluirán en los informes mensuales del servicio. El SOC en coordinación con la Entidad ejecutará todas las medidas necesarias para mitigar ciberataques dirigidos a la infraestructura TI del MININTER. En tal sentido, el SOC deberá generar de forma proactiva (sin necesidad de ser reportado por la Entidad) los correspondientes tickets de atención ante la ocurrencia de incidencias.
- ✓ En lo sucesivo, se entenderá por Alta Disponibilidad (o también llamado HA) a la capacidad de un sistema o componente del sistema, para estar continuamente operando ante la ocurrencia de una falla o avería (incidencia), lo cual se logra mediante la redundancia de equipos interconectados y será validado simulando el fallo de uno de ellos.
- ✓ Se precisa que los equipos de respaldo o "Spare" estarán ubicados en el centro de datos del MININTER, debidamente rackeados pero no energizados. Se encenderán para fines de actualización de la configuración, actualización del firmware, pruebas previamente coordinadas entre el Proveedor y la Entidad; y/o reemplazo del equipo principal en caso de avería.
- ✓ Todos los equipos provistos por el PROVEEDOR deben ser instalados en el Centro de Datos del MININTER, raqueados en dos (02) gabinetes de comunicaciones de 42RU cada uno. El PROVEEDOR deberá proporcionar todos los accesorios que resulten necesarios para ello.



PERU

Ministerio del Interior

5.1. COMPONENTE 1: SERVICIO DE ACCESO A INTERNET EN LA SEDE PRINCIPAL

El presente componente consta de tres (03) sub componentes de servicios

COMPONENTE 1: SERVICIO DE ACCESO A INTERNET EN LA SEDE PRINCIPAL	
SUB COMPONENTE	DENOMINACIÓN
1	Servicio de Acceso a Internet en la Sede Principal
2	Administrador de Ancho de Banda
3	Switch Core en alta disponibilidad

5.1.1. Sub Componente 1: Servicio de Acceso a Internet en la Sede Principal

- ✓ El PROVEEDOR deberá implementar un acceso a internet a través de un enlace dedicado con un ancho de banda de 365 Mbps, con tasa de acceso garantizada al 100% (overbooking 1:1), debiendo incluir un enlace de respaldo del mismo ancho de banda, empleando para ambos casos como medio físico, fibra óptica. Se precisa que la fibra óptica y el equipamiento que será utilizado en la implementación de cada uno de los medios de transmisión para la provisión del servicio deberán ser nuevos y de primer uso.
- ✓ El enlace de respaldo de acceso a Internet deberá estar configurado en modo pasivo, el cual se deberá activar de manera automática, en caso ocurra una caída del enlace principal, manteniendo el mismo ancho de banda. El enlace de respaldo partirá desde un nodo diferente del enlace principal y tener una ruta diferente al utilizado por el enlace principal, para lo cual el PROVEEDOR deberá adjuntar a su informe final de implementación del servicio, el plano impreso en tamaño A2 o superior, donde se muestre las rutas a seguir y el nombre del PoP al que se conecta. El PROVEEDOR deberá garantizar que la ruta física de la fibra óptica y nodo (PoP) deben ser diferentes entre el enlace principal y el enlace de contingencia.
- ✓ El PROVEEDOR debe garantizar que el ancho de banda proporcionado sea el mismo desde la puerta de enlace hasta la salida internacional.
- ✓ El PROVEEDOR deberá garantizar la Alta Disponibilidad de los Enlaces de Internet, debiendo proveer los equipos que sean necesarios para tal fin.
- ✓ El PROVEEDOR debe estar autorizado por el Ministerio de Transportes y Comunicaciones - MTC para proveer servicios de transmisión de datos y/o Internet.
- ✓ El PROVEEDOR deberá contar como mínimo con dos (02) servidores DNS redundantes, donde se deberá registrar las direcciones IP públicas del MININTER. Los servidores DNS deberán soportar publicaciones en IPv4 e IPv6. Se precisa que los DNS redundantes deberán estar ubicados en diferentes locales y/o zonas geográficas.
- ✓ El servicio deberá estar preparado para migrar a velocidades mayores de la solicitada, soportando un crecimiento de hasta el 50% de la velocidad solicitada (Ejemplo: 550 Mbps). Se precisa que los incrementos de ancho de banda serán tratados de acuerdo a ley mediante una Adenda.
- ✓ El PROVEEDOR deberá brindar equipos (routers) que soporten un crecimiento de hasta el 50% del ancho de banda solicitado. Cada enlace deberá tener su propio router (principal y respaldo). El Proveedor, facultativamente podrá ofrecer equipos que soporten un mayor crecimiento de ancho de banda.
- ✓ El PROVEEDOR proporcionará como mínimo sesenta y cuatro (64) direcciones IPs públicas para IPv4 y sesenta y cuatro (64) direcciones IPs públicas para IPv6, para la publicación de los servicios de la Entidad, con la capacidad de aumentar hasta el doble de acuerdo a los



PERÚ Ministerio del Interior

requerimientos de la Entidad y sin costo adicional para el MININTER. Se precisa que en el pool de sesenta y cuatro (64) direcciones IPs públicas versión 4 están incluidas las 5 IPs por defecto (IP de red, IP de gateway de ambos enlaces, IP virtual e IP de broadcast) quedando disponibles cincuenta y nueve (59) direcciones IPs públicas versión 4.

- ✓ El servicio de Internet incluirá todo el equipamiento, conectores, cables, componentes y materiales necesarios para la interconexión con los equipos de seguridad perimetral y/o equipos de comunicación en alta disponibilidad de la Entidad.
- ✓ La disponibilidad mensual del servicio de acceso a internet en la sede principal, no debe ser menor a 99.95% lo cual será verificado aplicando la siguiente fórmula:

$$\text{Disponibilidad} = \left(\frac{THM - \sum \text{Tiempo Imputable}}{THM} \right) \times 100$$

Donde:

- THM=Total de Horas del Mes
- TPR=Tiempo de parada de reloj

El tiempo de parada de reloj se define como aquel tiempo en el cual, notificada la avería por la Entidad, ésta no logra brindarle al PROVEEDOR las facilidades de acceso a sus equipos ubicados en las instalaciones de la Entidad.

- TTA=Tiempo Total de Avería

El Tiempo Total de Avería se define como el tiempo transcurrido desde que se le notifica al PROVEEDOR respecto a la avería presentada, hasta el momento en el que el PROVEEDOR soluciona o resuelve la avería.

- Tiempo Imputable=(TTA-TPR)

5.1.2. Sub Componente 2: Administrador de Ancho de Banda

- ✓ El PROVEEDOR debe brindar dos (02) equipos (appliances), para la gestión y administración del ancho de banda de los enlaces de Internet, donde uno (01) de ellos estará en calidad de respaldo o "Spare", se precisa que los equipos no estarán en alta disponibilidad (activo-pasivo o activo-activo). Ambos equipos deben ser de la misma marca y modelo.
- ✓ Los equipos deben permitir visualizar a nivel de aplicación y protocolos el consumo de tráfico, así como también, la aplicación de políticas de Calidad de Servicio y Priorización de Tráfico.
- ✓ Los equipos no deben estar embebidos sobre enrutadores, firewalls, NGFW y/o UTM.



PERU

Ministerio del Interior

EQUIPO DE ADMINISTRADOR DE ANCHO DE BANDA**CANTIDAD: DOS (02)**

DESCRIPCIÓN	DETALLES TECNICOS
Capacidad	<ul style="list-style-type: none"> Deberá contar como mínimo con dos (02) bridges, es decir 4 puertos de 1GbE; con bypass interno que impida la interrupción ante eventos de falla por energía del equipo. Deberá estar licenciado para poder gestionar 550 Mbps de throughput simétrico (bajada y subida) inicialmente, y con capacidad de poder incrementar (con licenciamiento adicional) a 1 Gbps de throughput por lo menos. Respecto al licenciamiento, es responsabilidad del proveedor garantizar la continuidad y calidad del servicio durante la vigencia del contrato, para lo cual deberá tomar todas las previsiones del caso. Deberá soportar como mínimo 200 mil flujos concurrentes. Deberá soportar como mínimo 200 mil paquetes por segundo. Deberá contar con al menos 3,000 aplicaciones identificadas. También se aceptará que el equipo de administración de ancho de banda deberá soportar como mínimo 10 niveles de priorización y permitir la agrupación de aplicaciones según su naturaleza y criticidad según se requiera y capacidad de asignar cuotas (GB) por usuario.
Funcionalidades	<ul style="list-style-type: none"> La solución deberá proveer la funcionalidad de Calidad de Servicio (QoS) para proteger el ancho de banda de aplicaciones críticas y contener el tráfico no deseado tanto en IPv4 e IPv6. Las políticas o reglas de control de ancho de banda deben permitir: priorización de tráfico, definir un mínimo ancho de banda garantizado y un máximo de ancho de banda permitido. También se aceptará que la solución propuesta tenga la capacidad de entregar en el administrador de ancho de banda los servicios de visibilidad, control, aceleración y caché en la misma unidad. Deberá contar con la funcionalidad de distribución de tráfico equitativo, la cual reparte el ancho banda por igual entre todos los dispositivos conectados. Este cálculo de repartición se realiza de forma dinámica constantemente, no es un valor estático y podrá ejecutarse para el tráfico excedente luego de que se haya priorizado las aplicaciones críticas de la Entidad. Posibilidad de crear múltiples políticas de control independientes entre sí, para las distintas áreas de la Entidad. Deberá soportar la creación de políticas basadas en tiempo. Los periodos se pueden configurar de acuerdo a las necesidades de la Entidad. La solución deberá integrarse con el Directorio Activo (AD) de la Entidad con la finalidad de manejar políticas basadas en usuarios. Permitir la creación de aplicaciones personalizadas de la propia Entidad para su visibilidad y control. Estas aplicaciones se podrán crear a través de IP y/o puerto y/o URL. Deberá agrupar aplicaciones en categorías existentes y/o personalizadas como: redes sociales, P2P, actualizaciones de software, video y música. Así como también se debe poder crear grupos de aplicaciones personalizadas.
Monitoreo y Administración	<ul style="list-style-type: none"> Deberá considerar una consola de administración gráfica en el mismo equipo que permita administrar, configurar y generar reportes del equipo Administrador de Ancho de Banda. Se deberá poder mostrar información de reportes al menos de los últimos 12 meses. Monitoreo en tiempo real con actualizaciones de como mínimo 5 segundos, que permita realizar un análisis de tráfico en profundidad hasta la búsqueda de una estación de trabajo y un servicio específico, para el diagnóstico de problemas y cuellos de



PERU Ministerio del Interior

EQUIPO DE ADMINISTRADOR DE ANCHO DE BANDA**CANTIDAD: DOS (02)**

DESCRIPCIÓN	DETALLES TÉCNICOS
	<p>botella en la red.</p> <ul style="list-style-type: none"> La solución debe contar con un dashboard y/o también se aceptará visualizador de tráfico mediante gráficos y tablas y/o reportes, que muestre en tiempo real y en simultáneo distintos gráficos de indicadores del comportamiento y consumo de la red Minimamente se requiere tráfico total, aplicaciones de mayor consumo, IP internas o usuarios de mayor consumo, IP externas de mayor consumo y el desempeño de la calidad de las aplicaciones (dependiendo del fabricante este último indicador puede llamarse score de aplicaciones, salud de aplicaciones, entre otros) La solución deberá mostrar estadísticas del tráfico de descarga y de subida en un periodo de tiempo configurable Deberá permitir la generación reportes basados en gráficos en los cuales se muestre el consumo por IP, subred, aplicaciones, usuarios (requiere integración con el Directorio Activo). El equipo deberá permitir el envío de alarmas por medio de email y por traps (snmp). Opcionalmente, el equipo podrá tener la capacidad de monitorear y asociar alertas en la medición de la cantidad de flujos concurrentes iniciados. Conexiones TCP abortadas, ignoradas y rechazadas. Además de que el reporte solicitado sea sobre el estado de salud TCP. El equipo deberá poder conectarse con el servidor de actualizaciones del fabricante para que pueda descargar e instalar las actualizaciones remotamente. De esta forma se garantizará que el equipo siempre se encuentre actualizado con la última versión publicada por el fabricante. El equipo debe soportar la exportación de información a aplicaciones de colección externa a través de NetFlow, donde el puerto de envío UDP sea configurable. El equipo debe garantizar el almacenamiento de datos en su disco duro interno de por lo menos los últimos 12 meses, independiente de la presencia de un sistema de colección externa, para la posterior generación de reportes y estadísticas. El software para el manejo de reportes y acceso a la consola de gestión del equipo debe ser provisto en el mismo appliance sin utilizar hardware (servidor) ni software adicional, ni virtualizando el equipo. Se precisa que el hardware y software solicitado debe ser integrado y soportado en su totalidad directamente por un mismo fabricante y que no se aceptará alguna solución de tipo software que dependa de sistemas operativos genéricos (Windows o Linux) que deban ser instalados previamente. Opcionalmente el postor podrá brindar una certificación otorgada directamente por el fabricante. Capacidad de limitar el acceso a la consola de gestión web del equipo para un grupo definido de direcciones IP, previniendo el acceso no autorizado al equipo. Se aceptará también que el equipo cuente con una interface de red exclusiva para la gestión del equipo, conectada a una red de administración (diferente de la red del tráfico a administrar).
Otras consideraciones	<ul style="list-style-type: none"> El soporte del equipo de administración de ancho de banda debe ser integral realizado por el PROVEEDOR quien deberá realizar el soporte tanto del hardware como del software como parte del servicio y este contactará con el fabricante para el debido soporte, en caso sea necesario mediante su centro de operaciones o centro



PERÚ Ministerio del Interior

EQUIPO DE ADMINISTRADOR DE ANCHO DE BANDA

CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	<p>de servicios.</p> <ul style="list-style-type: none"> El PROVEEDOR deberá gestionar el servicio de administración de ancho de banda, realizando las configuraciones en coordinación con el personal designado de la Entidad. Asimismo, dicho servicio debe asegurar la misma disponibilidad que el servicio de internet y bajo las mismas penalidades en caso de incumplimiento. La configuración y gestión estará a cargo del PROVEEDOR, debiendo asignar al personal designado del MININTER una cuenta con nivel de escritura y una cuenta con nivel de lectura para fines de supervisión, monitoreo y generación de reportes. Estos usuarios serán distintos a los que tendrá el PROVEEDOR del servicio. El servicio incluirá todo el equipamiento, conectores, cables, componentes y materiales necesarios para la interconexión con los equipos de seguridad perimetral y/o equipos de comunicación en alta disponibilidad de la Entidad.
Inducción	<p>Se deberá proporcionar un entrenamiento en administración, configuración básica del equipo y resolución de problemas, el cual estará dirigido a 04 profesionales de la OSTC, con un tiempo mínimo de duración de 12 horas, a realizarse de manera presencial en las instalaciones de la Entidad o de manera virtual (en línea con el expositor), dentro del plazo de implementación (120 días calendarios) establecido en el numeral VIII. PLAZO DE EJECUCIÓN DE LA PRESTACIÓN, siendo el expositor, personal certificado por el fabricante del equipo propuesto. Se deberá entregar certificados de participación a los profesionales designados por la OSTC.</p>

5.1.3. Sub Componente 3: Switch Core

- ✓ El PROVEEDOR debe brindar dos (02) equipos SWITCH CORE con las siguientes características técnicas mínimas

EQUIPO DE SWITCH CORE EN ALTA DISPONIBILIDAD

CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
Hardware	<ul style="list-style-type: none"> Switches Core de tipo Chasis. Número de slots: 04 Número de slots para tarjetas: 02 Numero de slots de supervisión: 02 Redundancia de supervisión: Si Ancho de banda por slot : 480 Gbps Numero de bahías para energía: 04 Número de bahías para ventiladores: 01 Unidades de rack: 6 RU Tarjeta de línea para Fibra: 01 tarjeta de 48 puertos Tarjeta de línea para Cobre: 01 tarjeta de 48 puertos 10/100/1000 (RJ-45) Deberá tener un puerto de administración fuera de banda, tipo RJ-45 Deberá tener un puerto serial tipo RS-232 o RJ45 o micro USB Deberá tener un puerto tipo USB Todos los puertos deberán soportar tasas completas (full rate) independiente al tamaño depaquetes transmitidos



PERU Ministerio del Interior

EQUIPO DE SWITCH CORE EN ALTA DISPONIBILIDAD**CANTIDAD: DOS (02)**

DESCRIPCION	DETALLES TÉCNICOS
	<ul style="list-style-type: none"> • Deberá tener instalado un sistema de alimentación de energía redundante con capacidad de ser retirado en caliente (Hot Swap) • Las fuentes de energía deberán soportar 200-240 VAC a 60 Hz. • Se deberán incluir los cables de energía eléctrica con terminación tipo C13 (tomas de energía utilizadas dentro del Centro de Datos) • Soporte de fabricante, el cual garantice una atención con el centro de soporte de fabricante 24x7 y reemplazo de partes, con tiempo de respuesta menor a 4 horas. EL CONTRATISTA ganador deberá gestionar la atención al centro de Soporte del fabricante.
Funcionalidades	<ul style="list-style-type: none"> • Toda funcionalidad de software, establecida para el funcionamiento del switch de red y que cumpla con las características técnicas descritas a continuación, deberá contar con el respectivo licenciamiento y la capacidad de actualizarse sin incurrir en costos adicionales para la entidad, durante el plazo de responsabilidad del CONTRATISTA. • Contar con la última versión estable del sistema operativo recomendado por el fabricante, la cual se deberá actualizar durante el plazo máximo de responsabilidad del CONTRATISTA, sin que ello incurra en costos adicionales para la entidad. • Contar con un sistema operativo modular, que permita la separación del plano de control y del plano de datos. • Permitir exportar copias de seguridad de configuración mediante FTP o SFTP, TFTP y/o USB y SCP. • Soporte de interfaces de programación de aplicación abiertas (APIs) y scripting. • Deberá tener licenciamiento habilitado para las tecnologías de enrutamiento y switching tales como BGP, GRE o IS-IS, MSDP, OSPF, PBR, PIM SSM o PIM SM, VRF, VXLAN, EVPN o SRv6. • Capacidad instalada de Balanceo de carga persuasivo y Ruteo Tenant multicast o ECMP • Deberá tener la capacidad de operar en diversos modos, tales como: Core, Agregación y Gateway. • Deberá soportar la carga del firmware y/o parches de seguridad en caliente, es decir, sin que sea necesario desconectar el switch de la red, detener servicios para el usuario final o apagar el equipo, siempre que se defina una alta disponibilidad. • Operatividad en capa 2 y capa 3. • Soporte para enrutamiento basado en políticas (PBR). • Soporte para listas de Control de Acceso en Capa 2 (ingress) y 3 (ingress y egress): 700 entradas de ingreso y 1000 entradas de egreso. • Rutas IPv4 multicast: 4,094 • Entradas de MAC: 98,000 • Numero de Port Channels o enlaces agregados: 32 • Número de VLAN: 4040 • Número de instancias VRF: 256 • Enrutamiento unicast, multicast basado en hardware, es decir, que utilice recursos de hardware destinados para tal finalidad, sea mediante ASIC o mecanismos de reservación de recursos de hardware del sistema.
Cumplimiento de normas, Estándares	<ul style="list-style-type: none"> • RFC-791 IPv4 • RFC-792 ICMP • RFC-793 TCP • RFC-826 ARP • RFC-8200 o IPv6



PERU

Ministerio del Interior

EQUIPO DE SWITCH CORE EN ALTA DISPONIBILIDAD

CANTIDAD: DOS (02)

DESCRIPCION	DETALLES TÉCNICOS
	<ul style="list-style-type: none"> • RFC-1901 o SNMPv2c • RFC-3414 SNMPv3 • RFC-2328 OSPFv2 • RFC-5340 OSPFv3 • RFC-2453 RIPv2 • RFC-1105 BGP o BGP4 • RFC-4271 BGP-4RFC-5798 VRRP • RFC-7348 VXLAN • RFC-7432 BGP MPLS-Based Ethernet VPN (EVPN) o EVPN • RFC-2236 IGMP v2 • RFC-3376 IGMP v3 • RFC-7761 PIM-SM • RFC-1256 IPv4 ICMP Router Discovery • RFC-2138 o RFC-2865 o RADIUS Authentication • RFC-2139 o RFC-2866 o RADIUS Accounting • IEEE 802.3ab 1000BASE-T, Gigabit sobre cobre. • IEEE 802.3z 1000BASE-X, Gigabit sobre fibra. • IEEE 802.3ae 10 Gigabit Ethernet • IEEE 802.3ba 40/100 Gigabit Ethernet • IEEE 802.1d, STP • IEEE 802.1q, trunking • IEEE 802.1s, MSTP • IEEE 802.1w, RSTP • IEEE 802.1ab LLDP • IEEE 802.3ad, LACP • IEEE 802.3x, Control de flujo. • IEEE 802.1p o PCP, Calidad de Servicio y DSCP
Gestión y Monitoreo	<ul style="list-style-type: none"> • Administración remota mediante SSH versión 2, HTTPS • Administración local mediante conexión serial. • Permitir múltiples sesiones simultáneas de conexión remota. • Permitir múltiples niveles de privilegios de acceso. • Registro de eventos vía Syslog y Syslog Remoto. • Soporte de protocolos de transferencia de archivos TFTP y/o SFTP. • Soporte para permitir procesos de debug para el análisis detallado de fallas y tráfico de datos. • Soporte para contar con herramientas que permitan recolectar datos para el análisis de tráfico en tiempo real. Debug de paquetes, Consulta a Tabla ARP, etc. Dichas herramientas podrán ser internas (mediante el switch de red) y/o externas (mediante una consola de gestión). • Análisis de tráfico usando protocolos tipo Netflow y/o sFlow en todos los puertos de los switches, sin que ello impacte en el procesamiento del equipo. • Brindar la funcionalidad de "puerto espejo" por puerto físico o grupo de puertos. • Soporte de diagnóstico mediante línea de comandos, que permita verificar el hardware usando diferentes pruebas predefinidas en demanda o calendarizadas.
Accesorios que deben incluirse (por cada switch core)	<ul style="list-style-type: none"> • Cuatro (04) TRANCEIVERS 100G SFP Base-SR para fibra óptica tipo multimodo OM4 con conector LC. • Cuatro (04) TRANCEIVERS 40G SFP Base-SR para fibra óptica tipo multimodo OM4 con conector LC. • Doce (12) TRANCEIVERS 10G SFP Base-SR para fibra óptica tipo multimodo OM3 y OM4 con conector LC.



PERÚ

Ministerio del Interior

EQUIPO DE SWITCH CORE EN ALTA DISPONIBILIDAD CANTIDAD: DOS (02)	
DESCRIPCIÓN	DETALLES TÉCNICOS
	<ul style="list-style-type: none"> Doce (12) TRANCEIVERS 1G SFP Base-SR para fibra óptica tipo multimodo OM3 con conector LC. Cuarenta y ocho (48) TRANCEIVERS 1G Base-T para cableado UTP categoría 6. Cuatro (04) Cables de fibra óptica con conector LC/LC OM4 (soporte de 100 Gbps) de 3 mt de longitud. Cuatro (04) Cables de fibra óptica con conector LC/LC OM4 (soporte de 40 Gbps) de 3 mt de longitud.
Condiciones mínimas de la instalación	<ul style="list-style-type: none"> Los switches de red deberán ser configurados en una topología de alta disponibilidad activo-activo dentro del Centro de Datos y con los parámetros de red (direccionamiento IP versión 4 y versión 6) que el MINISTERIO disponga (Dual Stack). Se deberá trasladar la configuración de los switches Core a satisfacción del Ministerio. Los switches de red deberán ser configurados con los parámetros de enrutamiento que el MINISTERIO defina, debiendo restablecer la conectividad hacia la red de servidores, red de distribución, la Internet y redes remotas de usuarios. Los switches de red deberán ser configurados con los parámetros SNMPv2c y SNMPv3 que el MINISTERIO disponga. Los switches de red deberán ser configurados con los parámetros de ruteo hacia los switches de distribución que el MINISTERIO disponga. Al finalizar el contrato, estos equipos Switch Core pasarán a ser propiedad del Ministerio sin costo adicional, debiendo coordinar con el Ministerio el procedimiento para la transferencia de la propiedad.
Inducción	Se deberá proporcionar un entrenamiento en administración, configuración básica del equipo y resolución de problemas, el cual estará dirigido a 04 profesionales de la OSTC, con un tiempo mínimo de duración de 12 horas, a realizarse de manera presencial en las instalaciones de la Entidad o de manera virtual (en línea con el expositor), dentro del plazo de implementación (120 días calendarios) establecido en el numeral VIII. PLAZO DE EJECUCIÓN DE LA PRESTACIÓN, siendo el expositor, personal certificado por el fabricante del equipo propuesto. Se deberá entregar certificados de participación a los profesionales designados por la OSTC.

5.2. COMPONENTE 2: SERVICIO DE SEGURIDAD GESTIONADA DE EQUIPOS PERIMETRALES.

El presente componente consta de cuatro (04) subcomponentes de servicios

COMPONENTE 2: SERVICIO DE SEGURIDAD GESTIONADA DE EQUIPOS PERIMETRALES	
SUB COMPONENTE	DENOMINACIÓN
1	NEXT GENERATION FIREWALL (NGFW) EN ALTA DISPONIBILIDAD.
2	SOLUCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIOS SIMPLES Y DISTRIBUIDOS.
3	SISTEMA FIREWALL DE APLICACIONES WEB.
4	SOLUCIÓN DE PROTECCIÓN DE AMENAZAS AVANZADAS EN ALTA DISPONIBILIDAD.



PERU Ministerio del Interior

5.2.1. Sub Componente 1: Next Generation Firewall (NGFW) en Alta disponibilidad

- ✓ El PROVEEDOR debe brindar dos (02) equipos Next Generation Firewall (NGFW) con las siguientes características técnicas mínimas.

NEXT GENERATION FIREWALL (NGFW) EN ALTA DISPONIBILIDAD CANTIDAD: DOS (02)	
DESCRIPCIÓN	DETALLES TÉCNICOS
Características Next Generation Firewall (NGFW)	<p>Dos (02) Equipos Next Generation Firewall (NGFW) de tipo hardware (appliance), del mismo fabricante y del mismo modelo.</p> <p>Debe incluir como mínimo:</p> <ul style="list-style-type: none">- Prevención de amenazas.- Análisis de Malware.- Control de Aplicaciones.- Filtrado URL.- Identificación de Usuarios.- Filtro de Datos.- VPN IPsec y VPN SSL.- Análisis de tráfico cifrado.
Modos HA	Como mínimo Activo/Pasivo, Activo/Activo.
Fail Over	Se podrá configurar como mínimo mediante supervisión de interfaces y supervisión de rutas.
Throughput	<p>Características técnicas mínimas en tráfico y sesiones:</p> <ul style="list-style-type: none">- 15 Gbps Next Generation Firewall throughput (*)- 7.2 Gbps Threat Prevention throughput (**)- 9 Gbps IPSEC VPN throughput (***)- 4 millones de sesiones o conexiones concurrentes <p>(*) Sera medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones o transacciones medidas en condiciones empresariales), con las siguientes funcionalidades habilitadas simultáneamente: Firewall, Control de aplicaciones y Logging activo.</p> <p>(**) Sera medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones o transacciones medidas en condiciones empresariales), con las siguientes funcionalidades habilitadas simultáneamente: Firewall, Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/Anti-Bot, prevencion de amenazas avanzadas de día cero (Sandboxing), Filtrado de URL y Logging activo.</p> <p>(***) Sera medido sobre transacciones 64 KB HTTP o empleando protocolo AES-128.</p> <p>Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección.</p>



PERU

Ministerio del Interior

NEXT GENERATION FIREWALL (NGFW) EN ALTA DISPONIBILIDAD
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
Interfaces de Red	<p>Como mínimo 8 interfaces de red con la capacidad de operar a 1 Gbps, se precisa que el proveedor deberá provisionar 8 interfaces de red (fibra o cobre) de 1Gbps, las cuales deben integrarse a la infraestructura de acuerdo a la topología de red requerida en el presente TDR</p> <p>Como mínimo con 1 interfaz de red dedicado para la administración, la cual tendrá la capacidad de operar a 1 Gbps.</p> <p>Debe contar como mínimo 1 interfaz de tipo consola o similar.</p> <p>Capacidad de operar en 03 modos de manera simultánea mediante el uso de sus interfaces físicas, modo sniffer o tap (monitoreo y análisis del tráfico de la red), capa 2 (L2) y capa 3 (L3).</p> <ul style="list-style-type: none"> Modo sniffer, para inspección vía un puerto espejo del tráfico de datos de la red. Modo capa 2 (L2), para inspección de datos en línea y tener visibilidad y control del tráfico a nivel aplicación. Modo capa 3 (L3), para inspección de datos en línea y tener visibilidad y control del tráfico a nivel aplicación. Modo de trabajo mezclado sniffer, L2 y L3 en diferentes interfaces físicas. Generar ruteo virtual para al menos 10 ruteadores virtuales, manejo de tráfico entre diferentes zonas de seguridad, subredes, soportando al menos 80 zonas de seguridad y un mínimo de 10 sistemas virtuales. (licenciado)
Protocolo IP	<ul style="list-style-type: none"> Todas las funciones Next Generation Firewall (NGFW) deben poder soportar las versiones IPv4 e IPV6. Debe permitir descifrar el tráfico entrante y saliente. Debe soportar TLS 1.3 Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar las claves privadas, para evitar un uso indebido por parte de los administradores.
Prevención de Amenazas (virus, malware y spyware)	<p>Deberá realizar protección contra amenazas de red, bloqueo de virus, spyware, control de transferencia de archivos, control de la navegación en internet y bloqueo de archivos por tipo.</p> <p>Deberá incluir protección contra virus en contenido web y javascript, software espía y gusanos.</p> <p>Protección contra descargas de archivos ejecutables maliciosos a través de protocolo HTTP y HTTPS.</p> <p>Escaneo de virus en protocolos HTTP, HTTPS, SMTP, POP3 y SMB como mínimo.</p>



PERÚ

Ministerio del Interior

NEXT GENERATION FIREWALL (NGFW) EN ALTA DISPONIBILIDAD
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	<p>Deberá permitir la inspección en archivos comprimidos que usan algoritmo deflate (zip, gzip, etc).</p> <p>Como mínimo deberá soportar el bloqueo de 50 tipos de archivos.</p> <ul style="list-style-type: none"> La actualización de firmas de ataques deberá ser diaria y/o semanal y/o de emergencia. Las firmas deberán estar basadas en patrones del malware y/o hashes. <p>Deberá incluir los siguientes mecanismos de IPS basados en:</p> <ul style="list-style-type: none"> Análisis de patrones de estado. Análisis de decodificación de protocolo. Análisis para detección de anomalías de protocolo. Análisis heurístico. IP desfragmentación. Re ensamblado de paquetes de TCP. Permita el diseño de firmas de vulnerabilidades. Identificación de botnet por comportamiento. Identificación de malware moderno, basado en un sistema de detección en la nube.
Control de acceso a internet y transmisión de datos	<p>Deberá contar con herramientas de visibilidad que permitan administrar el tráfico de aplicaciones, permitiendo la ejecución de aplicaciones autorizadas.</p> <p>Deberá incluir como mínimo la capacidad de actualización para identificar nuevas aplicaciones.</p> <p>Deberá incluir como mínimo la capacidad de creación de políticas basadas en la visibilidad y control de quien esté usando qué aplicaciones, a través de la integración con servicios de directorio. Autenticación via ldap, directorio activo y base de datos local.</p> <p>Deberá incluir la capacidad de creación de políticas basadas en el control por aplicación, categoría de aplicación, sub-categoría, tecnología y factor de riesgo.</p> <p>Deberá incluir la capacidad de creación de políticas basadas en el control por usuario, grupos de usuarios o dirección IP.</p> <p>Deberá incluir la capacidad de creación de políticas basadas en "traffic shaping" por aplicación, usuario, fuente, destino, túnel vpn-ipsecc-ssl.</p> <p>Deberá permitir el control, sin instalación de cliente de software, en equipos que soliciten salida a internet para que antes de iniciar la navegación, se despliegue un portal de autenticación residente en el firewall (captive portal) con soporte a autenticación por client certificate.</p> <ul style="list-style-type: none"> Soporte a autenticación kerberos. Como mínimo la solución deberá ser capaz de detectar los



PERU

Ministerio del Interior

NEXT GENERATION FIREWALL (NGFW) EN ALTA DISPONIBILIDAD
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	<p>siguientes ataques complejos de DNS (incluso el dominio no sea conocido por la inteligencia de amenazas del fabricante): DNS Tunneling, Domain Generation Algorithm (DGA), Anonimizadores.</p> <p>La actualización de la base de datos debe ser automática con opción a hacerla manual vía tftp.</p> <p>Identificación, control (uso de aplicaciones por usuario mediante interacción con LDAP, Directorio Activo o Radius y Dirección IP) y visibilidad de al menos 950 aplicaciones incluyendo peer-to-peer, Facebook, Twitter y Web 3.0. Esta identificación debe ser de manera independiente al puerto lógico y/o aplicaciones que usan los puertos 80 y 443. La identificación de aplicaciones también puede ser a través de una base de datos de firmas de aplicaciones, en estos casos, deberá soportar más de 9,000 aplicaciones identificadas.</p>
Filtrado URL	<p>Deberá contar con una base de datos local en el dispositivo de filtrado de URL.</p> <p>Debe incluir la capacidad de creación de políticas basadas en la visibilidad y control de quién está utilizando cual URLs a través de la integración de directorio activo, autenticación vía LDAP, Active Directory, y base de datos locales.</p> <p>Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL.</p> <p>Debe soportar un cache local de URL en el dispositivo, evitando el delay de la comunicación / validación de las URLs.</p> <p>Debe poseer como mínimo 60 categorías de URLs, que protejan como mínimo de: Phishing, SPAM, Botnets, Anonymizer, Hacking, Inactive Sites y Spyware/ Malicious Sites.</p> <p>Debe soportar la creación de categorías de URL custom.</p> <p>Debe soportar la exclusión de URLs del bloqueo por categoría.</p> <p>Se podrá configurar una página de bloqueo y permitir la customización.</p> <ul style="list-style-type: none"> • Debe soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuarios. • Deberá contar con un módulo de seguridad que adicionalmente a las firmas y heurística, utilice algoritmos de aprendizaje de máquina (Machine Learning) de manera local en el Firewall y en tiempo real, este módulo deberá funcionar como una capa de seguridad adicional que permita analizar el malware de día cero no detectado por firmas ni heurística.
VPN IPSEC Y VPN SSL	<p>Debe soportar al menos 2,000 túneles VPN IPsec.</p> <p>Deberá permitir la configuración de políticas de seguridad y</p>



PERÚ

Ministerio del Interior

NEXT GENERATION FIREWALL (NGFW) EN ALTA DISPONIBILIDAD
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	<p>visibilidad para las aplicaciones que circulan dentro de los túneles ssl.</p> <p>Deberá permitir el transporte IPsec con ssl fail back y decrypt ssl (entrada y salida).</p> <p>Deberá contar con un software cliente VPN para los sistemas operativos Windows 8, Windows 10, Windows 11, Mac OS, para brindar servicio al menos 2,000 usuarios concurrentes.</p> <p>Así mismo, se podrá configurar en dispositivos Apple IOS y Android versiones superiores a 6.0, como mínimo utilizando cliente VPN de los propios dispositivos IOS y Android.</p> <p>Deberá permitir crear políticas para tráfico VPN SSL.</p> <p>Como mínimo autenticación VPN SSL mediante ldap, base de datos propia.</p>
Otras Características	<p>Permite especificar la política por tiempo, horario o determinado periodo (día, mes, año, día de la semana y hora).</p> <p>Debe ser posible crear políticas por usuario, grupo de usuarios, IP, redes, países y zonas de seguridad.</p> <p>Soporte de 4,000 redes virtuales vians 802.1q.</p> <p>Traducción de direcciones de red (nat) por fuente y destino, por direcciones IP dinámicas y pool de puertos.</p> <p>Protocolos como mínimo bgp, ospf y rip2, dhcp server y dhcp relay.</p> <p>Soporte de jumbo frames 9200 bytes.</p> <p>En caso de protocolos desconocidos, se podrán asignar firmas propias.</p> <p>Descripción y control de tráfico sshv2.</p> <p>Control de tráfico ipv4 e ipv6, este último también incluye visibilidad e inspección de amenazas en aplicaciones y control de contenido ipv6 debe ser soportado en interfaces trabajando en L2 y L3.</p> <p>Deberá contar con la funcionalidad de exportación de bitácoras (logs) de filtrado, vista de tráfico URL y amenazas.</p> <p>Deberá permitir la administración via web, cli, syslog, snmp V2, Administración basada en roles.</p>
Reportes	<p>Deberá incluir la capacidad de proporcionar un resumen gráfico de aplicaciones utilizadas, y amenazas encontradas diariamente.</p> <p>Deberá permitir el control de transferencia de datos no autorizados con herramienta para realizar patrones definidos por usuario.</p>



PERU Ministerio del Interior

NEXT GENERATION FIREWALL (NGFW) EN ALTA DISPONIBILIDAD
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	<p>Deberá permitir la creación de reportes personalizables.</p> <p>Deberá contar con herramienta para crear filtros de monitoreo de las sesiones históricas en el firewall ya sea por aplicación, IP origen e IP destino.</p> <p>Deberá tener la capacidad para generar un reporte gráfico que permita visualizar los cambios en el uso de aplicaciones en la red con respecto a un periodo de tiempo anterior, para permitir comparar los diferentes consumos realizados por las aplicaciones en el tiempo presente con respecto al pasado.</p> <p>Generación de reportes con mapas geográficos generados en tiempo real para la visualización de orígenes y destinos del tráfico generado en la institución.</p> <p>El equipo deberá proporcionar como mínimo los siguientes conjuntos de reportes:</p> <ul style="list-style-type: none"> - Utilización de ancho de banda de entrada y salida por aplicación (top 10). - No. De sesiones por aplicación (top 10). - Comparativo semanal de aplicaciones corriendo en la red que pudieran incrementar o decrementar su utilización (top 10). - Utilización (en bytes) por aplicación (top 10). - Origen y destino del tráfico por aplicación-usuario (top 10). - Eventos / ataques por: origen, categoría, amenaza (top 10). - Nivel de riesgo de la red. - Principales aplicaciones que circulan por el firewall (top 25). - Principales direcciones IP destino por protocolo (top 25). - Las principales direcciones IP para cada uno de los protocolos y aplicaciones principales (top 50).
Administración	<p>Un (01) servidor syslog externo de uso exclusivo, que se empleará para la administración y recolección de eventos, alertas, logs y reportes de los NGWF que se instalarán en la Sede Central; podrá presentarse en modalidad virtual (Virtual Appliance) del mismo fabricante, debe tener su respectiva licencia de software de sistema operativo, de gestión de la seguridad, deberá tener un mínimo de 2 TB de almacenamiento y el resto de recursos (Procesamiento, Memoria, etc). serán dimensionados por el PROVEEDOR.</p> <p>Con la finalidad de facilitar la administración y la integridad de registros Logs, el servidor puede ser de distinto fabricante, siempre y cuando se asegure el nivel de disponibilidad requerido.</p>
Inducción	<p>Se deberá proporcionar un entrenamiento en administración, configuración básica del equipo y resolución de problemas, el cual estará dirigido a 04 profesionales de la OSTC, con un tiempo mínimo de duración de 24 horas, a realizarse de manera presencial en las instalaciones de la Entidad o de manera virtual (en línea con el expositor), dentro del plazo de implementación (120 días calendario) establecido en el numeral VIII. PLAZO DE</p>



PERU Ministerio del Interior

NEXT GENERATION FIREWALL (NGFW) EN ALTA DISPONIBILIDAD
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	EJECUCIÓN DE LA PRESTACIÓN, siendo el expositor, personal certificado por el fabricante del equipo propuesto. Se deberá entregar certificados de participación a los profesionales designados por la OSTC.

5.2.2. Sub Componente 2: Solución contra ataques de Denegación de Servicios Simples y Distribuidos

- ✓ El PROVEEDOR debe brindar dos (02) equipos de tipo hardware (appliances) de propósito específico, para la protección contra ataques de denegación de servicios simples y distribuidos, donde uno (01) de ellos estará en calidad de respaldo o "Spare". Ambos equipos deben ser de la misma marca y modelo y cumplir con las siguientes características técnicas mínimas.

SOLUCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIOS SIMPLES Y DISTRIBUIDOS
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
Interfaces de Red	Mínimo 4 interfaces de red con la capacidad de operar a 1 Gbps.
	Mínimo 1 interfaz de red dedicada para la administración, con la capacidad de operar a 1 Gbps.
	Debe contar como mínimo 1 interfaz de tipo consola o similar.
Throughput	Mínimo 06 Gbps mitigación de ataques
	Mínimo 02 Gbps para tráfico legítimo
	Número de sesiones / conexiones simultáneas ilimitadas (stateless).
Protocolo IP	El equipo deberá operar y proteger en todas sus funcionalidades tanto en direcciones IPv4 e IPV6.
Características Generales	La solución deberá inspeccionar el tráfico en modo L2 del modelo OSI.
	Permitir la inspección "in—line" de dos segmentos de red independientes en modo transparente, se precisa que la protección es tanto para tráfico entrante como tráfico saliente.
	Contar con fuentes redundantes.
	Deberá proteger contra ataques conocidos y dia-cero: flooding DoS / DDoS, incluyendo el mal uso: TCP, UDP, ICMP, IGMP y ataques fragmentados.
	Deberá proteger contra todo tipo de ataques de inundación SYN utilizando mecanismos avanzados SYN Cookies.
	Prevenir los ataques SYN-ACK.
	Deberá proteger contra ataques de inundaciones a páginas HTTP que hacen mal uso de los recursos del servidor web.



PERÚ

Ministerio del Interior

SOLUCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIOS SIMPLES Y DISTRIBUIDOS
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	Prevención de SIP INVITE y Bye floods.
	Deberá proteger contra ataques de conexión half open, SYN attacks, request attacks y full session attacks.
	Deberá contar con Servicio de actualizaciones de seguridad (SUS) actualizaciones semanales y actualizaciones de emergencia.
	El usuario podrá definir las firmas de ataques.
	Cumplimiento de RFC y verificación de máquina de estado de al menos un (01) protocolo.
	Protección contra TCP Stream Reassembly, IP Defragmentation.
	Listas de acceso por dirección IP y protocolo; Black/White por dirección IP.
	Deberá soportar protocolos compatibles como: ICMP, UDP, TCP DNS, HTTP, HTTPS, SIP como mínimo y de manera opcional protocolos adicionales podrán ser definidos por el usuario.
	Deberá soportar alertas SNMP V2 y V3, Syslog, E-mail.
	Deberá soportar SNMP V2 y V3, HTTP, HTTPS, SSH, Telnet, de manera opcional podrá soportar console (seleccionable por el usuario).
	Deberá poder sincronizar con servidores NTP.
	Debe permitir exportar en tiempo real parámetros de comportamiento, tales como: - Patrones de tráfico normal - Los ataques en tiempo real y botnets, opcionalmente las firmas de ataques en curso DoS / DDoS y/o otros.
	Debe proteger en tiempo real y prevenir ataques intrusiones de red conocida y emergente.
	Debe proteger y prevenir ataques no basados en la vulnerabilidad que hacen mal uso de los recursos del servidor, incluyendo: - Application DoS - HTTP, SIP, y otros ataques de inundación. - Authentication defeat - ataques de fuerza bruta - Information theft — Scan de Aplicaciones.
	Proteger contra DoS/DDoS flood attacks que hacen mal uso de los recursos de ancho de banda de red.
	Deberá mostrar en tiempo real, las firmas generadas por cada patrón de ataque.
	Deberá Bloquear ataques sin bloquear el tráfico de los usuarios legítimos.
	Opcionalmente podrá soportar la aceleración de hardware dedicado contra ataques DDoS.



PERU

Ministerio del Interior

SOLUCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIOS SIMPLES Y DISTRIBUIDOS
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	<p>Deberá poder realizar escalabilidad del sistema:</p> <ul style="list-style-type: none"> - Selección de plataforma escalable con actualizaciones de licencia para el incremento de rendimiento - "Hands-off" - Deberá tener la función de autoaprendizaje y auto adaptarse a las condiciones cambiantes de la red: debe requerir un mínimo de configuración y afinamiento sobre el tiempo. - Prevención totalmente automatizada a través de firmas automáticas en tiempo real. - Deberá tener visibilidad completa del comportamiento de la red, ataques, y los detalles del ataque. <p>Capacidad de recibir y utilizar los certificados y pares de llaves público/privadas para los servidores web protegidos</p> <p>Opcionalmente podrá contar con las siguientes funcionalidades:</p> <ul style="list-style-type: none"> - Inspeccionar y monitorear todos los datos HTTP y la aplicación, incluyendo, los encabezados HTTP, campos de formularios, y el cuerpo HTTP. - Inspeccionar las peticiones y respuestas HTTP. - Capacidad de decodificar datos a su mínima expresión y validarla.
Administración	<p>Una (01) consola para la administración, reportes y consolidación de todas las alertas de la solución, la cual podrá ser del tipo Hardware (Appliance) o virtual Appliance del mismo fabricante o podrá estar embebida en el equipo principal.</p> <p>Debe contar con fuente de poder y discos, ambos redundantes (Sólo en el caso que el equipo sea del tipo Hardware Appliance o Virtual Appliance).</p> <p>Opcionalmente todos los componentes que conformen la solución de este lote único, podrán ser administrados en forma centralizada a través de un software de administración o módulo de gestión que permita la administración y operación de los dispositivos en forma centralizada.</p> <p>La consola de administración del equipo deberá realizar backup diarios en forma automática de toda la información almacenada en el mismo, incluyendo las configuraciones de todos los módulos administrados y tener la capacidad de transferirlos automáticamente a un servidor remoto utilizando los protocolos SSH y/o HTTPS y/o SCP y/o SFTP</p> <p>Debe permitir la definición de distintas políticas de seguridad, entendiéndose como tal, al conjunto de reglas bajo el cual estará controlada una determinada aplicación.</p> <p>Debe permitir elegir la política de seguridad a ser implementada en una aplicación, como así también la aplicación de políticas distintas para aplicaciones distintas.</p> <p>Debe permitir la reconfiguración de las distintas políticas de seguridad definidas por el usuario y políticas que estén siendo utilizadas en la protección de una aplicación.</p> <p>Toda la configuración, administración y monitoreo de la solución se efectuará</p>



PERU Ministerio del Interior

SOLUCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIOS SIMPLES Y DISTRIBUIDOS
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	<p>a través de la consola.</p> <p>El acceso a la consola de administración debe realizarse a través del protocolo http(s) como mínimo y mediante autenticación por medio de usuarios locales, opcionalmente mediante autenticación por certificados digitales y/o tokens.</p> <p>La consola permitirá la notificación de un determinado evento mediante: Email y/o Syslog y/o SNMP Trap.</p> <p>La consola debe permitir la asignación de perfiles de administración por usuarios y estos perfiles deben permitir separar roles de administración y monitoreo.</p>
Gestión de logs	<p>Proporcionar una vista centralizada de los logs, entendiendo como tal, la unificación de los logs de la totalidad de los componentes que conforman la solución.</p> <p>Los logs de todos los componentes de la solución deberán cumplir con las siguientes características:</p> <ul style="list-style-type: none"> - Poder ser transferido hacia el servidor de administración externo. - Capacidad de ser exportados y/o capturados desde el servidor de administración, a un formato de texto, para poder utilizar herramientas de análisis de terceros. - En caso utilizar un servidor administración externo, los equipos deben poder almacenar en forma local los logs, para aquellos casos que existan inconvenientes en la comunicación con el servidor central. <p>La administración debe permitir la visualización en tiempo real de los logs de actividad de la solución DDoS y las modificaciones de configuración que los administradores pudieran efectuar.</p> <p>La administración debe permitir, como mínimo, lo siguiente:</p> <ul style="list-style-type: none"> - Agregar, eliminar o modificar la configuración en un entorno gráfico. - Efectuar la configuración de los componentes de la solución. - Visualizar los registros de auditoría, alertas de seguridad y eventos del sistema. - Generar reportes ajustables por el usuario.
Monitoreo y alertas	<p>Deberá soportar como mínimo SNMP v2 y v3 para control y monitoreo.</p> <p>Soportar la consulta, mediante protocolo SNMP, de la siguiente información:</p> <ul style="list-style-type: none"> - Uso de CPU. - Uso de Memoria. - Estado de cada una de las interfaces de red. - Tráfico en cada una de las interfaces de red. <p>Soportar la generación de alarmas mediante:</p> <ul style="list-style-type: none"> - Traps SNMP y/o - Email y/o - Syslog.



PERU Ministerio del Interior

SOLUCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIOS SIMPLES Y DISTRIBUIDOS
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	<p>Generar alarmas ante los siguientes eventos:</p> <ul style="list-style-type: none"> - Degradación de la performance. - Falla de cualquiera de los componentes de la solución. - Problemas de conectividad. <p>Poseer alarmas automáticas y/o notificaciones automáticas de eventos de seguridad.</p> <p>La administración debe permitir la visualización en tiempo real de los logs correspondientes a los eventos que hayan violado una política de seguridad determinada, detallando como mínimo:</p> <ul style="list-style-type: none"> - IP Origen y IP destino. - Puerto origen y puerto destino. - Fecha y/o hora de ocurrencia. - Nombre de la aplicación asociada. (Opcional) - Descripción del motivo por el cual fue categorizada. (opcional). - Nombre del evento. (opcional) - Severidad del evento. (opcional) - Comando SQL (opcional). - Usuario de base de datos y sistema operativo (opcional). - Base de datos, esquema y tablas afectadas (opcional)". <p>El administrador puede categorizar los distintos eventos en función de distintos criterios a ser definidos, se precisa que dicha categorización se podrá realizar desde la misma administración o al momento de ser exportados.</p>
Reportes	<p>Permitir la generación de reportes, de todo evento que se registre en los LOGS (eventos de seguridad, eventos del sistema, eventos de error y/o otros) de la solución ofertada, en los formatos CSV y PDF y/o HTML.</p> <p>Permitir la elección de información a ser incluida en los reportes.</p> <p>Capacidad de automatizar la generación de reportes y su posterior remisión por email. Así mismo también se aceptará el soporte de generación de eventos de seguridad incluyendo el usuario aplicativo, si este efectivamente se ha registrado.</p>
Otros	El fabricante de la solución deberá contar con un servicio de investigación sobre vulnerabilidades y ciberamenazas.
Inducción	Se deberá proporcionar un entrenamiento en administración, configuración básica del equipo y resolución de problemas, el cual estará dirigido a 04 profesionales de la OSTC, con un tiempo mínimo de duración de 15 horas, a realizarse de manera presencial en las instalaciones de la Entidad o de manera virtual (en línea con el expositor), dentro del plazo de implementación (120 días calendarios) establecido en el numeral VIII. PLAZO DE EJECUCIÓN DE LA PRESTACIÓN, siendo el expositor, personal certificado por el fabricante del equipo propuesto. Se deberá entregar certificados de participación a los profesionales designados por la OSTC.



PERU Ministerio del Interior

5.2.3. Sub Componente 3: Sistema firewall de aplicaciones Web

- ✓ El PROVEEDOR deberá brindar dos (02) equipos (appliances) de propósito específico, para la protección de las aplicaciones WEB del MININTER, donde uno (01) de ellos estará en calidad de respaldo o "Spare". Ambos equipos deben ser de la misma marca y modelo y cumplir con las siguientes características técnicas mínimas.

FIREWALL DE APLICACIONES WEB CANTIDAD: DOS (02)	
DESCRIPCIÓN	DETALLES TÉCNICOS
Interfaces de Red	Como mínimo 4 Interfaces de red, con la capacidad de operar a 1 Gbps.
	Como mínimo 1 interfaz dedicada para la administración, con la capacidad de operar a 1Gbps.
	En el caso que el equipo ofertado permita el despliegue en modo bridge-inline, todas las interfaces del dispositivo deben incluir ByPass físico y/o lógico a fin de garantizar la disponibilidad del servicio en caso de una falla del equipo.
Throughput	Mínimo 1 Gbps.
Protocolo IP	El equipo deberá operar y proteger tanto a direcciones IPv4 e IPV6.
	Equipo para protección de aplicaciones WEB contra amenazas registradas OWASP Top Ten vulnerabilities 2021.
	El sistema debe proteger contra las siguientes amenazas. <ul style="list-style-type: none"> - SQL injection. - Cross-site scripting (XSS). - Parameter tampering. - Hidden field manipulation. - Session manipulation. - Cookie poisoning. - Stealth commanding. - Backdoor and debug options. - Application buffer overflow attacks. - Brute force attacks. - Data encoding. - Unauthorized navigation. - Gateway circumvention. - Web server reconnaissance. - SOAP and Web services manipulation.
	El sistema como mínimo debe contar con los siguientes mecanismos de protección: <ul style="list-style-type: none"> - El dispositivo deberá soportar esquemas de seguridad positiva y negativa. - El sistema deberá proteger contra ataques nuevos no registrados. - Deberá contar con mecanismo que garantice protección de la mayoría de los ataques no registrados también conocidos como ataques de día cero. - El sistema deberá soportar filtros de seguridad que bloqueen ataques de fuerza bruta. - El sistema deberá soportar filtros de seguridad que bloqueen ataques a la base de datos.



PERU Ministerio del Interior

FIREWALL DE APLICACIONES WEB**CANTIDAD: DOS (02)**

DESCRIPCIÓN	DETALLES TÉCNICOS
	<ul style="list-style-type: none"> - El sistema deberá soportar filtros de seguridad que bloqueen ataques de métodos y parámetros HTTP y HTTPS. - El sistema deberá soportar filtros de seguridad para proteger las sesiones de usuarios remotos. - El sistema deberá soportar filtros de seguridad que protejan servicios web. - El sistema deberá soportar filtros de seguridad de XML. - El sistema deberá brindar protección Anti-Scraping, mediante filtros o módulo de seguridad.
	El sistema deberá bloquear tráfico malicioso (bloquear ataque), permitiendo únicamente tráfico legítimo de los usuarios.
	El sistema deberá soportar como mínimo aprendizaje sin manipulación del administrador.
	<ul style="list-style-type: none"> • El sistema deberá registrar cambios en la configuración. • La solución deberá tener la capacidad de vincular y correlacionar todas sus capas individuales de seguridad, por ejemplo: fraude, apropiación de cuentas, geolocalización de IP, etc., etc. para vincular todas estas capas juntas y tomar una decisión frente a una amenaza. • La solución deberá prevenir bots maliciosos e identificar malos comportamientos como anti-scraping o screen scraping en las aplicaciones.
	El sistema deberá permitir la generación de reportes por: aplicaciones y de manera opcional por filtros de seguridad y/o otros.
	Deberá soportar los siguientes modos de operación: <ul style="list-style-type: none"> - Passive – Detección (Alertamiento). - Active – Detección y mitigación (Bloqueo).
	El dispositivo deberá soportar integración con sistemas de gestión centralizados.
	El dispositivo deberá permitir la actualización de firmas y software desde la consola Web.
	El equipo deberá soportar arquitectura clúster de alta disponibilidad Activo - Pasivo con sincronización de reglas entre los equipos.
	El sistema deberá permitir URL Access Restrictions.
	El sistema deberá permitir la restricción de parámetros como logical application attack, buffer overflow, zero day attacks, mediante políticas.
	El sistema deberá proteger contra scrapping o web scrapping
	El sistema deberá evitar ataques de tipo cookie poisoning.
Arquitectura	El dispositivo deberá soportar integración con sistemas de gestión centralizados.



PERU Ministerio del Interior

FIREWALL DE APLICACIONES WEB
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	Debe soportar el despliegue como mínimo en modo Reverse proxy transparente y/o Reverse Proxy explícito, así mismo de manera opcional podrá soportar el despliegue en modo Bridge- Inline.
	Almacenamiento efectivo mínimo de 1 TB y fuentes de energía redundantes.
Gestión y administración	El sistema de gestión centralizado debe permitir administrar la solución de WAF.
	El sistema WAF deberá incluir una consola del mismo fabricante para presentar reportes unificados y alertas de ataques en la misma consola.
	El sistema de gestión interno del equipo debe ser tipo Web con definiciones de roles (RBAC) por una interfaz de administración dedicada.
	El sistema deberá soportar administración simplificada, a través de la réplica de políticas y datos estadísticos aprendidos.
Inducción	Se deberá proporcionar un entrenamiento en administración, configuración básica del equipo y resolución de problemas, el cual estará dirigido a 04 profesionales de la OSTC, con un tiempo mínimo de duración de 15 horas, a realizarse de manera presencial en las instalaciones de la Entidad o de manera virtual (en línea con el expositor), dentro del plazo de implementación (120 días calendarios) establecido en el numeral VIII. PLAZO DE EJECUCIÓN DE LA PRESTACIÓN, siendo el expositor, personal certificado por el fabricante del equipo propuesto. Se deberá entregar certificados de participación a los profesionales designados por la OSTC.

5.2.4. Sub Componente 4: Solución de Protección de Amenazas Avanzadas en Alta Disponibilidad

- ✓ El PROVEEDOR debe brindar dos (02) equipos de tipo hardware (Appliance) de propósito específico, para la protección de amenazas avanzadas en Alta Disponibilidad, ambos equipos deben ser de la misma marca y modelo y cumplir con las siguientes características técnicas mínimas.

SOLUCIÓN DE PROTECCIÓN DE AMENAZAS AVANZADAS EN ALTA DISPONIBILIDAD
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
Interfaces de Red	Deberá contar como mínimo con 10 interfaces de 01 Gbps o 02 interfaces de 10 Gbps SFP+ cada una, para ser configurado en modo bridge o inline. Debe operar en modo bypass (fail-open) interno que impida la interrupción ante eventos de falla por energía del equipo.
	Como mínimo 1 interfaz para la administración, con capacidad de operar a 1 Gbps.
Throughput	Como mínimo 02 Gbps.



PERU

Ministerio del Interior

**SOLUCIÓN DE PROTECCIÓN DE AMENAZAS AVANZADAS EN ALTA DISPONIBILIDAD
CANTIDAD: DOS (02)**

DESCRIPCIÓN	DETALLES TÉCNICOS
Protocolo IP	El equipo deberá operar y proteger tanto a direcciones IPv4 e IPV6.
Funcionalidades Básicas	Se requiere una solución de emulación de amenazas, para la detección y prevención de amenazas avanzada, en los segmentos de red protegidos por la solución.
	La solución debe permitir realizar en forma automática un almacenamiento de seguridad local, USB, y/o remoto de la configuración y/o base de datos de alertas y contenido. El contenido almacenado debe poder ser restaurado desde una locación remota, USB o una copia local.
	Capacidad de disco de mínimo de 02 TB.
	Capacidad de soportar como mínimo 3,000 usuarios, incluyendo usuarios móviles.
	Soportar mínimo 20 VMs (Máquinas Virtuales).
	La solución debe soportar una interfaz de gestión separada e independiente de las interfaces por donde dan servicio.
	La solución debe proveer redundancia en sus fuentes de alimentación y ventiladores y discos.
	No se permitirán soluciones que hagan parte o todo el análisis de sandbox en la nube.
	Debe soportar autenticación integrada por protocolo AAA (Autenticación, Autorización y Auditoría) o LDAP (soportando Active Directory). Además, debe soportar usuarios locales.
	Debe soportar la visualización de todos los usuarios, indicando: <ul style="list-style-type: none"> - Nombre del usuario. - Rol. - Estado de la cuenta. - Última vez que se utilizó. - Cantidad de veces que se utilizó. - Dirección IP desde donde se conectó la última vez.
	La solución debe soportar la autenticación de SSH por clave pública y privada.
	La solución debe soportar la definición de mínimamente los siguientes roles: <ul style="list-style-type: none"> - Administrador, con capacidad de gestionar todo en los dispositivos. - Operador, con capacidad limitada para gestionar los elementos asociados a la operación de los dispositivos, no de las alertas o reportes. - Monitoreo, con capacidad de sólo lectura de todo en los dispositivos. - Analista, con capacidad de gestión de sólo alertas y reportes. No tienen permisos de gestión de la infraestructura.
	Debe soportar y operar en modo en línea, analizando el tráfico de navegación (HTTP y HTTPS), tráfico de correo (SMTP, SMTPS, IMAP) y tráfico de redes compartidas Microsoft (CIFS, SMBv3, SMBv3 multi-channel).



PERU Ministerio del Interior

SOLUCIÓN DE PROTECCIÓN DE AMENAZAS AVANZADAS EN ALTA DISPONIBILIDAD
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	<p>Debe tener la capacidad de bloquear el tráfico malicioso en tiempo real.</p> <p>Opcionalmente podrá contar con la capacidad de crear reglas tipo Snort para implementar bloqueos personalizados sobre el contenido del tráfico.</p> <p>Debe poder analizar todo el tráfico en búsqueda de tráfico HTTP/HTTPS, sin necesidad de que se le especifique el puerto TCP que debe analizar.</p> <p>La solución debe ser capaz de detectar la actividad maliciosa después del ataque, capturando información del tráfico de red originado en la máquina comprometida. Esta funcionalidad debe soportar la definición de listas blancas para ignorar el tráfico con destino a una serie de IPs conocidas.</p>
Análisis de Sandboxing	<p>El sistema de Sandbox debe soportar el análisis de plataformas de 32 y 64 bits.</p> <p>Con el fin de analizar los distintos tipos de archivo malicioso, las máquinas virtuales deben soportar por defecto como mínimo:</p> <ul style="list-style-type: none"> - Archivos Microsoft Office files (doc/docx, xls/xlsx, ppt/pptx). - Archivos PDF. - Objetos Flash, inclusive SWF embebido dentro de SWF. - Objetos Shockwave. - Contenido Java JDK & JRE. - Objetos Quicktime. - Objetos Realplayer. - Objetos Windows Media Player. - Contenido Microsoft.NET framework. - Contenido Microsoft Visual C++ Redistributable. - Contenido Microsoft Silverlight. - Imágenes (jpg, jpeg, gif, tiff, ico, png). - Contenido Microsoft DirectX. <p>La solución debe detectar, analizar y bloquear ataques de inyección DLL que traten de modificar aplicaciones que están instaladas en el sistema operativo, tales como herramientas de MS Office.</p> <p>El entorno de inspección virtual debe ser capaz de emular el sistema operativo y el browser como si se tratara del equipo host, comunicándose a los servidores web que intentan infectar al equipo. Para realizarlo no debe requerir conectarse a algún otro dispositivo que tenga como función proporcionar firmas de malware, ni alguna otra dependencia externa.</p> <p>Por cada una de las infecciones por malware detectadas, mostrar los siguientes campos como mínimo:</p> <ul style="list-style-type: none"> - Detalles de amenaza, PCAP, IP Origen, Encabezados (fuente) - Detalle de los cambios realizados al sistema operativo, indicando las alertas maliciosas detectadas durante el análisis del comportamiento de la amenaza, el tipo y la versión del sistema operativo. <p>El sistema de protección de malware debe detectar vulnerabilidades sin necesidad de conocer la firma, es decir, a través del comportamiento de la amenaza.</p>



PERU

Ministerio del Interior

SOLUCIÓN DE PROTECCIÓN DE AMENAZAS AVANZADAS EN ALTA DISPONIBILIDAD
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	<p>Debe soportar la ejecución e inspección de los siguientes tipos de archivos: 3gp, asf, avi, bat, chm, cmd, com, csv, dll, doc, docx, exe, flv, gif, hop, hml, htm, hwp, ico, jar, jpg, js, lnk, midi, mov, mp3, mp4, mpg, pdf, png, ppsx, ppt, pptx, qt, rm, rmi, rtf, swf, tiff, url, vbs, vcf, vcs, wav, wma, wsf, xls, xlsx, xml.</p> <p>La solución debe registrar toda la actividad que un objeto malicioso trate de ejecutar, registrando las modificaciones del sistema operativo/aplicación que logre modificar, tales como:</p> <ul style="list-style-type: none"> - Registro de interacción con el sistema operativo, mutex. - Registro de comportamiento de aplicación. - Registro de actividad sobre gestión de procesos - Registro de actividad sobre archivos. - Registro de uso de APIs. - Registro de comunicaciones de red. - Modificaciones en la registry de Windows. - Actividad directa sobre el hardware. - Exploits. - Inyección de código en DLLs. <p>La solución debe ser capaz de detectar todos los objetos que ya han sido analizados y evitar un doble análisis.</p> <p>La solución debe ofrecer una herramienta gráfica para poder analizar los cambios realizados en las máquinas virtuales sobre el sistema operativo.</p> <p>La solución debe soportar el uso y procesamiento de hash en SHA256 y/o MD5.</p>
Inducción	<p>Se deberá proporcionar un entrenamiento en administración, configuración básica del equipo y resolución de problemas, el cual estará dirigido a 04 profesionales de la OSTC, con un tiempo mínimo de duración de 24 horas, a realizarse de manera presencial en las instalaciones de la Entidad o de manera virtual (en línea con el expositor), dentro del plazo de implementación (120 días calendarios) establecido en el numeral VIII. PLAZO DE EJECUCIÓN DE LA PRESTACIÓN, siendo el expositor, personal certificado por el fabricante del equipo propuesto. Se deberá entregar certificados de participación a los profesionales designados por la OSTC.</p>

5.3. COMPONENTE 3: SERVICIO DE INTERCONEXIÓN PARA LAS SEDES DEL MININTER.

El presente componente consta de tres (03) sub componentes de servicios

COMPONENTE 3: SERVICIO DE INTERCONEXIÓN PARA LAS SEDES DEL MININTER.	
SUB COMPONENTE	DENOMINACIÓN
1	Servicio de acceso a la VPN-MININTER para la Sede Principal.
2	Servicio de acceso a la VPN-MININTER para las Sedes Remotas.
3	Plataforma de Monitoreo.



PERU Ministerio del Interior

- ✓ La topología de la VPN-MININTER deberá ser todos contra todos (full mesh), con sus respectivas sedes, es decir, la comunicación entre sedes debe ser directa una a una, sin necesidad de pasar por la Sede Principal.
- ✓ La red del PROVEEDOR deberá tener la capacidad para soportar datos, voz, video y manejar QoS (calidad de servicio).
- ✓ Los protocolos soportados por la red del PROVEEDOR de servicio serán IPv4 e IPv6, considerando la implementación de una futura migración desde IPv4 hacia IPv6 (de acuerdo al Decreto Supremo N° 081-2017-PCM) durante el periodo de la prestación del servicio. El PROVEEDOR deberá realizar las configuraciones necesarias en los equipos de su propiedad, para la migración a IPv6 cuando la Entidad lo requiera; y sin costo adicional para la Entidad; incluyendo si fuera necesario la implementación de una Demo previo a la Transición. El personal encargado de la OG TIC – MININTER brindará todas las facilidades técnicas con los equipos de su propiedad.
- ✓ El Enlace principal y secundario de la Sede Principal deben de pertenecer a Puntos de Presencia – PoP de distintas ubicaciones físicas en la infraestructura del PROVEEDOR.
- ✓ El backbone de la red del PROVEEDOR en Lima Metropolitana deberá ser redundante y estar basado en una plataforma 100% en fibra óptica, con protocolo de transporte MPLS. Para el caso de las sedes remotas se aceptarán extensiones al backbone sobre enlaces de fibra óptica y/o radio enlace.
- ✓ Referente a los circuitos de datos, El MININTER podrá modificar la ubicación de las Sedes Remotas a un máximo de seis (06) sedes remotas durante el periodo de la prestación del servicio (sin generar costo alguno para la Entidad), considerando el mismo número identificador de circuito de datos y el mismo tipo de acceso. Las nuevas ubicaciones serán en lugares de condiciones similares a las de la relación inicial. Se precisa que los posibles traslados estarán sujetos a que el Contratista cuente con facilidades técnicas para la implementación del servicio, pudiendo requerirse el traslado dentro de la misma jurisdicción provincial territorial.
- ✓ Se precisa que la Entidad comunicará al PROVEEDOR de las posibles nuevas ubicaciones de las Sedes Remotas con una anticipación no menor a cuarenta y cinco (45) días calendarios. El Proveedor deberá confirmar la presencia de facilidades técnicas, en un plazo máximo de 15 días calendario contados a partir del día siguiente de haberse formulado el requerimiento por parte de la Entidad. De ser afirmativa la respuesta del Proveedor, éste deberá realizar la implementación en un plazo máximo de 30 días calendario, contados a partir del día siguiente de haberse confirmado la presencia de facilidades técnicas.
- ✓ Los accesos de fibra óptica desde el nodo más cercano del PROVEEDOR hasta la sede principal del MININTER deberán ser a través de canalizaciones subterráneas. La acometida dentro de la sede principal del MININTER hasta el equipamiento de comunicaciones será subterránea y/o canalizada. No se aceptarán accesos de fibra aérea para la Sede Principal (Edificio MININTER). Si fuera necesario realizar obras civiles y/o canalizaciones dentro o fuera de los locales para la instalación de los servicios propuestos, estos deberán ser realizadas por el PROVEEDOR, así como la subsanación de las mismas.
- ✓ Se precisa que el Proveedor podrá hacer uso del canalizado interno de la Entidad, en la medida que este cuente con espacio disponible para el tendido de la acometida hasta el equipamiento de comunicaciones; caso contrario, el Proveedor deberá realizar un nuevo canalizado.
- ✓ El PROVEEDOR deberá brindar la interconexión de datos para las Sedes Remotas, utilizando cualquiera de los siguientes medios de transporte: fibra óptica o radio enlace (de acuerdo a las facilidades técnicas en la sede remota), respetando los parámetros mencionados en este documento y validando el tema de disponibilidad. Se precisa que el equipamiento que será utilizado en las sedes remotas (medio de fibra óptica o radio enlace)



PERU Ministerio del Interior

para la implementación de cada uno de los medios de transmisión para la provisión de los servicios deberán ser nuevos y de primer uso.

- ✓ El PROVEEDOR debe asegurar un nivel de disponibilidad mensual para el servicio de interconexión de sedes, considerando los siguientes medios de acceso y zonas geográficas.

MEDIO DE ACCESO	LIMA Y URBANO	SEMI URBANO	RURAL
Fibra Óptica	$\geq 99.90\%$	$\geq 99.80\%$	$\geq 99.00\%$
Radio punto a punto	$\geq 99.30\%$	$\geq 99.00\%$	$\geq 98.50\%$

- ✓ El MININTER se encargará de provisionar los elementos necesarios para la instalación de los enlaces en sus Sedes Remotas, así como también de todos los componentes a instalarse en la Sede Principal, por lo cual se considera lo siguiente:

- Tomacorrientes
- Energía eléctrica.
- Bandeja y unidades rackeables (para la instalación del equipamiento).
- Switch de comunicaciones.

- ✓ Para la realización de cualquier trabajo de instalación que deba ser efectuado dentro de las instalaciones del MININTER, la Entidad garantizará al Contratista todas las facilidades técnicas que sean necesarias; así como todos los accesos que correspondan para el cumplimiento de la implementación.

- ✓ El Proveedor, ante la ocurrencia de un evento generador de atraso en la implementación del servicio que escape a su responsabilidad, deberá comunicarlo y sustentado oportunamente a la Entidad, solicitando la correspondiente ampliación de plazo.

5.3.1. Sub Componente 1: Servicio de acceso a la VPN-MININTER para la Sede Principal

- ✓ El PROVEEDOR deberá implementar un circuito de datos de acceso a la VPN-MININTER, como línea dedicada principal, simétrica, a través de fibra óptica y que deberá tener como mínimo un ancho de banda de 200 Mbps.
- ✓ El PROVEEDOR deberá implementar un (01) circuito de datos de acceso a la VPN-MININTER, como línea dedicada de respaldo, simétrica, a través de fibra óptica que deberá llegar de un nodo diferente al nodo de la línea dedicada principal y una ruta diferente a la ruta de la línea dedicada principal y que deberá tener como mínimo un ancho de banda de 200 Mbps.
- ✓ Para cada uno de los circuitos de datos, la configuración de los equipos del PROVEEDOR deberá permitir un caudal IP 130 Mbps con prioridad en la transmisión de datos y un caudal IP de 5 Mbps con prioridad en la transmisión de voz sobre IP. Si las comunicaciones de voz no ocupan los 5 Mbps, los equipos deberán reasignar en forma dinámica para la transmisión de datos la parte del ancho de banda no ocupada.
- ✓ Para cada uno de los dos circuitos, los equipos de comunicaciones deberán tener como mínimo 04 puertos Ethernet 10/100/1000 Base-T para el acceso a la LAN.
- ✓ La conmutación al enlace de respaldo deberá ser automática cuando el enlace principal presente falla y/o avería, debiendo desactivarse de forma automática en cuanto se recupere la conectividad en el enlace principal.
- ✓ El PROVEEDOR deberá proveer, instalar y configurar los circuitos de datos y todo el equipamiento de comunicaciones necesario para la prestación del servicio, así como asegurar la interoperabilidad entre todas las Sedes Remotas consideradas en el Anexo B, durante la vigencia del contrato.



PERU Ministerio del Interior

5.3.2. Sub Componente 2: Servicio de acceso a la VPN-MININTER para las Sedes Remotas

- ✓ Se instalarán cuarenta (40) circuitos de datos (según Anexo B), con acceso simétrico por fibra óptica y/o radio enlace; con tasa de acceso garantizada del 100%. (Según Anexos A y B).
- ✓ La comunicación entre los nodos deberá realizarse bajo el esquema de un grupo cerrado de usuarios, para tal efecto deberá asignarse direcciones IP privadas para cada acceso simétrico.
- ✓ La Red WAN del PROVEEDOR deberá soportar el transporte del tráfico de Telefonía IP.
- ✓ La transmisión y recepción de datos, debe realizarse sobre un canal seguro dentro de la red de datos del PROVEEDOR, es decir el canal debe ser exclusivo para el uso del MININTER, constituyendo una red privada inaccesible desde Internet para usuarios externos no autorizados.
- ✓ El PROVEEDOR deberá incluir un equipo de comunicaciones (router) por cada circuito de datos, este equipo debe ser de última generación y con los sistemas operativos actualizados.
- ✓ Para la sede remota en RENIEC, se precisa que se podrá provisionar el servicio desde el MININODO del RENIEC en reemplazo de un router dedicado. Para la realización de cualquier trabajo de instalación que deba ser efectuado dentro de las instalaciones de la sede remota en RENIEC, la Entidad garantizará al Contratista todas las facilidades técnicas que sean necesarias; así como todos los accesos que correspondan ante la RENIEC para el cumplimiento de la implementación.

5.3.3. Sub Componente 3: Plataforma de Monitoreo

- ✓ El PROVEEDOR deberá proveer una herramienta de monitoreo para los Enlaces de Datos e Internet de la Entidad, con software de medición de ancho de banda, la cual estará instalada en la sede principal del MININTER.
- ✓ La herramienta de monitoreo debe tener una interfaz gráfica de múltiples idiomas.
- ✓ La herramienta deberá sensar en tiempo real mediante el protocolo SNMP, como mínimo a doscientos (200) dispositivos, entre equipos de comunicaciones, equipos de seguridad y servidores, a través de una consola única centralizada. Se precisa que los dispositivos serán distribuidos de la siguiente manera: 50 routers, 100 switches, 40 servidores y 10 equipos de seguridad. Donde se va a monitorear como mínimo 2 puertos por dispositivo.
- ✓ La herramienta deberá mostrar la disponibilidad de los dispositivos sensados, donde se pueda mostrar como mínimo las siguientes métricas de desempeño: disponibilidad, pérdida de paquetes, uso de CPU, uso de Memoria, nivel de carga, ancho de banda, tráfico entrante y saliente. Opcionalmente el Proveedor podrá brindar las métricas de latencia, jitter y RTT.
- ✓ La herramienta debe permitir obtener en tiempo real, los reportes y gráficas de las métricas indicadas en el punto anterior, disponiendo de una capa de analítica que sea capaz de mostrar los diferentes reportes agrupados en cuadros de mando personalizables.
- ✓ La herramienta deberá soportar protocolo IPv4 e IPv6.
- ✓ La herramienta deberá mostrar el estatus de equipos, interfaces y/o volúmenes (interfaces virtuales o Vlans).
- ✓ La herramienta debe poder recolectar datos mediante los protocolos Syslog, SNMP y opcionalmente Netflow, para temas de auditoría y cumplimiento.
- ✓ La herramienta debe permitir la generación de alarmas estáticas, mediante definición de



PERU

Ministerio del Interior

umbrales y adaptativas basadas en patrones.

- ✓ Visor de eventos de alarmas activas en el momento de la consulta, permitiendo escalar el problema si el periodo desde que se generó la alarma es mayor al aceptable. Envío de traps SNMP por cada evento producido por cada alarma.
- ✓ Capacidad para generar informes automatizados que se puedan programar y exportar en formato PDF, CSV y/o JPG.
- ✓ Debe obtener como mínimo los siguientes datos:
 - ✓ Red
 - Número de flujos, rendimiento total, volumen total, tráfico de bajada, tráfico de subida, paquetes transmitidos, paquetes recibidos, duración de la actividad, rendimiento máximo.
 - ✓ HTTP / HTTPS
 - Tiempo de disponibilidad del servicio, datos medios, datos pico, no accesibilidad del servicio, relación de falla de sesión, tiempo de sesión, tiempo de configuración, transacciones, corte de transferencia de datos, falla de acceso al servicio.
 - ✓ Chequeo de salud (estas Métricas mediante SNMP)
 - Consumo de memoria, consumo de CPU, estadísticas de memoria, carga del procesador, operación del disco, estadísticas del proceso, caída de paquetes.

5.4. COMPONENTE 4: SERVICIO DE TELEFONÍA FIJA.

Dicho componente está constituido por las siguientes características que a continuación se detallan:

- ✓ El PROVEEDOR debe habilitar el servicio de telefonía fija corporativa para la Sede Principal del Ministerio del Interior mediante un enlace telefónico de troncal SIP, con 100 canales simultáneos para comunicación con la red telefónica pública conmutada (PSTN, Public Switched Telephone Network), los cuales serán para llamadas entrantes y salientes con la Central Telefónica existente en la Sede Principal del MININTER. Estos enlaces deben ser habilitados y configurados por el PROVEEDOR del servicio.
- ✓ El PROVEEDOR deberá ejecutar el servicio de portabilidad numérica sin costo adicional para la entidad, ello con la finalidad de no ver afectada la numeración actual de sus líneas primarias existentes en el MININTER.
- ✓ El PROVEEDOR deberá asignar 100 DID (Direct Inward Dial).
- ✓ El PROVEEDOR deberá tener en cuenta que la tarificación y/o facturación debe realizarse utilizando la unidad de medida de tiempo del segundo, no del minuto.
- ✓ Se detalla la cantidad de minutos mensuales requeridos por tipo de llamada:

TIPO DE LLAMADA	MINUTOS MENSUALES
Discado Directo Local	35,000
Discado Directo Nacional	30,000
Discado Directo Celular (Todos los operadores de telefonía móvil)	15,000
Discado Directo Internacional (Fijo Celular)	2,000

- ✓ Mediante contacto autorizado asignado por la OGTIC del MININTER, se podrá solicitar minutos adicionales de presentarse la necesidad al agotarse el saldo en la bolsa contratada, esos minutos adicionales deberán considerarse al mismo precio por minuto de la bolsa asignada y deberá facturarse en un recibo independiente indicando el detalle del consumo.



PERU Ministerio del Interior

5.5. ATENCIÓN DE REQUERIMIENTOS E INCIDENCIAS

- ✓ Se entenderá por incidencia, a la interrupción no planificada del funcionamiento de un servicio o a la reducción en la calidad del mismo.
- ✓ El MININTER reportará los requerimientos e incidencias, a través de cualquiera de los siguientes medios de comunicación: teléfono o correo electrónico, para la generación del respectivo ticket de atención, debiendo EL PROVEEDOR indicar los números de teléfono y buzones de correo electrónicos de atención a la firma del contrato, para cada uno de los componentes y subcomponentes que conforman la presente contratación.
- ✓ El MININTER podrá efectuar llamadas de servicio de lunes a domingo, incluyendo feriados, desde las 00:00 hasta las 24:00 horas, para el reporte de averías.
- ✓ El PROVEEDOR deberá contar con un Centro de Atención de Llamadas o Atención al Cliente, disponible las 24 horas del día los 365 días del año, para atención de reportes de incidencias y requerimientos.
- ✓ EL SOC o NOC (según sea el caso), ante la ocurrencia de una incidencia, dispondrá de 30 minutos para generar de manera proactiva el número de ticket de atención, el mismo que deberá ser remitido al buzón de correo electrónico habilitado por la Entidad. Sin perjuicio de ello, la Entidad podrá reportar al proveedor la ocurrencia de una incidencia.
- ✓ Se precisa que no se considerarán averías imputables al contratista y por ende no se considerará penalidad, en los siguientes escenarios:
 - Actividades de mantenimiento planificado por parte del proveedor o el cliente, a raíz de las cuales la red o parte de esta queda fuera de servicio por un período
 - Interrupción o degradación del servicio causado por negligencia, error u omisión de cliente. (Ej. Manipulación de cables, cambios en configuración de equipos, etc.)
 - Interrupción o degradación del servicio causado por falla en los equipos de propiedad y responsabilidad del cliente (Ej. Switches LAN, UPS, etc.)
 - Falla o suspensión eléctrica en la localidad.
 - Eventos de avería masiva causada por terceros. (Vandalismo, atentados, desastres naturales, etc.)
 - Eventos que involucren revisión de Planta Externa de Cobre o Fibra desde las 08:00 p.m. a 08:00 a.m. Por disposición Policial y/o Municipal no se permiten trabajos en los postes o armarios por medidas de seguridad.
- ✓ Las demoras en la autorización de ingreso en el local o sede del cliente, ya sea por procedimiento de seguridad y/o protección ambiental que los técnicos deban seguir antes de ingresar al local del cliente, serán consideradas como tiempo de parada de reloj.
- ✓ Se debe entender como Tiempo Máximo de Atención (TMA), al tiempo que transcurre desde que el PROVEEDOR toma conocimiento de la incidencia (ya sea de forma proactiva a través de sus propias herramientas de monitoreo o mediante notificación de la Entidad), hasta que remita a la Entidad, el nro. de ticket de atención, lo cual será aplicable a todos los componentes y subcomponentes de la presente contratación.
- ✓ Se entenderá por tiempo máximo de subsanación (TMS), al tiempo transcurrido desde la generación del ticket de atención, hasta la comunicación del PROVEEDOR con el personal del Ministerio del Interior, indicando la finalización de dicha atención. Cabe señalar que la conformidad de la finalización de la atención, será brindada por el personal encargado del Ministerio del Interior, siendo los tiempos máximos de subsanación los siguientes:

Componente	Descripción	TMS
N° 1	Servicio de Internet	2 horas
N° 2	Servicio de Seguridad Gestionada	2 horas
N° 4	Servicio de Telefonía Fija	4 horas

Tiempos máximos de subsanación de los componentes 1, 2 y 4



PERU Ministerio del Interior

TIPO ZONA	Acceso Fibra	Acceso Radio Punto a Punto
Lima y Urbano	4 horas	4 horas
Semiurbano	12 horas	24 horas
Rural	48 horas	48 horas

Tiempos máximos de subsanación del componente 3:
Servicio de Interconexión para las Sedes del MININTER

- ✓ Las actividades o provisiones de equipamiento, componentes, aplicaciones y/o licenciamiento que deba ejecutar el PROVEEDOR para la atención y subsanación de incidencias del presente servicio, serán sin costo alguno para el Ministerio del Interior.
- ✓ El MININTER gestionará los permisos para los accesos en los inmuebles donde se encuentren sus sedes, brindando las facilidades necesarias para que el PROVEEDOR efectúe las labores en las sedes. El MININTER proporcionará los datos del personal de contacto de las sedes para la realización de las labores.

VI. REGLAMENTOS TÉCNICOS, NORMAS METROLOGICAS Y/O SANITARIAS (De corresponder)

No corresponde:

VII. REQUISITOS MÍNIMOS DEL PROVEEDOR (Obligatorio)

Para la implementación de los servicios

El PROVEEDOR asignará profesionales para la implementación del servicio.

Personal clave:

Jefe de Proyecto (Una (01) persona)

Un Ingeniero Electrónico o de Sistemas o de Telecomunicaciones o de Informática o de Computación o de Telemática, titulado, colegiado y habilitado, quien será el responsable por parte del PROVEEDOR, de las coordinaciones y gestión de la implementación del servicio. Deberá contar con certificación PMP (Profesional en Dirección de Proyectos) y tener experiencia mínima de tres (03) años en gestión de proyectos de Telefonía fija y/o Internet y/o Banda Ancha y/o Seguridad Gestionada y/o Interconexión de Datos y/o Red de Datos y/o Red WAN para la transmisión de datos, voz, e internet a nivel nacional y/o Línea Dedicada para Transmisión de Datos y/o Línea Dedicada para Transmisión de Internet y/o Transmisión de Datos.

Actividades

- Planificar, identificar y priorizar las acciones, actividades y recursos. Elaborar plan de trabajo y cronograma de actividades mínimas.
- Supervisar y controlar la ejecución de las actividades y en especial los recursos: humanos y tecnológicos.
- Resolver las incidencias y problemas, gestionar riesgos.
- Monitorear y supervisar el cumplimiento del plan de trabajo y actividades.
- Presentar al área usuaria los avances en la ejecución de actividades y comunicar los resultados.
- Interactuar entre el área usuaria y el proveedor para la absolución de consultas por parte del área usuaria.

Especialista Implementador (cuatro (04) personas)

Mínimo bachiller en Ingeniería Electrónica o de Sistemas o de Telecomunicaciones o de Informática o de Computación o de Telemática, con experiencia mínima de dos (02) años en implementación y/o configuración y/o instalación de servicios de Internet y/o Banda Ancha y/o



PERÚ Ministerio del Interior

Seguridad Gestionada y/o Interconexión de Datos y/o Red de Datos y/o Red WAN para la transmisión de datos, voz, e internet a nivel nacional y/o Línea Dedicada para Transmisión de Datos y/o Línea Dedicada para Transmisión de Internet y/o Transmisión de Datos.

Deberá contar con personal que posea como mínimo con una de las siguientes certificaciones:

Certificación en la marca de la solución de NGFW ofertada
Certificación en la marca de la solución de Anti DDoS ofertada
Certificación en la marca de la solución de Firewall de Aplicaciones Web ofertada
Certificación en la marca de la solución de Protección de Amenazas Avanzadas ofertada

Actividades

- Instalación y configuración del equipamiento de la solución ofertada.
- Ejecutar pruebas de conectividad y funcionamiento de la solución ofertada
- Verificar que la solución implementada cumpla con lo solicitado por el área usuaria
- Elaborar la documentación técnica para el informe técnico final

Para la ejecución de los servicios implementados

El PROVEEDOR asignará dos (02) profesionales residentes, para el monitoreo y aseguramiento de la operatividad, calidad, entre otros, de los servicios de conectividad, transmisión de datos, internet y seguridad gestionada, desde el día siguiente de haberse culminado la etapa de implementación de los servicios y cuya vigencia será hasta la finalización del contrato.

El horario de trabajo en el MININTER será de lunes a viernes de 08:00 a 16:45 horas.

El MININTER proporcionará un ambiente adecuado para sus labores diarias, y el PROVEEDOR deberá asignar los equipos de cómputo para dicho personal.

Los requisitos mínimos de los profesionales serán los siguientes:

Residente de Datos (Una (01) persona)

Bachiller o Titulado en Ingeniería Electrónica o de Sistemas o de Telecomunicaciones o de Informática o de Computación o de Telemática, con experiencia laboral mínima de dos (02) años en la implantación de servicios similares (Servicios de Internet y/o Banda Ancha y/o Seguridad Gestionada y/o Interconexión de Datos y/o Red de Datos y/o Red WAN para la transmisión de datos, voz, e internet a nivel nacional y/o Línea Dedicada para Transmisión de Datos y/o Línea Dedicada para Transmisión de Internet y/o Transmisión de Datos) al objeto de la convocatoria.

Deberá contar como mínimo con las siguientes certificaciones vigentes:

- Certificación oficial a nivel profesional y/o asociado de networking, switching y/o routing de la marca de equipos de comunicaciones propuestos en la oferta del Postor.

Actividades del Residente de Datos

- ❖ Administrar todos los equipos de los componentes 1 y 3, deberá asegurarse que todas las plataformas y/o servicios contratados por la entidad se encuentren operando y remitiendo información según su operación y funcionamiento
- ❖ Responder a los incidentes y requerimientos de los componentes 1 y 3 en constante coordinación con el NOC del Contratista y los especialistas de la Entidad.
- ❖ Atención de incidencias referidas a los componentes 1 y 3, como la saturación de los enlaces de datos e internet, intermitencia en el servicio, lentitud del servicio, identificaciones de IPs de mayor consumo entre otros
- ❖ Atención de requerimientos, optimizaciones y configuraciones lógicas del equipamiento de los componentes 1 y 3, las cuales deben ser aprobadas por los especialistas de la Entidad

La documentación que acredite el cumplimiento de los requisitos mínimos del Residente de Datos,



PERU Ministerio del Interior

deberá ser remitida a la OGTIC hasta antes de la culminación de la etapa de implementación de los servicios.

Residente de Ciberseguridad (Una (01) persona)

Bachiller o Titulado en Ingeniería Electrónica o de Sistemas o de Telecomunicaciones o de Informática o de Computación o de Telemática, con experiencia laboral mínima de dos (02) años en administración de soluciones de ciberseguridad.

Conocimiento y experiencia en la instalación, configuración, soporte técnico y solución de problemas de los equipos y aplicaciones del COMPONENTE 2: SERVICIO DE SEGURIDAD GESTIONADA DE EQUIPOS PERIMETRALES, propuestos en la oferta del Postor.

Deberá contar como mínimo, con una (01) de las siguientes certificaciones vigente a la fecha de culminación de la etapa de implementación del servicio:

- Certified Ethical Hacker (CEH) y/o
- Certified Security Analyst (ECSA/LPT) y/o
- CompTIA PenTest+ y/o
- Certified Information Systems Security Professional (CISSP) y/o
- Mile2 CPTe (Certified Penetration Testing Engineer) y/o
- Mile2 CPEH Certified Professional Ethical Hacker y/o
- Mile2 CSWAE (Certified Secure Web Application Engineer) y/o
- GIAC Penetration Tester y/o
- OSCE (Offensive Security Certified Expert) y/o
- OSCP (Offensive Security Certified Professional) y/o
- OPST (OSSTMM Professional Security Tester) y/o
- OPSA (OSSTMM Professional Security Analyst) y/o
- Certificación eLearnSecurity infraestructura: eJPT, eCPPT y/o
- Certificación eLearnSecurity aplicaciones: eWPT, eMAPT

Actividades del Residente de Ciberseguridad

- ❖ Administrar todos los equipos del componente 2, deberá asegurarse que todas las plataformas y/o servicios contratados por la entidad se encuentren operando y remitiendo información según su operación y funcionamiento.
- ❖ Responder a los incidentes y requerimientos de seguridad en constante coordinación con SOC y los especialistas de la Entidad.
- ❖ Definir estándares y controles de seguridad apropiados para la plataforma de seguridad gestionada, los cuales serán revisados y aprobados por los especialistas de la Entidad para su implementación.
- ❖ Implementar políticas y procedimientos de seguridad, optimizaciones y configuraciones lógicas del equipamiento de seguridad, las cuales deben ser aprobadas por los especialistas de la entidad.
- ❖ Proponer reuniones técnicas mensuales con los especialistas de la Entidad referente a:
 - Ataques reportados durante el mes y como fueron estos tratados/mitigados.
 - Cambios realizados sobre la configuración solicitados por la Entidad.
 - Cumplimiento de los Niveles de Servicio.
 - Gestión del servicio por parte del proveedor.

La documentación que acredite el cumplimiento de los requisitos mínimos del Residente de Ciberseguridad deberá ser remitida a la OGTIC hasta antes de la culminación de la etapa de implementación del servicio.

VIII. PLAZO DE EJECUCIÓN DE LA PRESTACIÓN (Obligatorio)

El plazo de la ejecución de la prestación es de MIL NOVENTA Y SEIS (1096) días calendario contabilizados a partir del día siguiente de suscrito el acta de implementación del servicio, la cual será emitida por la Oficina de Servicios de Tecnologías y Comunicaciones (OSTC -OGTIC).

MINISTERIO DEL INTERIOR

CONCURSO PUBLICO N° 005-2022-IN-OGAF-OAB-PRIMERA CONVOCATORIA

SERVICIO DE INTERCONEXION, SEGURIDAD, ACCESO A INTERNET Y SERVICIO DE TELEFONIA FIJA PARA EL MININTER



PERU Ministerio del Interior

Plazo de Implementación

El plazo máximo para la implementación del servicio es de CIENTO VEINTE (120) días calendario, contados a partir del día siguiente de la firma del contrato.

IX. DOCUMENTOS PARA LA FIRMA DEL CONTRATO

- El PROVEEDOR, debe entregar la estructura de costos desagregada por Componente, Sub Componente y Sede para la suscripción del contrato.
- Para el caso del servicio de Telefonía Fija, el PROVEEDOR, debe entregar la estructura de costos por tipo de llamada para la suscripción del contrato.
- EL PROVEEDOR debe presentar los números telefónicos de su Centro de Atención de Llamadas y/o Atención al Cliente.
- EL PROVEEDOR deberá presentar los documentos que acrediten el perfil profesional del personal indicado en el numeral VII.
- EL PROVEEDOR deberá presentar su estructura de costos en el siguiente formato

COMPONENTE	SUB COMPONENTE	DESCRIPCIÓN	Costo por MB	Costo Mensual (\$/)	Costo Anual (\$/)	Costo Total 3 años (\$/)
1 SERVICIO DE ACCESO A INTERNET EN LA SEDE PRINCIPAL	1	SERVICIO DE ACCESO A INTERNET EN LA SEDE PRINCIPAL				
		- Sede Central (Enlace Internet Principal)				
		- Sede Central (Enlace Internet Respaldo)				
	2	ADMINISTRADOR DE ANCHO DE BANDA				
2 SERVICIO DE SEGURIDAD GESTIONADA DE EQUIPOS PERIMETRALES	3	SWITCH CORE EN ALTA DISPONIBILIDAD				
	1	NEXT GENERATION FIREWALL (NGFW) EN ALTA DISPONIBILIDAD				
	2	SOLUCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIOS SIMPLES Y DISTRIBUIDOS				
	3	SISTEMA FIREWALL DE APLICACIONES WEB				
3 SERVICIO DE INTERCONEXIÓN PARA LAS SEDES DEL MININTER	4	SOLUCIÓN DE PROTECCIÓN DE AMENAZAS AVANZADAS EN ALTA DISPONIBILIDAD				
	1	SERVICIO DE ACCESO A LA VPN-MININTER para la Sede Principal				
		- Sede Central (Enlace IPVPN Principal)				
		- Sede Central (Enlace IPVPN Respaldo)				
		SERVICIO DE ACCESO A LA VPN-MININTER para las Sedes Remotas:				
	2	- Sede Remota 1 (Nombre de la Sede)				
		- Sede Remota 2 (Nombre de la Sede)				
		- Sede Remota 3 (Nombre de la Sede)				
4 SERVICIO DE TELEFONÍA FIJA		- Sede Remota N (Nombre de la Sede)				
	3	PLATAFORMA DE MONITOREO				
		TIPO DE LLAMADA		Costo por Segundo		
		Discado Directo Local				
		Discado Directo Nacional				
		Discado Directo Celular (Todos los operadores de telefonía móvil)				
		Discado Directo Internacional (Fijo Celular)				
		TOTAL				

X. ENTREGABLES (Obligatorio)

Los entregables deben ser presentados por el PROVEEDOR en digital, a través de la Mesa de Partes Digital del MININTER (<https://sistemas.mininter.gob.pe/mesadepartesdaigital/>). Cabe señalar que la presentación de los documentos será de lunes a viernes en el horario de 8:00 a.m. a 4:00 p.m. de acuerdo a lo señalado en la guía para la presentación online de documentos (<https://sistemas.mininter.gob.pe/mesadepartesdaigital/guia-usuanc/>). Los trámites presentados en la Mesa de Partes Digital, con posterioridad a la hora de atención establecida serán registrados al día hábil siguiente.



PERU Ministerio del Interior

Entregables de la implementación

El PROVEEDOR deberá presentar un Informe Final dirigido hacia la OGTIC, en un plazo máximo de 20 días calendario, posterior a la suscripción del Acta de Implementación. El contenido de dicho informe será como mínimo el siguiente:

- Listado de equipos instalados por sede incluyendo números de serie, marca y modelo del equipo.
- Listado de direccionamiento IP de todos los equipos y circuitos digitales de cada sede instalada.
- Diagrama de diseño de la red instalada en el MININTER y configuración final en formato digital.
- Copia de las guías de entrega de los equipos instalados por el PROVEEDOR.
- Plano impreso en tamaño A2 o superior, donde se muestre la ruta disponible por ambos enlaces y el nombre de cada uno de los POP a los que se conectan.
- Deberá entregar un Acta de Instalación y Pruebas por cada sede instalada, la cual será suscrita entre el Personal de Informática o Administrador o Representante de la Sede del MININTER y el representante del PROVEEDOR.
- Acta de Implementación del servicio emitida por la OSTC-OGTIC.

El informe final deberá ser firmado por el Jefe de Proyecto del PROVEEDOR y deberá ser remitido a la OGTIC (MININTER) para su evaluación respectiva, aprobación y visación correspondiente; en el caso de encontrarse observaciones serán devueltas, mediante documento formal, para ser subsanadas en el plazo máximo de tres (03) días hábiles.

La evaluación que realizará el MININTER será bajo los documentos de ejecución entregados por el PROVEEDOR, donde se evaluará para cada sede implementada todos los servicios, así como la instalación, ubicación y validación de ancho de banda para el caso de las sedes remotas, esto será ejecutado por un personal responsable de la OSTC MININTER.

Entregables durante la vigencia del servicio

El PROVEEDOR entregará un informe dirigido hacia la OGTIC con periodicidad mensual, la misma que deberá ser presentada durante los primeros siete (07) días calendarios posteriores al mes del servicio. Dicho informe deberá contener como mínimo lo siguiente:

Para la gestión de enlaces de datos e Internet el PROVEEDOR deberá entregar:

- Reporte de incidentes ocurridos durante el mes del servicio, conteniendo la siguiente información: N° ticket asignado, N° del circuito digital (CD), nombre de la sede, fecha y hora de inicio del ticket, fecha y hora de cierre del ticket, descripción del problema, origen o causa del problema, acciones correctivas ejecutadas
- Reporte de Consumo de Ancho de Banda. Gráficas de consumo, enlaces con saturación, enlaces sin uso, enlaces normales, observaciones y recomendaciones respecto al consumo de ancho de banda de los enlaces de datos e internet.

Para la gestión de Seguridad Gestionada el PROVEEDOR deberá entregar:

- Reporte mensual del Top de consumo de internet, principales consumos de internet por orígenes. Top de ataques, Top de Vulnerabilidades encontradas en la red, principales fuentes y acciones contra ataques de denegación de servicio y recomendaciones en buenas prácticas en ciberseguridad.
- Reporte de Estado de los Equipos: Tiempo de operación, consumo de Recursos, estado del licenciamiento.

Para la gestión del Servicio de Telefonía Fija el PROVEEDOR deberá entregar:

- Reporte mensual del estado de la telefonía, problemas y solución ejecutada
- Reporte mensual del consumo de minutos del número principal, por tipo de llamada.



PERU

Ministerio del Interior

XI. FORMA DE PAGO (Obligatorio)

Pagos periódicos, mensuales por 36 meses, siendo un pago fijo mensual correspondiente a 1/36 del monto del Contrato Original, para lo cual se empleará la siguiente fórmula:

$$\text{Pago Mensual} = (1/36) \times 100\% \times M$$

Donde:

M = Monto del Contrato Original

El pago se ejecutará una vez validada la conformidad del servicio y firmada el Acta de Implementación del Servicio.

Para efectos del pago de las contraprestaciones ejecutadas por el PROVEEDOR, este deberá presentar la documentación durante los primeros cinco (05) días posteriores al mes del servicio para de efectos de conformidad, para tal efecto la Entidad deberá contar con la siguiente documentación:

- Informe mensual (Entregables durante la vigencia del servicio), el mismo que se encuentra indicado en el numeral X. ENTREGABLES, del presente documento.
- Factura.

El MININTER realizará el pago de las contraprestaciones pactadas a favor del PROVEEDOR dentro de los diez (10) días calendarios siguientes de la conformidad dada por el área usuaria, siempre que se verifiquen las condiciones establecidas en la orden de servicio y/o contrato.

XII. LUGAR DE PRESTACIÓN DEL SERVICIO (Obligatorio)

COMPONENTE 1: SERVICIO DE ACCESO A INTERNET EN LA SEDE PRINCIPAL

En el Centro de Datos de la Oficina General de Tecnologías de la Información y Comunicaciones – OGTIC, ubicado en la Sede Central del Ministerio del Interior sito en, Plaza 30 de agosto s/n Urb. Corpac - San Isidro - Lima.

COMPONENTE 2: SERVICIO DE SEGURIDAD GESTIONADA DE EQUIPOS PERIMETRALES.

En el Centro de Datos de la Oficina General de Tecnologías de la Información y Comunicaciones – OGTIC, ubicado en la Sede Central del Ministerio del Interior sito en, Plaza 30 de agosto s/n Urb. Corpac - San Isidro - Lima.

COMPONENTE 3: SERVICIO DE INTERCONEXIÓN PARA LAS SEDES DEL MININTER

- Sub Componente 1: Servicio de acceso a la VPN-MININTER para la Sede Principal
En el Centro de Datos de la Oficina General de Tecnologías de la Información y Comunicaciones – OGTIC, ubicado en la Sede Central del Ministerio del Interior sito en, Plaza 30 de agosto s/n Urb. Corpac - San Isidro - Lima.
- Sub Componente 2: Servicio de acceso a la VPN-MININTER para las Sedes Remotas
En cada una de las direcciones indicadas en el Anexo B

COMPONENTE 4: SERVICIO DE TELEFONÍA FIJA

En el Centro de Datos de la Oficina General de Tecnologías de la Información y Comunicaciones – OGTIC, ubicado en la Sede Central del Ministerio del Interior sito en, Plaza 30 de agosto s/n Urb. Corpac - San Isidro - Lima.

XIII. CONFORMIDAD DEL SERVICIO (Obligatorio)

Será brindada por el Director de la Oficina de Servicios de Tecnologías y Comunicaciones (OSTC) de la OGTIC, previa verificación del cumplimiento del servicio de acuerdo a lo establecido en el presente documento.

La conformidad se regula conforme a las disposiciones establecidas en el artículo 168° del



PERU Ministerio del Interior

Reglamento de la Ley de Contrataciones del Estado.

XIV. PENALIDADES (Obligatorio)**Penalidad por mora en la ejecución de la prestación del servicio:**

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

$$\text{Penalidad diaria} = 0.10 \times \text{Monto vigente} \\ F \times \text{Plazo vigente en días}$$

Donde F tiene los siguientes valores:

- a) Para plazos menores o iguales a sesenta (60) días para bienes, servicios en general, consultorías y ejecución: $F = 0.40$
- b) Para plazos mayores a sesenta (60) días: $F = 0.25$
 - b.1) Para bienes, servicios en general y consultorías: $F = 0.25$
 - b.2) Para obras: $F = 0.15$

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato o ítem que debió ejecutarse o, en caso que estos involucraran obligaciones de ejecución periódica o entregas parciales, a la presentación individual que fuera materia de retraso.

En caso no sea posible cuantificar el monto de la presentación materia de retraso, la Entidad puede establecer en los documentos del procedimiento de selección la penalidad a aplicarse.

Para los supuestos que, por la naturaleza de la contratación, la fórmula indicada en el presente artículo no cumpla con su finalidad, el Ministerio de Economía y Finanzas mediante Resolución Ministerial puede establecer fórmulas especiales para el cálculo de la penalidad por mora.

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 ese 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.

XV. OTRAS PENALIDADES (De corresponder)

OTRAS PENALIDADES			
N°	SUPUESTOS DE APLICACIÓN	FORMA DE CÁLCULO	PROCEDIMIENTO
1	Penalidad por exceso de tiempo en la atención	Monto de la penalidad = $0.10 \times \text{Valor de la UIT} \times \text{Cantidad de tickets}$	El tiempo máximo de atención (TMA) de cada requerimiento o incidencia reportada será de 30 minutos. Se aplicará una penalidad del 10% del valor de la UIT por cada ticket de atención, cuyo TMA supere los 30min. Dónde: UIT: Unidad Impositiva Tributaria vigente
2	Penalidad por exceso de tiempo de subsanación	Monto de la penalidad = $0.0014 \times \text{Monto mensual del servicio}$	La penalidad a aplicarse será de 0.14% por cada hora o fracción de hora excedida; y será aplicada al costo mensual del servicio en la sede afectada; costo que será tomado de la Estructura de costos que presentó el PROVEEDOR para la suscripción del contrato, para el componente de seguridad gestionada se aplicará sobre el costo mensual del sub componente afectado. Cabe precisar que 0.14% representa a la unidad de tiempo de 1 hora, considerando que el mes tiene en promedio 720 horas.

MINISTERIO DEL INTERIOR

CONCURSO PUBLICO N° 005-2022-IN-OGAF-OAB-PRIMERA CONVOCATORIA

SERVICIO DE INTERCONEXION, SEGURIDAD, ACCESO A INTERNET Y SERVICIO DE TELEFONIA FIJA PARA EL MININTER



PERU Ministerio del Interior

OTRAS PENALIDADES																	
N°	SUPUESTOS DE APLICACIÓN	FORMA DE CÁLCULO	PROCEDIMIENTO														
			En caso la avería afecte a toda la entidad, la aplicación de la penalidad se realizará sobre el monto mensual total de servicio.														
Penalidad por nivel de disponibilidad del servicio:																	
La disponibilidad es una medida que nos indica cuánto tiempo está operativo o funcionando un recurso o servicio informático, respecto a la duración total que se espera se mantenga operativo. Típicamente se expresa en porcentaje.																	
La disponibilidad del servicio contratado es responsabilidad del PROVEEDOR, a excepción de casos fortuitos, ajenas al PROVEEDOR como desastres naturales, vandalismo (robos de cable) o situaciones no previstas y no contemplados en la normatividad vigente, los cuales deberán ser debidamente sustentados y aprobados por el Ministerio del Interior.																	
3	Penalidad por nivel de disponibilidad del servicio: COMPONENTE 1: SERVICIO DE ACCESO A INTERNET EN LA SEDE PRINCIPAL	Monto de la penalidad = Monto mensual del servicio x Penalidad	El cálculo de disponibilidad se realizará de manera mensual para lo cual se aplicará la siguiente fórmula: $\text{Disponibilidad} = \left(\frac{\text{THM} - \text{Tiempo Imputable}}{\text{THM}} \right) \times 100$ Donde: THM=Total de Horas del Mes TPR=Tiempo de parada de reloj El tiempo de parada de reloj se define como aquel tiempo en el cual, notificada la avería por la Entidad, ésta no logra brindarle al PROVEEDOR las facilidades de acceso a sus equipos ubicados en las instalaciones de la Entidad. TTA=Tiempo Total de Avería El Tiempo Total de Avería se define como el tiempo transcurrido desde que se le notifica al PROVEEDOR respecto a la avería presentada, hasta el momento en el que el PROVEEDOR soluciona o resuelve la avería. Tiempo Imputable=(TTA-TPR) En caso no se logre alcanzar el nivel de disponibilidad establecido se aplicará la penalidad según la siguiente tabla: <table><tr><th>NIVEL DE DISPONIBILIDAD</th><th>PENALIDAD</th></tr><tr><td>De 99.95% a 100.00%</td><td>0%</td></tr><tr><td>De 99.80% a 99.94%</td><td>2%</td></tr><tr><td>De 99.70% a 99.79%</td><td>4%</td></tr><tr><td>De 99.60% a 99.69%</td><td>6%</td></tr><tr><td>De 99.50% a 99.59%</td><td>8%</td></tr><tr><td>Menor a 99.50%</td><td>10%</td></tr></table>	NIVEL DE DISPONIBILIDAD	PENALIDAD	De 99.95% a 100.00%	0%	De 99.80% a 99.94%	2%	De 99.70% a 99.79%	4%	De 99.60% a 99.69%	6%	De 99.50% a 99.59%	8%	Menor a 99.50%	10%
NIVEL DE DISPONIBILIDAD	PENALIDAD																
De 99.95% a 100.00%	0%																
De 99.80% a 99.94%	2%																
De 99.70% a 99.79%	4%																
De 99.60% a 99.69%	6%																
De 99.50% a 99.59%	8%																
Menor a 99.50%	10%																
4	Penalidad por nivel de disponibilidad del servicio: COMPONENTE 2: SERVICIO DE SEGURIDAD GESTIONADA DE EQUIPOS PERIMETRALES	Monto de la penalidad = Monto mensual del servicio x Penalidad	El cálculo de disponibilidad se realizará de manera mensual para lo cual se aplicará la siguiente fórmula: $\text{Disponibilidad} = \left(\frac{\text{THM} - \text{Tiempo Imputable}}{\text{THM}} \right) \times 100$ Donde: THM=Total de Horas del Mes TPR=Tiempo de parada de reloj El tiempo de parada de reloj se define como aquel tiempo en el cual, notificada la avería por la Entidad, ésta no logra brindarle al PROVEEDOR las facilidades de acceso a sus equipos ubicados en las instalaciones de la Entidad. TTA=Tiempo Total de Avería														



PERU Ministerio del Interior

OTRAS PENALIDADES																															
N°	SUPUESTOS DE APLICACIÓN	FORMA DE CÁLCULO	PROCEDIMIENTO																												
			<p>El Tiempo Total de Avería se define como el tiempo transcurrido desde que se le notifica al PROVEEDOR respecto a la avería presentada, hasta el momento en el que el PROVEEDOR soluciona o resuelve la avería.</p> <p>Tiempo Imputable=(TTA-TPR)</p> <p>En caso no se logre alcanzar el nivel de disponibilidad establecido para cada componente se aplicará la penalidad según corresponda a una de las siguientes tablas:</p> <p>Soluciones en alta disponibilidad</p> <table><tr><th>NIVEL DE DISPONIBILIDAD</th><th>PENALIDAD</th></tr><tr><td>De 99.80% a 100.00%</td><td>0%</td></tr><tr><td>De 99.70% a 99.79%</td><td>2%</td></tr><tr><td>De 99.60% a 99.69%</td><td>4%</td></tr><tr><td>De 99.50% a 99.59%</td><td>6%</td></tr><tr><td>De 99.40% a 99.49%</td><td>8%</td></tr><tr><td>Menor a 99.40%</td><td>10%</td></tr></table> <p>Resto de Soluciones</p> <table><tr><th>NIVEL DE DISPONIBILIDAD</th><th>PENALIDAD</th></tr><tr><td>De 99.50% a 100.00%</td><td>0%</td></tr><tr><td>De 99.40% a 99.49%</td><td>2%</td></tr><tr><td>De 99.30% a 99.39%</td><td>4%</td></tr><tr><td>De 99.20% a 99.29%</td><td>6%</td></tr><tr><td>De 99.10% a 99.19%</td><td>8%</td></tr><tr><td>Menor a 99.10%</td><td>10%</td></tr></table>	NIVEL DE DISPONIBILIDAD	PENALIDAD	De 99.80% a 100.00%	0%	De 99.70% a 99.79%	2%	De 99.60% a 99.69%	4%	De 99.50% a 99.59%	6%	De 99.40% a 99.49%	8%	Menor a 99.40%	10%	NIVEL DE DISPONIBILIDAD	PENALIDAD	De 99.50% a 100.00%	0%	De 99.40% a 99.49%	2%	De 99.30% a 99.39%	4%	De 99.20% a 99.29%	6%	De 99.10% a 99.19%	8%	Menor a 99.10%	10%
NIVEL DE DISPONIBILIDAD	PENALIDAD																														
De 99.80% a 100.00%	0%																														
De 99.70% a 99.79%	2%																														
De 99.60% a 99.69%	4%																														
De 99.50% a 99.59%	6%																														
De 99.40% a 99.49%	8%																														
Menor a 99.40%	10%																														
NIVEL DE DISPONIBILIDAD	PENALIDAD																														
De 99.50% a 100.00%	0%																														
De 99.40% a 99.49%	2%																														
De 99.30% a 99.39%	4%																														
De 99.20% a 99.29%	6%																														
De 99.10% a 99.19%	8%																														
Menor a 99.10%	10%																														
5	Penalidad por nivel de disponibilidad del servicio COMPONENTE 3: SERVICIO DE INTERCONEXIÓN PARA LAS SEDES DEL MININTER	Monto de la penalidad = Monto mensual del servicio x Penalidad	<p>El cálculo de disponibilidad se realizará de manera mensual para lo cual se aplicará la siguiente fórmula</p> $\text{Disponibilidad} = \left(1 - \frac{\sum \text{Tiempo Imputable}}{\text{Cantidad de Enlaces} \times \text{THM}} \right) \times 100$ <p>Donde:</p> <p>THM=Total de Horas del Mes TPR=Tiempo de parada de reloj</p> <p>El tiempo de parada de reloj se define como aquel tiempo en el cual, notificada la avería por la Entidad, esta no logra brindarle al PROVEEDOR las facilidades de acceso a sus equipos ubicados en las instalaciones de la Entidad.</p> <p>TTA=Tiempo Total de Avería</p> <p>El Tiempo Total de Avería se define como el tiempo transcurrido desde que se le notifica al PROVEEDOR respecto a la avería presentada, hasta el momento en el que el PROVEEDOR soluciona o resuelve la avería.</p> <p>Tiempo Imputable=(TTA-TPR)</p> <p>En caso no se logre alcanzar el nivel de disponibilidad establecido para cada componente se aplicará la penalidad según corresponda a una de las siguientes tablas:</p> <p>Acceso mediante FO</p> <table><tr><th>ZONA: LIMA y URBANO</th><th>PENALIDAD</th></tr><tr><td>NIVEL DE DISPONIBILIDAD</td><td></td></tr><tr><td>De 99.90% a 100.00%</td><td>0%</td></tr></table>	ZONA: LIMA y URBANO	PENALIDAD	NIVEL DE DISPONIBILIDAD		De 99.90% a 100.00%	0%																						
ZONA: LIMA y URBANO	PENALIDAD																														
NIVEL DE DISPONIBILIDAD																															
De 99.90% a 100.00%	0%																														



PERU Ministerio del Interior

OTRAS PENALIDADES

N°	SUPUESTOS DE APLICACIÓN	FORMA DE CÁLCULO	PROCEDIMIENTO	
			De 99.80% a 99.89%	2%
			De 99.70% a 99.79%	4%
			De 99.60% a 99.69%	5%
			De 99.50% a 99.59%	8%
			Menor a 99.50%	10%
			ZONA: SEMI URBANO NIVEL DE DISPONIBILIDAD	PENALIDAD
			De 99.80% a 100.00%	0%
			De 99.70% a 99.79%	2%
			De 99.60% a 99.69%	4%
			De 99.50% a 99.59%	6%
			De 99.40% a 99.49%	8%
			Menor a 99.40%	10%
			ZONA: RURAL NIVEL DE DISPONIBILIDAD	PENALIDAD
			De 99.00% a 100.00%	0%
			De 98.90% a 98.99%	2%
			De 98.80% a 98.89%	4%
			De 98.70% a 98.79%	6%
			De 98.60% a 98.69%	8%
			Menor a 98.60%	10%
			Acceso mediante Radio Punto a Punto	
			ZONA: LIMA y URBANO NIVEL DE DISPONIBILIDAD	PENALIDAD
			De 99.30% a 100.00%	0%
			De 99.20% a 99.29%	2%
			De 99.10% a 99.19%	4%
			De 99.00% a 99.09%	6%
			De 98.90% a 98.99%	8%
			Menor a 98.90%	10%
			ZONA: SEMI URBANO - RADIO NIVEL DE DISPONIBILIDAD	PENALIDAD
			De 99.00% a 100.00%	0%
			De 98.90% a 98.99%	2%
			De 98.80% a 98.89%	4%
			De 98.70% a 98.79%	6%
			De 98.60% a 98.69%	8%
			Menor a 98.60%	10%
			ZONA: RURAL NIVEL DE DISPONIBILIDAD	PENALIDAD
			De 98.50% a 100.00%	0%
			De 98.40% a 98.49%	2%
			De 98.30% a 98.39%	4%
			De 98.20% a 98.29%	6%
			De 98.10% a 98.19%	8%
			Menor a 98.10%	10%



PERU Ministerio del Interior

OTRAS PENALIDADES																	
Nº	SUPUESTOS DE APLICACIÓN	FORMA DE CÁLCULO	PROCEDIMIENTO														
5.	Penalidad por nivel de disponibilidad del servicio. COMPONENTE 4: SERVICIO DE TELEFONIA FIJA	Monto de la penalidad = Monto mensual del servicio x Penalidad	<p>El cálculo de disponibilidad se realizará de manera mensual para lo cual se aplicará la siguiente fórmula:</p> $\text{Disponibilidad} = \left(\frac{\text{THM} - \text{Tiempo inaputable}}{\text{THM}} \right) \times 100$ <p>Donde:</p> <p>THM=Total de Horas del Mes TPR=Tiempo de parada de reloj</p> <p>El tiempo de parada de reloj se define como aquel tiempo en el cual, notificada la avería por la Entidad, esta no logra brindar al PROVEEDOR las facilidades de acceso a sus equipos ubicados en las instalaciones de la Entidad</p> <p>TTA=Tiempo Total de Avería</p> <p>El Tiempo Total de Avería se define como el tiempo transcurrido desde que se le notifica al PROVEEDOR respecto a la avería presentada, hasta el momento en el que el PROVEEDOR soluciona o resuelve la avería</p> <p>Tiempo Imputable=(TTA-TPR)</p> <p>En caso no se logre alcanzar el nivel de disponibilidad establecido para cada componente se aplicará la penalidad según la siguiente tabla:</p> <table border="1"> <thead> <tr> <th>NIVEL DE DISPONIBILIDAD</th> <th>PENALIDAD</th> </tr> </thead> <tbody> <tr> <td>De 99.95% a 100.00%</td> <td>0%</td> </tr> <tr> <td>De 99.80% a 99.94%</td> <td>2%</td> </tr> <tr> <td>De 99.70% a 99.79%</td> <td>4%</td> </tr> <tr> <td>De 99.60% a 99.69%</td> <td>6%</td> </tr> <tr> <td>De 99.50% a 99.59%</td> <td>8%</td> </tr> <tr> <td>Menor a 99.50%</td> <td>10%</td> </tr> </tbody> </table>	NIVEL DE DISPONIBILIDAD	PENALIDAD	De 99.95% a 100.00%	0%	De 99.80% a 99.94%	2%	De 99.70% a 99.79%	4%	De 99.60% a 99.69%	6%	De 99.50% a 99.59%	8%	Menor a 99.50%	10%
NIVEL DE DISPONIBILIDAD	PENALIDAD																
De 99.95% a 100.00%	0%																
De 99.80% a 99.94%	2%																
De 99.70% a 99.79%	4%																
De 99.60% a 99.69%	6%																
De 99.50% a 99.59%	8%																
Menor a 99.50%	10%																

XVI. DISPOSICIONES DE CONFIDENCIALIDAD (Obligatorio)

El PROVEEDOR se obliga a mantener y guardar estricta reserva y absoluta confidencialidad de todos los documentos e informaciones del Ministerio del Interior a los que tenga acceso en la ejecución del servicio. Se entiende que la obligación asumida por el PROVEEDOR está referida no solo a los documentos e informaciones señalados como "confidenciales" si no a todos los documentos e informaciones que en razón del presente servicio o vinculado con la ejecución del mismo, puedan ser conocidos a través del PROVEEDOR.

XVII. CLÁUSULA DE ANTICORRUPCIÓN (Obligatorio)

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,



PERÚ Ministerio del Interior

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.

XVIII. OTROS (De corresponder)

No corresponde

MINISTERIO DEL INTERIOR
CONCURSO PUBLICO N° 005-2022-IN-OGAF-OAB-PRIMERA CONVOCATORIA
SERVICIO DE INTERCONEXION, SEGURIDAD, ACCESO A INTERNET Y SERVICIO DE TELEFONIA FIJA
PARA EL MININTER



PERÚ

Ministerio del Interior

ANEXO A
MINISTERIO DEL INTERIOR - NODO CENTRAL

N°	TIPO DE SERVICIO	SEDE	DPTO	PROV	DIST	DIRECCIÓN	Caudal de Voz	Velocidad
1	IPVPN PRINCIPAL	LIMA	LIMA	LIMA	SAN ISIDRO	AV. CANAVAL Y MOREYRA CORPAC - SAN ISIDRO	5 Mbps	200
2	IPVPN - BACKUP						5 Mbps	200
3	INTERNET PRINCIPAL	LIMA	LIMA	LIMA	SAN ISIDRO	AV. CANAVAL Y MOREYRA CORPAC - SAN ISIDRO	N/A	365
4	INTERNET SECUNDARIO						N/A	365



PERU Ministerio del Interior

ANEXO B

MINISTERIO DEL INTERIOR - SEDES REMOTAS

N°	NOMBRE DE SEDE	DPTO.	PROV.	DIST.	DIRECCIÓN	VELOCIDAD (Mbps)	CAUDAL VOZ	TIPO ZONA
1	PROCURADURÍA TRÁFICO DE DROGAS	Ancash	Huarez	Huarez	Av. Luzuriaga N° 527 Piso 3 Oficina 302	4	128 Kbps	Urbano
2	PROCURADURÍA TRÁFICO DE DROGAS	Ancash	Chimbote	Chimbote	Mz.C Lt 15 Urb. Mariscal Luzuriaga Nuevo Chimbote	4	128 Kbps	Urbano
3	DEFENSORÍA DE LA POLICÍA	Arequipa	Arequipa	Cercado	Urb. Los Víncos Mz. C Lt-5 San Jerónimo	4	128 Kbps	Urbano
4	PROCURADURÍA TRÁFICO DE DROGAS	Arequipa	Arequipa	Cercado	Cta. Los Girasoles N° 201 Piso 2 Residencial Selva Alegre Cercado	4	128 Kbps	Urbano
5	PROCURADURÍA TRÁFICO DE DROGAS	Ayacucho	Huamanga	Huamanga	Jr. San Martín N° 443, Interior H. Piso 3	4	128 Kbps	Urbano
6	PROCURADURÍA TRÁFICO DE DROGAS	Cajamarca	Cajamarca	Cajamarca	Jr. Luis Robaza Neyra N° 680 Piso 3	4	128 Kbps	Urbano
7	PROCURADURÍA TRÁFICO DE DROGAS	Cusco	Cusco	Cusco	Av. El Sol N° 948 Ofic. 307 Piso 3 - CC Cusco Sol - Plaza	4	128 Kbps	Urbano
8	PROCURADURÍA TRÁFICO DE DROGAS	Cusco	La Convención	Pichari	Jr. Huascar Mz. 1-1 Lote 14 Urb. Villa Central -Pichari	4	128 Kbps	Rural
9	PROCURADURÍA TRÁFICO DE DROGAS	Huánuco	Huánuco	Huánuco	Jr. 2 de Mayo N° 1310 Ofic. 06 Piso 4	4	128 Kbps	Urbano
10	PROCURADURÍA TRÁFICO DE DROGAS	Ica	Ica	Ica	Av. San Martín N° 446 Piso 2	4	128 Kbps	Urbano
11	DEFENSORÍA DE LA POLICÍA	Junín	Huancayo	El Tambo	Jr. Julio C. Tello N° 766	4	128 Kbps	Urbano
12	PROCURADURÍA TRÁFICO DE DROGAS	Junín	Huancayo	Tambo	Calle Real N° 582 Ofic. 204 Tambo	4	128 Kbps	Urbano
13	PROCURADURÍA TRÁFICO DE DROGAS	Junín	Salpo	Salpo	Jr. San Martín N° 796 Esg. con Julio C. Tello - Salpo	4	128 Kbps	Semiurbano
14	DEFENSORÍA DE LA POLICÍA	La Libertad	Trujillo	Trujillo	Calle Franz Schubert N° 743 Urb. Primavera	4	128 Kbps	Urbano
15	PROCURADURÍA TRÁFICO DE DROGAS	La Libertad	Trujillo	Trujillo	Ca. Puerto Príncipe Mz.G Lote 4 Urb. Las Capulianas	4	128 Kbps	Urbano
16	PROCURADURÍA TRÁFICO DE DROGAS	Lambayeque	Chiclayo	Chiclayo	Ca. Elías Aguirre N° 748 Oficina 202 Cercado	4	128 Kbps	Urbano
17	DEFENSORÍA DE LA POLICÍA	Lima	Lima	Jesús María	Av. Brasil Cars. 26 SN - Hospital Nacional PNP	4	128 Kbps	Urbano
18	DEFENSORÍA DE LA POLICÍA	Lima	Lima	Rimac	Complejo Policial "Juan Benites Luna" Jr. Los Cibeles N° 191	4	128 Kbps	Urbano
19	DIRECCIÓN GENERAL DE CRIMEN ORGANIZADO	Lima	Lima	Asa - Vialité	Av. Marco Puente Llanos S/N, Alt. Km 6.5 Carretera Central	4	128 Kbps	Urbano
20	DEFENSORÍA DE LA POLICÍA	Lima	Lima	Lince	Jr. Córdova N° 2580	6	128 Kbps	Urbano
21	OFICINA GENERAL DE ADMINISTRACIÓN	Lima	Callao	Cercado Callao	Av. Argentina N° 2175	6	128 Kbps	Urbano
22	DIRECCIÓN GENERAL DE ORDEN PÚBLICO	Lima	Lima	Pueblo Libre	Jr. José Santiago Wagner N° 2002	6	128 Kbps	Urbano
23	PROCURADURÍA DE TERRORISMO	Lima	Lima	Miraflores	Ca. Coronel Francisco Bolognesi N° 125 Piso 3	6	128 Kbps	Urbano
24	RENIEC	Lima	Lima	San Borja	Jr. Titiano Vecellio N° 245	6	128 Kbps	Urbano

MINISTERIO DEL INTERIOR
CONCURSO PUBLICO N° 005-2022-IN-OGAF-OAB-PRIMERA CONVOCATORIA
SERVICIO DE INTERCONEXION, SEGURIDAD, ACCESO A INTERNET Y SERVICIO DE TELEFONIA FIJA
PARA EL MININTER

N°	NOMBRE DE SEDE	DPTO.	PROV.	DIST.	DIRECCIÓN	VELOCIDAD (Mbps)	CAUDAL VOZ	TIPO ZONA
25	PROCURADURIA PUBLICA ESPECIALIZADA EN DELITOS DE ORDEN PUBLICO	Lima	Lima	Pueblo Libre	Parque Bahía N° 162	6	128 Kbps	Urbano
26	PROCURADURIA DE LAVADO DE ACTIVOS	Lima	Lima	San Isidro	Av. Ricardo Aguado (Calle Uno) N° 416 Urb. Corpac	10	128 Kbps	Urbano
27	PROCURADURIA DEL SECTOR INTERIOR	Lima	Lima	Lima	Jr. Brigadier Malco Pumacahua N° 2749	10	128 Kbps	Urbano
28	DIRECCIÓN GENERAL DE GOBIERNO INTERIOR	Lima	Lima	San Borja	Jifon Mercator N° 432	12	128 Kbps	Urbano
29	PROCURADURIA TRÁFICO DE DROGAS	Lima	Lima	San Isidro	Av. Republica de Panama N° 3542	12	128 Kbps	Urbano
30	DEFENSORIA DE LA POLICIA	Loreto	Iquitos	Iquitos	Calle Moore N° 568	4	128 Kbps	Urbano
31	PROCURADURIA TRÁFICO DE DROGAS	Loreto	Maynas	Iquitos	Jr. Moore N° 756 Oficina 1 - Maynas	4	128 Kbps	Urbano
32	PROCURADURIA TRÁFICO DE DROGAS	Madre de Dios	Tambopata	Tambopata	Av. Tambopata N° 457 Mz. 9L Lj. 5A Ofic. 201 Piso 2	4	128 Kbps	Urbano
33	PROCURADURIA TRÁFICO DE DROGAS	Moquegua	Mancos	Moquegua	Calle Tarapaca N° 350A Ofic. 04 Piso 2	4	128 Kbps	Urbano
34	PROCURADURIA TRÁFICO DE DROGAS	Piura	Piura	Piura	Calle Cusco N° 660 - Piso 2	4	128 Kbps	Urbano
35	PROCURADURIA TRÁFICO DE DROGAS	Puno	Puno	Puno	Jr. Arequipa N° 1146 Oficina 102	4	128 Kbps	Urbano
36	PROCURADURIA TRÁFICO DE DROGAS	Puno	San Román	Juliaca	Jr. La Mar N° 226 - 234, Ofic. 204 Barrio Zaramilla	4	128 Kbps	Urbano
37	PROCURADURIA TRÁFICO DE DROGAS	San Martín	Tarapoto	Tarapoto	Jr. Sachapichu N° 371 Piso 3	4	128 Kbps	Urbano
38	PROCURADURIA TRÁFICO DE DROGAS	Tarma	Tarma	Tarma	Ca. Hipólito Unzueta N° 608 Piso 2	4	128 Kbps	Urbano
39	PROCURADURIA TRÁFICO DE DROGAS	Tumbes	Tumbes	Tumbes	Ca. Los Topacios Mz E L1 18 Urb Jose Lishner Tudela Puyango	4	128 Kbps	Urbano
40	PROCURADURIA TRÁFICO DE DROGAS	Ucayali	Coronel Portilla	Callena	Paseo Lazaro Cohen N° 143 2do Piso, Ofic. 201 (Mz. 46-E, Lote 5C)	4	128 Kbps	Urbano

Firma del Responsable del Área Usuaría

3.2. REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD LEGAL
	HABILITACIÓN
	<u>Requisitos:</u> Autorización emitida por el Ministerio de Transportes y Comunicaciones para que el Contratista pueda brindar servicios de telecomunicaciones en el Perú, en la modalidad de servicios de interconexión, seguridad, acceso a internet y servicio de telefonía fija para el MININTER
	Importante <i>De conformidad con la Opinión N° 186-2016/DTN, la habilitación de un postor, está relacionada con cierta atribución con la cual debe contar el proveedor para poder llevar a cabo la actividad materia de contratación, este es el caso de las actividades reguladas por normas en las cuales se establecen determinados requisitos que las empresas deben cumplir a efectos de estar habilitadas para la ejecución de determinado servicio o estar autorizadas para la comercialización de ciertos bienes en el mercado.</i>
	<u>Acreditación:</u> Copia simple de la resolución vigente que autoriza la concesión para brindar servicios de telecomunicaciones o certificado de registro de empresas prestadoras de servicios de valor añadido
	Importante <i>En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito.</i>

B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.3.1	FORMACIÓN ACADÉMICA
	Jefe de Proyecto (01) <u>Requisitos:</u> Un Ingeniero Electrónico o de Sistemas o de Telecomunicaciones o de Informática o de Computación o de Telemática, titulado, colegiado y habilitado. <u>Acreditación:</u> El TÍTULO PROFESIONAL REQUERIDO 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: http://www.titulosinstitutos.pe/ , según corresponda. En caso TÍTULO PROFESIONAL REQUERIDO no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
	Especialista Implementador (04) <u>Requisitos:</u> Mínimo bachiller en Ingeniería Electrónica o de Sistemas o de Telecomunicaciones o de Informática o de Computación o de Telemática <u>Acreditación:</u>

El GRADO REQUERIDO 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: <http://www.titulosinstitutos.pe/>, según corresponda.

En caso el GRADO REQUERIDO no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

B.4 EXPERIENCIA DEL PERSONAL CLAVE

Jefe de Proyecto (01)

Experiencia

Experiencia mínima de tres (03) años en gestión de proyectos de Telefonía fija y/o Internet y/o Banda Ancha y/o Seguridad Gestionada y/o Interconexión de Datos y/o Red de Datos y/o Red WAN para la transmisión de datos, voz, e internet a nivel nacional y/o Línea Dedicada para Transmisión de Datos y/o Línea Dedicada para Transmisión de Internet y/o Transmisión de Datos.

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

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.

Especialista Implementador (cuatro (04) personas)

Experiencia

Experiencia mínima de dos (02) años en implementación y/o configuración y/o instalación de servicios de Internet y/o Banda Ancha y/o Seguridad Gestionada y/o Interconexión de Datos y/o Red de Datos y/o Red WAN para la transmisión de datos, voz, e internet a nivel nacional y/o Línea Dedicada para Transmisión de Datos y/o Línea Dedicada para Transmisión de Internet y/o Transmisión de Datos

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Importante

- Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.
- En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.
- Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.
- Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.

C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a DIEZ MILLONES Y 00/100 SOLES (S/10'000,000.00), por la prestación de servicios iguales o similares al objeto de la convocatoria, durante un periodo de ocho (08) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran servicios similares a los siguientes:</p> <ul style="list-style-type: none"> a) Servicio de Telefonía fija b) Servicio de Internet c) Servicio de Internet Banda Ancha d) Servicio de Seguridad Gestionada e) Servicio de Telefonía Móvil f) Servicio de Interconexión de Datos g) Servicio de Red de Datos h) Servicio de Red WAN para la transmisión de datos, voz, e internet a nivel nacional i) Servicio de Línea Dedicada para Transmisión de Datos j) Servicio de Línea Dedicada para Transmisión de Internet k) Servicio de Transmisión de Datos <p><u>Acreditación:</u></p> <p>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 pago³, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <p>En el caso de 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.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se</p>

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

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

(...)

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

presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**.

Cuando en los contratos, órdenes de 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.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.

Importante

- *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.*
- *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

Importante

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

CAPÍTULO IV
FACTORES DE EVALUACIÓN

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

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

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

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.

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 [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], que celebra de una parte [CONSIGNAR EL NOMBRE DE LA ENTIDAD], en adelante LA ENTIDAD, con RUC N° [.....], con domicilio legal en [.....], representada por [.....], identificado con DNI N° [.....], y de otra parte [.....], con RUC N° [.....], con domicilio legal en [.....], inscrita en la Ficha N° [.....] Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], debidamente representado por su Representante Legal, [.....], con DNI N° [.....], según poder inscrito en la Ficha N° [.....], Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [.....], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO DE SELECCIÓN]** para la contratación de [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], 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 [CONSIGNAR EL OBJETO DE LA CONTRATACIÓN].

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 PAGO¹⁰

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.

¹⁰ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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, 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 ÚLTIMO 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."

En el caso que corresponda, consignar lo siguiente:

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

Importante

Al amparo de lo dispuesto en el numeral 151.2 del artículo 151 del Reglamento de la Ley de Contrataciones del Estado, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato de la prestación accesorio como garantía de fiel cumplimiento de prestaciones accesorias, debe consignarse lo siguiente:

- "De fiel cumplimiento por prestaciones accesorias: [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."

Importante

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

CLÁUSULA 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 cumpliera a cabalidad con la subsanación, LA ENTIDAD puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

Este procedimiento no resulta aplicable cuando los servicios manifestamente 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 DÉCIMA: 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 UNDÉCIMA: 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 [CONSIGNAR TIEMPO EN AÑOS, NO MENOR DE UN (1) AÑO] año(s) contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA DUODECIMA: 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 TERCERA: 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 CUARTA: 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 QUINTA: 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 SEXTA: 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 SETIMA: SOLUCIÓN DE CONTROVERSIAS¹¹

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

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

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

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

CLÁUSULA DÉCIMA OCTAVA: 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 NOVENA: 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"

¹¹ 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).

MINISTERIO DEL INTERIOR

CONCURSO PUBLICO N° 005-2022-IN-OGAF-OAB-PRIMERA CONVOCATORIA

SERVICIO DE INTERCONEXION, SEGURIDAD, ACCESO A INTERNET Y SERVICIO DE TELEFONIA FIJA
PARA EL MININTER

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹².

¹² 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>

MINISTERIO DEL INTERIOR

CONCURSO PUBLICO N° 005-2022-IN-OGAF-OAB-PRIMERA CONVOCATORIA

SERVICIO DE INTERCONEXION, SEGURIDAD, ACCESO A INTERNET Y SERVICIO DE TELEFONIA FIJA
PARA EL MININTER

ANEXOS



Handwritten signatures and a circular stamp with the number 81.

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN**CONCURSO PÚBLICO N° 005-2022-IN-OGAF-OAB-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 N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :		Teléfono(s) :	
MYPE ¹³		Sí	No
Correo electrónico :			

Autorización de notificación por correo electrónico:

... [CONSIGNAR SÍ O NO] 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 subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de servicios¹⁴

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

Importante

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

¹³ 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.

¹⁴ 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° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 005-2022-IN-OGAF-OAB-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 ¹⁵	Sí	No	
Correo electrónico :			

Datos del consorciado 2			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE ¹⁶	Sí	No	
Correo electrónico :			

Datos del consorciado ...			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE ¹⁷	Sí	No	
Correo electrónico :			

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

... [CONSIGNAR SÍ O NO] 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.

¹⁵ 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.

¹⁶ Ibidem.

¹⁷ Ibidem.

2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de servicios¹⁸

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.

¹⁸ 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° 005-2022-IN-OGAF-OAB-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 N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 005-2022-IN-OGAF-OAB-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 N° 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 005-2022-IN-OGAF-OAB-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 N° 5

PROMESA DE CONSORCIO

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 005-2022-IN-OGAF-OAB-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 N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]**.

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, de conformidad con lo establecido por el artículo 140 del Reglamento de la Ley de Contrataciones del Estado, bajo las siguientes condiciones:

a) Integrantes del consorcio

1. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1].
2. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2].

b) Designamos a [CONSIGNAR NOMBRES Y APELLIDOS DEL REPRESENTANTE COMÚN], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], como representante común del consorcio para efectos de participar en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato correspondiente con [CONSIGNAR NOMBRE DE LA ENTIDAD].

Asimismo, declaramos que el representante común del consorcio no se encuentra impedido, inhabilitado ni suspendido para contratar con el Estado.

c) Fijamos nuestro domicilio legal común en [.....].

d) Las obligaciones que corresponden a cada uno de los integrantes del consorcio son las siguientes:

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [%]¹⁹

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²⁰

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES 100%²¹

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

²⁰ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²¹ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

MINISTERIO DEL INTERIOR
CONCURSO PUBLICO N° 005-2022-IN-OGAF-OAB-PRIMERA CONVOCATORIA
SERVICIO DE INTERCONEXIÓN, SEGURIDAD, ACCESO A INTERNET Y SERVICIO DE TELEFONIA FIJA
PARA EL MININTER

[CONSIGNAR CIUDAD Y FECHA]

Consortiado 1

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

Consortiado 2

Nombres, apellidos y firma del Consortiado 2
o de su Representante Legal
Tipo y N° de Documento de Identidad

Importante

De conformidad con el artículo 52 del Reglamento, las firmas de los integrantes del consorcio deben ser legalizadas.



ANEXO N° 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 005-2022-IN-OGAF-OAB-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 N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 005-2022-IN-OGAF-OAB-1
Presente.-

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²²	FECHA DE LA CONFORMIDAD DE SER EL CASO ²³	EXPERIENCIA PROVENIENTE ²⁴ DE:	MONEDA	IMPORTE ²⁵	TIPO DE CAMBIO VENTA ²⁶	MONTO FACTURADO ACUMULADO ²⁷
1										
2										
3										

²² 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.

²³ 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 período.

²⁴ 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".

²⁵ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

²⁶ 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.

²⁷ Consignar en la moneda establecida en las bases.

MINISTERIO DEL INTERIOR
CONCURSO PUBLICO N° 005-2022-IN-OGAF-OAB-PRIMERA CONVOCATORIA
SERVICIO DE INTERCONEXION, SEGURIDAD, ACCESO A INTERNET Y SERVICIO DE TELEFONIA FIJA PARA EL MININTER

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²²	FECHA DE LA CONFORMIDAD DE SER EL CASO ²³	EXPERIENCIA PROVENIENTE ²⁴ DE:	MONEDA	IMPORTE ²⁵	TIPO DE CAMBIO VENTA ²⁶	MONTO FACTURADO ACUMULADO ²⁷
4										
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 9

**DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)**

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 005-2022-IN-OGAF-OAB-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.

