

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

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



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

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

CONCURSO PÚBLICO N° 003-2023-SERNANP

CONTRATACIÓN DE SERVICIO DE SERVICIO DE ACCESO A INTERNET PARA LAS SEDES DE LAS OFICINAS DE LAS ÁREAS NATURALES PROTEGIDAS Y LA SEDE CENTRAL DEL SERNANP, MEDIANTE LÍNEAS DEDICADAS DE CONEXIÓN PERMANENTE A INTERNET, POR UN PERIODO DE 24 MESES

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

DEBER DE COLABORACIÓN

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

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

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

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

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

Importante

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

Importante

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

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

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

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

Advertencia

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

Importante

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

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

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, rechazo y el otorgamiento de la buena pro.

1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

Importante

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

CAPÍTULO II

SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

- *Una vez otorgada la buena pro, el comité de selección, está en la obligación de permitir el acceso de los participantes y postores al expediente de contratación, salvo la información calificada como secreta, confidencial o reservada por la normativa de la materia, a más tardar dentro del día siguiente de haberse solicitado por escrito.*
Luego de otorgada la buena pro no se da a conocer las ofertas cuyos requisitos de calificación no fueron analizados y revisados por el comité de selección.
- *A efectos de recoger la información de su interés, los postores pueden valerse de distintos medios, tales como: (i) la lectura y/o toma de apuntes, (ii) la captura y almacenamiento de imágenes, e incluso (iii) pueden solicitar copia de la documentación obrante en el expediente, siendo que, en este último caso, la Entidad deberá entregar dicha documentación en el menor tiempo posible, previo pago por tal concepto.*
- *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

CAPÍTULO III DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

- *En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*
- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establecen los numerales 149.4 y 149.5 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento.*

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

Importante

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

Advertencia

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

1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (<http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo>).

2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.

3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.

4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.

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

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

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

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

La Entidad puede entregar adelantos directos al contratista, los que en ningún caso exceden en

conjunto del treinta por ciento (30%) del monto del contrato original, siempre que ello haya sido previsto en la sección específica de las bases.

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

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

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

En el caso que se haya suscrito contrato con un consorcio, el pago se realizará de acuerdo a lo que se indique en el contrato de consorcio.

Advertencia

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

3.9. DISPOSICIONES FINALES

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

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre : Servicio Nacional de Áreas Naturales Protegidas por el Estado
RUC N° : 20478053178
Domicilio legal : Calle 17 N° 355 Urb. El Palomar San Isidro
Teléfono: : 717- 7500
Correo electrónico: : mcamacho@sernanp.gob.pe / mrivas@sernanp.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del servicio de acceso a internet para las sedes de las oficinas de las Áreas Naturales Protegidas y la Sede Central del SERNANP, mediante líneas dedicadas de conexión permanente a Internet, por un periodo de 24 meses, según los siguientes ítems:

- **ITEM A:** Servicio de internet en 22 locales a nivel nacional.
- **ITEM B:** Servicio de internet en la sede central y tres locales en Lima.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante FORMATO DE APROBACION DE EXPEDIENTE N° 018-2023-SERNANP-OA, de fecha 18 de mayo de 2023.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios – R.O

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 aplica la distribución de la buena pro.

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 24 meses en concordancia con lo establecido en el expediente de contratación y según el siguiente detalle:

PLAZO DE PRESTACIÓN DEL SERVICIO

Para el ITEM A y el ITEM B, cada servicio será brindado por un periodo de 24 meses.

- **Para el ITEM A**, el plazo de prestación del servicio será contabilizado a partir del día siguiente que se suscriba por parte del Contratista y la UOF TIC del SERNANP el Acta de Activación del Servicio.
- **Para el ITEM B**, el plazo de prestación del servicio será contabilizado a partir del día siguiente que se suscriba por parte del Contratista y la UOF TIC del SERNANP el Acta de Activación del Servicio.

PLAZO DE IMPLEMENTACIÓN E INICIO DEL SERVICIO

- **Para el ITEM A**, el plazo de implementación y activación del servicio será como máximo de cien (100) días calendarios contados a partir del día siguiente de la firma del contrato.
- **Para el ITEM B**, el plazo de implementación se iniciará desde el día siguiente de la firma del contrato hasta máximo 15 días calendarios antes de la culminación del servicio vigente (14 de septiembre del 2023).

Tener en cuenta que una vez terminada la implementación, este servicio se activará desde el día siguiente de la culminación del servicio vigente, es decir desde el 15 de septiembre del 2023.

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/. 5.00 (Cinco y 00/100 Soles) en caja de la Entidad, sito en Calle 17 N° 355 Urb. El Palomar San Isidro – Lima.

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° 30225, Ley de Contrataciones del Estado, en adelante la Ley.
- Decreto Supremo N° 344 - 2018-EF, Reglamento de la Ley de Contrataciones del Estado, en adelante el Reglamento y sus modificatoria.
- Ley N° 31638, Ley de Presupuesto del Sector Público para el Año Fiscal 2023.
- Ley N° 31639, Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2023.

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

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

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

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

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

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

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

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

Advertencia

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

- Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. (**Anexo N° 2**)
- Declaración jurada de cumplimiento de 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) Declaración jurada de plazo de prestación del servicio. **(Anexo N° 4)**⁴
- f) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)**
- g) El precio de la oferta en **SOLES**. Adjuntar obligatoriamente el **Anexo N° 6**.

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

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.

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:

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

Advertencia

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

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.

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/>

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación ⁶ (**Anexo N° 12**).
- i) Detalle de los precios unitarios del precio ofertado⁷.
- j) Estructura de costos⁸.
- k) Certificado de la marca a nombre del especialista que implementará la plataforma de la SOLUCIÓN DE FIREWALL DE APLICACIONES WEB.
- l) Certificación ISO27001 del centro de operaciones de Seguridad (SOC).
- m) Documento que acredite que el contratista es miembro activo y directo del NAP Perú.
- n) Con respecto a los routers del ITEM A, el contratista deberá brindar hoja técnica del fabricante donde indique el cumplimiento técnico del equipo propuesto.

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.*

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

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

⁸ Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.

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 Haya⁹.*
- *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 a través de el <https://mesadepartesvirtual.sernanp.gob.pe/mpv>, en el horario de lunes a viernes, de 08:30 a 16:30 horas, o en la **mesa de partes física del SERNANP**, sito en: Calle 17 N° 355 - Urb. El Palomar - San Isidro - Lima, en el horario de 08:30 a 16:30 horas.

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en el caso de los dos (02) ítems A y B, los pagos serán mensuales durante el periodo de la prestación del presente servicio.

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

- Informe mensual con los reportes correspondientes y la conformidad de la UOF de Tecnologías de la Información y Comunicaciones.
- Presentación de la factura por parte del contratista.
- Tener en cuenta que solo para el primer pago se deberá presentar el Plan de implementación, el Informe Final de la implementación y el Informe mensual.

Dicha documentación se debe presentar mediante la mesa de parte virtual: través de <https://mesadepartesvirtual.sernanp.gob.pe/mpv>, en el horario de lunes a viernes, de 08:30 a 16:30 horas, o en la mesa de partes física del SERNANP, sito en: Calle 17 N° 355 - Urb. El Palomar - San Isidro - Lima, en el horario de 08:30 a 16:30 horas

⁹ Según lo previsto en la Opinión N° 009-2016/DTN.

CAPÍTULO III REQUERIMIENTO

Importante

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

3.1. TERMINOS DE REFERENCIA

TERMINOS DE REFERENCIA N° 018-2023-SERNANP-UOFTIC

1. DENOMINACION DE LA CONTRATACIÓN

Servicio de acceso a internet para las sedes de las oficinas de las Áreas Naturales Protegidas y la Sede Central del SERNANP, mediante líneas dedicadas de conexión permanente a Internet, por un periodo de 24 meses.

2. FINALIDAD PUBLICA

El SERNANP debido a las labores diarias tanto administrativas como técnicas las cuales se encargan de la conservación de las ANP y su diversidad biológica, requiere contar con un servicio de comunicación y transmisión de información que asegure la continuidad de los servicios tecnológicos que brindamos a todos los usuarios internos y externos. De ello nace la necesidad de la contratación del Servicio de acceso a internet para las sedes de las oficinas de las Áreas Naturales Protegidas y la Sede Central del SERNANP mediante líneas dedicadas de conexión permanente a Internet.

Este servicio eleva los niveles de productividad y satisfacción, permitiendo una rápida comunicación y garantizando un medio directo para el intercambio de información institucional.

3. ANTECEDENTES

La ENTIDAD actualmente cuenta con servicios de Internet en los locales de provincia a través de una conexión a la sede central y desde ahí tienen el servicio de internet, servicio que fue implementado en una primera versión como piloto, obteniendo muchas ventajas administrativas y tecnológicas en cuanto al servicio. También indicar que actualmente la sede central sale por otro servicio de internet independiente con 3 locales aledaños conectados a este servicio.

Ahora se necesita contar con un servicio de acceso a internet para cada una de las sedes de las Áreas Naturales Protegidas y para la Sede Central del SERNANP, mediante líneas dedicadas de conexión permanente a Internet.

4. ALCANCE Y DESCRIPCION DE LOS SERVICIOS

Es importante tener en cuenta que el presente proyecto se va solicitar en dos ITEM

ITEM A es todo lo que corresponde a la implementación del servicio de internet en 22 locales a nivel nacional según el **cuadro A**.

ITEM B es todo lo que corresponde a la implementación del servicio de internet en la sede central y tres locales en Lima según el **cuadro B**.

Se precisa que el postor deberá desplegar los agentes necesarios y en coordinación con la entidad

Como información para el número de usuarios, en las sedes remotas puede variar entre 5 a 45 usuarios por sede. En la sede central hay 260 usuarios mas los servicios informáticos que brindamos desde nuestro data Center que también está en la sede central.

Cabe mencionar que los TERMINOS DE REFERENCIA N° 017-2023-SERNANP-UOFTIC dejan sin efecto los TERMINOS DE REFERENCIA N° 013-2023-SERNANP-UOFTIC

4.1. ITEM A (Servicio de Internet en 22 sedes a nivel nacional)

- 4.1.1. Acceso dedicado simétrico Carrier Class a internet, sin restricción de protocolo, puerto o aplicación; enlaces transparentes para todos los servicios IP; con un ancho de banda

en las Sedes Remotas, según Cuadro A

- 4..1.2. El overbooking 1:1 en el enlace internacional hace referencia al overbooking 1:1 hasta el Router de acceso de salida Internacional a Internet. Asimismo, deberá considerar incluir mínimo con 4 direcciones IPv4 y 4 direcciones IPv6, por cada sede del cuadro A.

Se precisa que las direcciones IPs solicitadas no serán consecutivas necesariamente

- 4..1.3. El protocolo de transporte a la nube del contratista debe ser MPLS.

- 4..1.4. El contratista deberá contar como mínimo con 2 proveedores TIER 1 y que cuente con las salidas internacionales de al menos uno de 20Gbps y contingencias de 10Gbps

- 4..1.5. La red del contratista deberá estar en capacidad de soportar IP Multicast e IPv6.

- 4..1.6. Los equipos routers que serán provistos como préstamo por parte del servicio por parte del contratista, deberán ser de tecnología vigente, nuevos, de primer uso y no presentar anuncio de EoL (End of Life) o EoS (End of Sale) por parte del fabricante, para ello deberá indicar el link del fabricante para confirmar la vigencia tecnológica.

Se precisa que los equipos routers deberán ser de propósito específico

Se precisa también que lo requerido se podrá acreditar con documentación técnica (datasheet y/o folletos y/o catálogos y/o brochures y/o link del fabricante y/o carta de fabricante) de los equipos propuestos

Los routers deberán cumplir con lo siguiente:

- Interfaces: mínimo cuatro (04) puertos 1GE RJ45 + 1SFP, 1 puertos USB 2.0.
- Routing: BGP, OSPF, RIP v1/v2, Rutas estáticas, ECMP, RPF y enrutamiento basado en rutas y políticas.
- Multicast: IGMP v1/v2/V3, PIM-SM y multicast dentro de un túnel IPSec.
- Alta disponibilidad: Activo/Activo, Activo/Pasivo.
- Gestión de tráfico (QoS): Garantizar ancho de banda, máximo ancho de banda, políticas de ingreso de tráfico, priorización de utilización de ancho de banda, marcado DiffServ.
- Switching L2: LACP, VLAN 802.1Q y autenticación de puerto basada en 802.1x.
- Capacidad mínima de memoria RAM/FLASH o Local Storage de 2GB *o que la solución soporte memoria RAM/FLASH 1GB o Local Storage de 2GB*
- Con el objetivo de controlar el tráfico de red el equipo router deberá brindar visibilidad y rastreo de aplicaciones, aplicar políticas de seguridad, QoS. Priorización y gestión de ancho de banda por nombre de aplicación.
Considerando que cada sede remota se requiere del equipo con estas capacidades se aceptará también que se incluya un equipo de seguridad y/o administrador de ancho de banda ya que el Firewall considerado es sólo para la sede central
- El equipo permitirá almacenar un mínimo de dos sistemas operativos para mantener la alta disponibilidad.
- Soporte de Identificación de Endpoint: IP, on-line/off-line, Sistema Operativo.
- Control de Aplicaciones conteniendo la descripción, factor de riesgo, dependencias, puertos usados y URL.
- El equipo no realizará NAT, funcionalidad será administrada por el Firewall
- Los equipos para las sedes remotas deberán soportar al menos 50 usuarios concurrentes.
- El contratista deberá brindar hoja técnica del fabricante donde indique el cumplimiento técnico del equipo propuesto. *También lo requerido se podrá acreditar con documentación técnica (datasheet y/o folletos y/o catálogos y/o brochures y/o link del fabricante y/o carta de fabricante) de los equipos propuestos. Esto será entregado a la firma del contrato*
- Los equipos routers deberán tener habilitados los protocolos SNMP, Netflow u otros similares, de manera tal que se puedan monitorear el consumo de BW. Se deberá hacer entrega de las credenciales de acceso de solo lectura, definidas en los Routers instalados, a la UOF TIC del SERNANP
Se aclara que este punto se solicitará al contratista en el momento indicado durante la ejecución contractual

Se precisa que como parte de la propuesta el postor debe considerar un equipo de seguridad NGFW de la misma marca de la solución de seguridad perimetral solicitada en el ÍTEM B, para cada sede donde se instale un enlace de internet.

Considerando que cada sede remota se requiere del equipo con estas capacidades se aceptará también que se incluya un equipo de seguridad y/o administrador de ancho de banda ya que el Firewall considerado es sólo para la sede central

La ubicación de todos los equipos en las sedes del SERNANP a nivel nacional deberá ser aprobada antes de su instalación por la jefatura de cada sede.

Como parte del presente servicio el contratista deberá entregar e instalar gabinetes con llaves a cada Router en los locales de provincia, los cuales podrán retirarlos y llevárselos al final del contrato. Estos costos deberán estar incluidos y serán asumidos enteramente por el contratista.

Se precisa que la entidad brindará un espacio adecuado dentro de sus instalaciones para la instalación del gabinete solicitado.

Se precisa que el tamaño de gabinete a instalar quedará a criterio del proveedor, tomando en cuenta el número de RU de los equipos que este instalará.

Se aclara que la entidad proveerá los espacios necesarios para la instalación del router y los gabinetes en las sedes remotas y un punto de conexión de energía eléctrica con la que cuenta ese local. El contratista deberá proveer un UPS para protección de sus equipos para cada sede para los equipos propuestos por el contratista, los cuales podrán retirarlos y llevárselos al final del contrato.

Se precisa que en los equipos UPS solicitados solo se conectarán los equipos brindados por el proveedor.

- 4.1.7.** El contratista deberá realizar los trabajos necesarios dentro o fuera del local, incluyendo su trámite de permisos municipales, obras civiles y otros necesarios sin que esto implique costo adicional para el SERNANP. El servicio es considerando llave en mano incluyendo todos los equipos necesarios para el cumplimiento del presente servicio.

Las direcciones y solicitudes de ancho de banda de las sedes remotas se muestran en el siguiente cuadro A:

Cuadro A

N°	Direccion Fisica	UBICACIÓN	ANP Beneficiadas	Ubicación geográfica según google maps	BW solicitado
----	------------------	-----------	---------------------	--	------------------

1	Urb. Pampas de Aymaña F-12, Cotahuasi, La Unión - Arequipa	Arequipa	Reserva Pasajística Subcuenca del Cotahuasi	https://www.google.com/maps/place/Oficina+SERNANP+Reserva+Paisaj%C3%ADstica+Subcuenca+del+Cotahuasi/@-15.2092851,-72.8952875,18.75z/data=!4m8!1m2!2m1!1sUrb.+Pampas+de+Ayma%C3%B1a+F-12,+Cotahuasi,+La+Uni%C3%B3n+-+Arequipa!3m4!1s0x916afb55ae87076b:0xd47db1ac1d175ac4!8m2!3d-15.2092599!4d-72.8953587	15
2	Federico Sal y Rosas N° 555, Huaraz	Ancash	Parque Nacional Huascaran UO ANCASH	https://www.google.com/maps/place/Jir%C3%B3n+Federico+Sal+y+Rosas+555,+Huaraz+02001/@-9.5329481,-77.530067,21z/data=!4m5!3m4!1s0x91a90d1af9e3c0eb:0xaa9f938a9b41209d!8m2!3d-9.532883!4d-77.5301166	20

3	Urbanización Santa Martha Mz. M - Lote 02, Abancay	Apurimac	Santuario Nacional de Ampay	https://www.google.com/maps/place/13%C2%B037'38.2%22S+72%C2%B052'38.2%22W/@-13.6270343,-72.8786161,17.75z/data=!4m6!3m5!1s0x0:0x0!7e2!8m2!3d-13.6272835!4d-72.8772859	10
4	Mz k-Lote 12 Centro Poblado Pucarumi-Distrito de Quinua	Ayacucho	Santuario Histórico de de la Pampa de Ayacucho	https://www.google.com/maps/place/Sede+Administrativa+y+PCV+-+Santuario+Hist%C3%B3rico+de+la+Pampa+de+Ayacucho/@-13.0424453,-74.1370672,17z/data=!4m12!1m6!3m5!1s0x910d7f88ef640d61:0xc0b8276934f4e637!2sSede+Administrativa+y+PCV+-+Santuario+Hist%C3%B3rico+de+la+Pampa+de+Ayacucho!8m2!3d-13.0429052!4d-74.1354686!3m4!1s0x910d7f88ef640d61:0xc0b8276934f4e637!8m2!3d-13.0429052!4d-74.1354686?hl=es-419	10

5	Av. San Juan N° 724 - Cutervo Cutervo - Cajamarca	Cajamarca	Parque Nacional de Cutervo	https://www.google.com/maps/place/Av.+San+Juan+724,+Cutervo+06701/@-6.3839102,-78.8177361,21z/data=!4m5!3m4!1s0x91b37b4257ecb56d:0x799c33b84d370f32!8m2!3d-6.3839008!4d-78.8177963	10
6	Jr. Zarumilla N° 350, San Ignacio, Cajamarca	Cajamarca	Santuario Nacional Tabaconas Namballe	https://www.google.com/maps/place/Av+Zarumilla+350,+San+Ignacio+06845/@-5.1453957,-79.0052835,19.71z/data=!4m2!1m5!3m4!2zNcKwMDgnNDMuOSJITDc5wrAwMCcxNy44Ic!8m2!3d-5.1455362!4d-79.0049519!3m5!1s0x91b56811211b9ae7:0xacde03d848fd4541!8m2!3d-5.1456006!4d-79.0049697!16s%2Fg%2F11s9Ibz21g?hl=es	15

7	URB. SANTA MARTHA E-12 APROVITE SAN JERONIMO	Cusco	Parque Nacional del Manu	https://www.google.com/maps/place/Oficina+Parque+Nacional+Manu/@-13.5405966,-71.8979839,19z/data=!3m1!4b1!4m5!3m4!1s0x916e7fb136e0ee29:0xa2c30f9930767493!8m2!3d-13.5405966!4d-71.8974367	20
8	JR. SABAS SARAZOLA K-17, SANTA ANA, LA CONVENCION	Cusco	Santuario Nacional Megantoni	https://www.google.com/maps/place/@-12.859727,-72.6933457,18z/data=!3m1!4b1!4m13!1m7!3m6!1s0x91727de3d222e32b:0x652d5dd44496c552!2sJr.+Sabas+Sarazola,+Quillabamba+08741!3b1!8m2!3d-12.8598065!4d-72.6926575!3m4!1s0x91727d0763b5411b:0x4b911bcf731bde29!8m2!3d-12.8597292!4d-72.6924255	25
9	Jr. Elías Mabama N°290-PP.JJ. Túpac Amaru	Huanuco	Parque Nacional Tingo María	https://www.google.com/maps/place/Oficina+Parque+Nacional+Tingo+Maria/@-9.3084702,-76.0051433,17z/data=!4m8!1m2!2m1!1sJr.+Elias+Mabama+290+tingo+maria!3m4!1s0x91a64182c308b3c1:0x3d597dc503e488a1!8m2!3d-9.30806!4d-76.0031524	10

10	Car. Punta Pejerrey Km. 27 Paracas-Pisco-Ica	Ica	Reserva Nacional de Paracas UO ICA	https://www.google.com.pe/maps/place/Centro+de+Interpretacion,+Sendero+al+Mirador,+11550/@-13.8681078,-76.2737574,19z/data=!3m1!4b1!4m2!1m6!3m5!1s0x91107d34e49bcec5:0xa8fa3dd9e6d16c16!2sMuseo+de+Sitio+Julio+C.+Tello!8m2!3d-13.8684451!4d-76.2730245!3m4!1s0x91107d34e4de0735:0xfd885e4d685ebaa0!8m2!3d-13.8681078!4d-76.2732102	25
11	Jr. San Martín N° 138 Lado Oeste, Junín	Junín	Santuario Histórico de Chacamarca Reserva Nacional de Junín	https://www.google.com/maps/place/SERNA+NP+Reserva+Nacional+de+Jun%C3%ADn++Santuario+Hist%C3%B3rico+de+Chacamarca/@-11.160766,-75.9952242,19z/data=!3m1!4b1!4m5!3m4!1s0x9108f227090a9377:0xfd654ca98addf59!8m2!3d-11.1607673!4d-75.994677	15
12	Av. Huancavelica N° 3113 El Tambo Huancayo	Junín	Reserva Paisajística Nor Yauyos-Cochas UO JUNIN	https://www.google.com.pe/maps/place/12%C2%B002'29.8%22S+75%C2%B014'00.1%22W/@-12.0407503,-75.2332006,17z/data=!4m5!3m4!1s0x0:0x0!8m2!3d-12.041597!4d-75.233362	20
13	Av. Antonio Raymondi Mz. A, Lote 3, 4, 5 en Urbanización Juan Ramon, San Ramón.	Junín	Santuario Nacional Pampa Hermosa UO CERRO DE PASCO Bosque de Protección Pui Pui	https://www.google.com/maps/place/SERNA+NP+Selva+Central/@-11.1227447,-75.3654066,17z/data=!3m1!4b1!4m5!3m4!1s0x91090daa3e5dc52f:0x1ab0b8c1d4029dbb!8m2!3d-11.1227447!4d-75.3632179	25

14	Calle Los Laureles N° 330, Urb. Salaverry - Chiclayo	Lambayeque	Santuario Histórico Bosque de Pómac Refugio de Vida Silvestre Laquipampa UO LAMBAYEQUE Refugio de Vida Silvestre Bosques Nublados de Udimá Bosque de Protección Pagaibamba Coto de Caza Sunchubamba	https://www.google.com/maps/place/Los+Laureles+330,+Chiclayo+14011/@-6.7727355,-79.858098,19.75z/data=!4m5!3m4!1s0x904cef1de6e412a3:0x5086a0ca1e6b2616!8m2!3d-6.7726606!4d-79.8581473	25
15	Calle Jorge Chavez N° 930, Iquitos - Maynas	Loreto	Parque Nacional Gúeppi-Sekime Reserva Nacional Pacaya-Samiria Reserva Nacional Allpahuayo Mishana Reserva Nacional Matsés Reserva Nacional Pucacuro UO LORETO Reserva Comunal Airo Pai Reserva Comunal Huimeki Parque Nacional Yaguas	https://www.google.com/maps/place/Jorge+Chavez+930,+Iquitos+16001/@-3.7480484,-73.2636992,20z/data=!4m5!3m4!1s0x91ea100f7020d755:0x90a826280e85a7c0!8m2!3d-3.7480329!4d-73.2638662	50
16	Av. Ernesto de Souza S/N, Cahchacucho - Huallay	Pasco	Santuario Nacional de Huayllay	https://www.google.com/maps/place/-10.953156,-76.314240/@-10.9527824,-76.3141265,20z	10
17	Av. Los Cocos Mz. H-23 Urb. Club Grau-Piura	Piura	Coto de Caza El Angolo UO- PIURA Zona Reservada Illescas	https://www.google.com/maps/place/SERNA+NP+-+ETNORTE/@-5.1912706,-80.6341907,17.75z/data=!4m5!3m4!1s0x904a1a827c017693:0x831536d10089779c!8m2!3d-5.1911558!4d-80.6330502	25

18	PASAJE 2 DE FEBRERO N° 154, PUNO	Puno	Parque Nacional Bahuaia-Sonene	https://www.google.com/maps/place/SERNANP/@-15.8406292,-70.030311,21z/data=!4m1!3m1!3m6!1s0x915d69eba3211a17:0x58b466faa1e8de1712sPasaje+2+de+febrero,+Puno+21001!3b1!8m2!3d-15.8406098!4d-70.0301344!3m4!1s0x915d69ebbce79895:0x3259a5fff316f18f!8m2!3d-15.8405842!4d-70.0303155	25
19	Jr. Angel Delgado Morey 565, Barrio Partido Alto - Tarapoto, San Martin	San Martin	Parque Nacional Cordillera Azul	https://www.google.com.pe/maps/place/ClMA+Parque+Nacional+Cordillera+Azul/@-6.4759448,-76.3729212,17z/data=!3m1!4b1!4m5!3m4!1s0x91ba095668efca4f:0x4b55edc5b2ed301!8m2!3d-6.4759448!4d-76.3707325	30
20	Carretera a Pósic-KM 01 Mz -47 LT-11, Sector Nueva Rioja – Rioja	San Martin	Bosque de Protección Alto Mayo	https://www.google.com/maps/place/Oficina+SERNANP/@-6.0476624,-77.1752935,17z/data=!3m1!4b1!4m5!3m4!1s0x91b727acfbab2e1:0x9cab407244292641!8m2!3d-6.0476624!4d-77.1731048	20
21	Av. Panamericana Norte N° 1739, Tumbes	Tumbes	Parque Nacional Cerro de Amotape	https://www.google.com/maps/place/Servicio+Nacional+de+Areas+Naturales+Protegidas+-+SERNANP/@-3.5552896,-80.4440958,17z/data=!3m1!4b1!4m5!3m4!1s0x90338d39bda4c8f7:0xcdeab653d5736dac!8m2!3d-3.555295!4d-80.4419071	35
22	Av. Túpac Amaru - Mz G Lote 10, Calletería - Ucayali	Ucayali	Parque Nacional Alto Purús	https://www.google.com/maps/place/SERNANP/@-8.3767896,-74.5556269,19.75z/data=!4m5!3m4!1s0x91a3bcfd692e92fb:0x68edc4f3353d657b!8m2!3d-8.3768063!4d-74.5557734	35

El cuadro en Excel lo pueden descargar del siguiente link

<http://foldersgd2.sernanp.gob.pe/index.php/s/8ALtmFN48NFBawn>

4.2. **ITEM B (Servicio de Internet en la Sede Central y 3 locales en Lima)**

- 4..2.1.** Sede central: mínimo 120 direcciones IPv4 públicas y 32 direcciones IPv6
Se precisa que el número de direcciones solicitadas incluye la dirección de red, de gateway y broadcast
- 4..2.2.** Para la sede central el contratista deberá considerar un acceso dedicado simétrico Carrier Class a internet, sin restricción de protocolo, puerto o aplicación; enlaces transparentes para todos los servicios IP; con un ancho de banda de 120Mbps. Todos los equipos a ser instalados como parte del servicio, así como las licencias necesarias si se diera el caso, deberán estar preparados para un ancho de banda de 120Mbps, es decir no se aceptará cambio de los equipos instalados.
- 4..2.3.** El servicio de Internet de la Sede central, deberá ser brindado las 24 horas del día, los siete (7) días de la semana, los trescientos sesenta y cinco (365) días del año, con una disponibilidad mínima mensual de 99.90%.
Se precisa que el servicio de internet solicitado será de dos enlaces principal y backup
- 4..2.4.** Para la sede central, el servicio de acceso dedicado a Internet deberá contar con una alta disponibilidad en modo activo /pasivo, que se activará de manera automática en caso de falla del enlace principal. El acceso de contingencia deberá garantizar el mismo ancho de banda contratado del acceso principal y el router debe tener las mismas características que el router del enlace principal.
- 4..2.5.** Se aclara que lo solicitado es que el servicio de acceso dedicado a Internet deberá contar con una alta disponibilidad en modo activo /pasivo, que se activará de manera automática en caso de falla del enlace principal. El acceso de contingencia deberá garantizar el mismo ancho de banda contratado del acceso principal y el router debe tener las mismas características que el router del enlace principal.
- 4..2.6.** Para el caso de que el servicio pueda verse afectado por causas externas ajenas al operador se tomará en cuenta las normas regulatorias vigentes emitidas por el Ministerio de Transportes y Telecomunicaciones y el OSIPTEL (Decreto Supremo N° 013- 93-TIC - Texto Único Ordenado de la Ley de Telecomunicaciones y demás normas vigentes)
- 4..2.7.** El contratista deberá incluir como parte del servicio, sin costos adicionales para la institución, el servicio de registro de nuestros dominios en sus DNS, brindándonos el nombre y teléfonos (fijo y celular) y correo electrónico de uno o más contactos de emergencia para casos que el SERNANP requiera apoyo inmediato, los requerimientos de cambio de dominio serán realizados de lunes a viernes en horario de oficina (8am - 6pm) y deberán ser atendidos en máximo 24 horas. Asimismo, es necesario que el contratista brinde el servicio de registro de nuestros dominios en sus DNS; o igualmente válido será que el contratista brinde acceso a una plataforma autogestionable para que la entidad pueda realizar sus registros de dominio y subdominios. Los servidores DNS del contratista deben ser redundantes y ubicados geográficamente en sitios diferentes, al ser un servicio es responsabilidad del contratista brindar alta disponibilidad de DNS.
- 4..2.8.** El contratista debe tener redundancia de servidores DNS en arreglos de alta disponibilidad. Deberá demostrar mediante un diagrama de red su propuesta que posee servidores DNS. Se aclara que la redundancia de servidores DNS en arreglos de alta disponibilidad se refiere a que deben estar distribuidos en ubicaciones geográficas diferentes.
- 4..2.9.** El contratista deberá realizar los trabajos necesarios dentro o fuera del local, incluyendo su trámite de permisos municipales, obras civiles y otros necesarios sin que esto implique costo adicional para el SERNANP. El servicio es considerando llave en mano incluyendo todos los equipos necesarios para el cumplimiento del presente servicio.
- 4..2.10.** El contratista deberá implementar una línea de contingencia desde un NODO y ruta diferente para línea de la sede central, con las mismas características, la configuración será Activo- Pasivo.
Se precisa que el proveedor debe incluir todo lo necesario para la correcta implementación y operación del servicio, por tanto el SERNANP no brindará ningún

equipo switch LAN

- 4..2.11.** El equipo router para las sedes central deberá soportar al menos 500 usuarios concurrentes

Cuadro B

Sede	Ubicación	Ancho de Banda	OBSERVACIONES
Almacén	Sede Av. José Gálvez Barrenechea 165 San Isidro	30 Mbps	Con las características del servicio del ITEM A
OCI	Sede Av. José Gálvez Barrenechea 696 San Isidro	25 Mbps	Con las características del servicio del ITEM A
Al frente	Calle diecisiete 438 San Isidro	30 Mbps	Con las características del servicio del ITEM A
Sede Central	Calle diecisiete 355 San Isidro	120 Mbps	Con las características del servicio del ITEM B

- 4..2.12.** El SERNANP proporcionará espacio en los gabinetes de comunicaciones (para el caso de la sede central) para alojar los equipos que serán instalados por el contratista, El SERNANP será responsable de brindar la energía para dichos equipos.

Se precisa que la entidad proporcionará espacio en gabinetes y puntos eléctricos estabilizados para los equipos instalados en la sede central, para las sedes de provincia el postor deberá considerar lo solicitado en los TDR para la correcta implementación y operación del servicio

Se aclara que la entidad proveerá los puertos necesarios de cobre de su switch para la conexión de los equipos del contratista.

Se precisa que los equipos a implementar por el contratista se encontrarán en un mismo gabinete lo cual incluye routers, switches, firewall, WAF y anti-ransomaware, Pero se aclara que los cableados de datos necesarios para conexión de nuestros equipos con los equipos que instalará el contratista, deberán ser provistos por el mismo contratista sin costo alguno para la entidad.

Se aclara que la entidad proveerá un punto de conexión de energía eléctrica comercial estabilizada (220 VAC) en la sede central.

- 4..2.13.** Como parte de esta implementación, se tendrá que configurar un máximo de 20 equipos en la sede central con una velocidad de carga y descarga mayor que los demás usuarios para que puedan realizar trabajos especializados y no se vean perjudicados en caso el ancho de banda se vea saturado por los demás usuarios. La velocidad de ancho de bando para estos usuarios de trabajos especializados se tendrá que definir en coordinación con la UOF TIC del SERNANP.

✓ **SERVICIO DE MITIGACION DE DDoS**

- 4..2.14.** El contratista debe brindar una solución AntiDDoS en la nube del contratista y desplegada en territorio nacional que debe cumplir con los siguientes requerimientos:
- El servicio debe tener una capacidad de mitigación de al menos 30 Gbps.

Se precisa que la capacidad de mitigación debe ser de al menos 30Gbps desde la nube del postor

- El servicio deberá tener incorporado un módulo IPS para ataques DoS a nivel de aplicación
- El servicio deberá contar con un motor de creación de firmas en tiempo real, de manera automática sin intervención humana, que además permita la protección contra ataques día cero.
- El servicio deberá operar bajo una arquitectura Always On que garantice que solamente el tráfico de ingreso cursara por el mitigador y no así el tráfico de salida, garantizando de esta manera que no se mantienen sesiones concurrentes activas en la solución Anti DDoS
- El servicio de mitigación de ataques DDoS debe estar desplegado bajo una arquitectura Always On o siempre en línea, garantizando de esta manera que el tráfico sea inspeccionado todo el tiempo, por tal motivo no se aceptaran soluciones de desvío tráfico.
- El contratista deberá crear múltiples usuarios en una consola de monitoreo MSSP dedicada, que permita visualizar las estadísticas y monitoreo de los ataques, del servicio contratado, en tiempo real.
- Los usuarios asociados a la consola deberán poder generar reportes de forma autónoma.
- El contratista debe tener implementada una solución de mitigación de ataques de denegación de servicios dedicada dentro de su nube local (territorio nacional). Al menos el mitigador, debe ser de tipo Appliance, de tecnología específica para la mitigación de ataques DDoS, por lo que no se aceptaran soluciones que tengan este propósito como una funcionalidad como ser, Firewalls, ADC, routers o cualquier otro dispositivo que no sea dedicado.
- La solución debe ser de tipo Stateless por lo que se requiere que únicamente el tráfico de ingreso pase por el mitigador.

✓ **SOLUCIÓN DE SEGURIDAD PERIMETRAL**

Se deberá considerar 02 equipos nuevos y configurados en alta disponibilidad. Además, se deberá adjuntar, previo a la instalación y configuración del o los equipos a instalar e implementar, una carta del fabricante confirmando que no tienen anuncio de "End-of-Life" ni "End-of-Sale", indicando el modelo del equipo que están ofreciendo para esta solución. La solución deberá cumplir con las siguientes características mínimas:

4.2.15. DESCRIPCION

- Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.
- El fabricante debe pertenecer al cuadrante de líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 8 reportes.
- El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls
- El fabricante deberá tener una efectividad de seguridad mayor o igual al 97% según el último reporte de NSS Labs para Next Generation Firewall.
- La plataforma propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS, dicha certificación se presentará previo a la instalación y configuración del o los equipos a instalar e implementar
- La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.
- Ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support.
- Los equipos NGFW deberán tener soporte vigente de fabrica durante todo el periodo del contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware

4.2.16. CAPACIDAD

- Throughput de Prevención de Amenazas de 780Mbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Seguridad avanzada en DNS, Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. 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. 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.
- El equipo debe soportar como mínimo 120 mil sesiones simultaneas y 8 mil nuevas sesiones por segundo, medidos con paquetes en capa 7.
- Disco interno de 240 GB o superior.
- El equipo debe contar con 6 interfaces de cobre 1GB RJ45, 2 (dos) de ellas dedicadas para soportar la sincronización de estado y configuración dentro del clúster de alta disponibilidad.
- El equipo debe soportar 8 interfaces 1 GB SFP
- El equipo debe contar con un puerto de administración dedicado fuera de banda de 1GB.
- El equipo debe contar con un puerto de consola RJ45

4.2.17. CARACTERÍSTICAS GENERALES

- El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.
- Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.
- Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel.
- Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.
- Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.

4.2.18. FUNCIONALIDADES DE FIREWALL

- Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos) y categorías de aplicaciones.
- Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa.
- Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
- Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
- Debe mostrar la primera y última vez que se utilizó una regla de seguridad.
- Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
- Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.

4.2.19. DESCIFRADO DE TRÁFICO SSL/TLS

- Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.
- Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.
- Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.
- Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.
- Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS
- Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI).
- Sebe permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar el no descifrado de páginas con contenido sensible, mientras forzar el descifrado de páginas de clasificación de riesgo alto o medio
- Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.
- Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).

4.2.20. PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (DoS)

- Debe ser posible definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood.
- Para el caso de los SYN Flood debe ser posible utilizar SYN Cookies como medidas de defensa
- La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor)
- La protección contra ataques Flood deberá permitir definir al menos 3 tipos de umbrales, el primero para generar una alerta al administrador, el segundo para activar la protección y el tercero para restringir el acceso en su totalidad en base a dicha política de DoS
- Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo
- La protección contra ataques de escaneo deberá permitir definir una lista de excepciones basadas en direcciones IP origen, a los cuales no se le aplicarán la protección.
- Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route
- Debe proteger contra ataques basados en protocolos No-IP en interfaces Layer 2 (como Appletalks, Banyan, VINES, Novell, SCADA), la solución deberá soportar la definición de protocolos a ser aceptados en base al formato Ethertype (Hex).
- Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia dicho equipo.

4.2.21. CONTROL DE APLICACIONES

- Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
- **Podrá** identificar y crear políticas de seguridad basadas en aplicaciones de Sistemas de Infraestructura Crítica (ICS) como addp, bacnet, modbus, dnp3, coap, dlms, iccp, iec-60870-5-104, mms-ics, rockwell, siemens, entre otros.

- Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.
- Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
- Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.
- Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto y protocolo, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.
- Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.
- Con el objetivo de identificar aplicaciones propietarias a nivel de capa 7, la solución debe permitir nativamente la creación de aplicaciones personalizadas desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante.
También se podría optar por esta otra opción:
[Con el objetivo de identificar aplicaciones propietarias a nivel de capa 7, la solución debe permitir nativamente la creación de aplicaciones personalizadas desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante y/o generar firmas para las aplicaciones propietarias a partir de una herramienta provista por el propio fabricante](#)
- Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en sus atributos.
- Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.

4.2.22. PREVENCIÓN DE AMENAZAS

- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.
- Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por spyware en entornos corporativos
- Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.
- El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
- Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia.
- Debe incorporar una plataforma de sandbox basada en nube para el análisis de ejecutables desconocidos.
- Con el objetivo de tener la información de amenazas actualizada, la plataforma deberá ser capaz de actualizar su base de firmas en tiempo real sin afectar el performance del equipo.
- Debe soportar granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.
- Debe identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que el Firewall pueda bloquear dichas consultas DNS.
- Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
- Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.
- Debe soportar la creación de firmas de IPS basadas en el formato de Snort.

4..2.23. ANALISIS DE MALWARE DE DÍA CERO

- La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.
- La plataforma de Sandboxing podrá ser ofrecido en Nube (Cloud), On-premise o ambos. Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y MacOS.
- Deberá ser capaz de analizar 4000 archivos por hora realizando análisis dinámico (es decir, no uso de firmas)
- En caso de tratarse de una plataforma de Sandboxing Cloud, deberá cumplir con los siguientes requerimientos:
 - Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
 - Deberá ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades terceras.
 - Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II de AICPA, ISO 27017 e ISO 27018.
- En caso de tratarse de una plataforma de Sandboxing On-premise, deberá cumplir con los siguientes requerimientos:
 - Deberá ser desplegado en Alta Disponibilidad (Activo-Pasivo), con el objetivo de mantener los controles de ciberseguridad en caso de falla de uno de los equipos.
 - Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows, MacOS, Linux y Android.
- Debe admitir topologías de implementación en modo sniffer o en línea (in-line)
- Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
- El Next Generation Firewall debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB (versiones 1, 2 y 3). Tanto en IPv4 como en IPv6.
- Debe permitir al administrador la descarga del archivo original analizado por el Sandbox.
- Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.
- Permitir la subida de archivos al sandbox de forma manual y vía API.
- Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
- La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.

4..2.24. FILTRO DE CONTENIDO WEB

- Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
- Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía Active Directory, LDAP en general y base de datos local.
- Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs
- Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing.
- Debe contar con multi categorías de URL, que permita conocer si una web de una categoría determinada está catalogada como riesgo bajo, medio o alto.

- Debido a que diariamente se crean decenas de miles de nuevas páginas web, la solución deberá ser capaz de analizar en tiempo real si la página web tiene contenido malicioso cuando un usuario intenta acceder.
- El análisis en tiempo real deberá determinar si la página web desconocida (no categorizada en la base de datos del fabricante), tiene contenido javascript malicioso, phishing, actividad de command and control y otros tipos de contenido malicioso.
- Debe permitir la creación de categorías personalizadas.
- Debe permitir la customización de la página de bloqueo.
- Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site.
- Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing.

4..2.25. IDENTIFICACION DE USUARIOS

- Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell Directory, Exchange y base de datos local.
- Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.
- Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI.
- Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.
- Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios.
- Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
[Se aclara que el postor podrá incluir una solución de doble autenticación con el objetivo de lograr la capacidad requerida](#)
- Debe permitir la definición de grupos dinámicos de usuarios.

4..2.26. QOS

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

4..2.27. VPN

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

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

4..2.28. ADMINISTRACION Y MONITOREO

- Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante
- [Podrá](#) remitir exportar las reglas de seguridad en formato CSV y PDF
- Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.
- Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
- Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino)
- Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
- [Podrá](#) contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política
- Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se superpongan reglas generales sobre reglas específicas (shadowing rules).
- Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.
- Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
- Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó, su IP y el horario de la alteración;
- Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.
- Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispysware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.

- La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.

✓ **SOLUCIÓN DE FIREWALL DE APLICACIONES WEB**

Se deberá adjuntar una carta del fabricante, previo a la instalación y configuración del o los equipos a instalar e implementar, confirmando que los equipos son nuevos, de primer uso y no tienen anuncio de "End-of-Life" ni "End-of-Sale", indicando el modelo del equipo que están ofreciendo para esta solución. La solución deberá cumplir con las siguientes características mínimas:

- El Contratista deberá de proporcionar una solución de seguridad WAF (Firewall de Aplicaciones Web) que será instalada en el Centro de Datos de SERNANP, deberá ser de tecnología vigente y con soporte del fabricante durante todo el período del contrato.
- Características Generales:
 - La solución estará compuesta por un (01) equipo WAF y una consola externa, todos del mismo fabricante.
Se precisa que la solución debe encontrarse en alta disponibilidad con equipos dedicados, para el caso de la consola externa se considerará opcional la alta disponibilidad.
 - La solución de seguridad de aplicaciones web deberá estar presente en los últimos tres (03) reportes del "Cuadrante Mágico de Gartner", en el cuadrante de Líderes para Web Application Firewalls.
- La solución deberá tener varios mecanismos de despliegue (deployment) contando como mínimo con puente transparente en línea (Bridge L2), Proxy Reverso Explícito o Transparente. Se valorará como *opcional* la capacidad de inspeccionar tráfico en modo "Sniffing", utilizando PORT MIRROR de un Switch o algún TAP de red, para poder monitorear el tráfico sin realizar cambios en la red.
- En caso de proveer una solución en modo Bridge L2, por lo menos 2 de sus interfaces deben incluir bypass / fail-open / fail-close configurable tanto para fallas de hardware como software.
- Hardware e Interfaces:
 - Deberá incluir un módulo SSL de menos 6,000 RSA/sec (2048bits).
 - Contar como mínimo con 4 interfaces de cobre 1 GE, todos estos puertos deben contar con capacidad de hacer bypass. Además de soportar dos interfaces 10GE SFP+ con soporte bypass
 - Deberá contar con memoria RAM de 16GB.
 - Disco duro de 2 x 2TB (RAID 1).
- Performance:
 - Soportar como mínimo un throughput de 500 Mbps de tráfico HTTP/HTTPS.
- Características WAF:
 - La solución deberá detectar, alertar y bloquear, en tiempo real, cualquier comportamiento malicioso conocido y/o desconocido.
 - La solución deberá contar con un modo de aprendizaje que permita definir cuáles son las acciones esperadas y aceptadas para los usuarios. Esta información deberá estar disponible para automatizar la configuración del modelo positivo de seguridad.
 - El modo aprendizaje, deberá aprender la estructura y elementos de la aplicación y esta información deberá estar disponible para automatizar la configuración del modelo positivo de seguridad. Como mínimo debe aprender sobre: Host válidos, URLs, parámetros, cookies, tipo de contenido de los parámetros, caracteres aceptados, longitud del valor esperado. Debe reconocer los elementos codificados en Base64.
 - El modo aprendizaje debe ser capaz de seguir activo aun cuando se encuentre en modo de protección o bloqueo, permitiendo la incorporación de nuevos parámetros, sin necesidad de realizarlo en forma manual.
 - Respecto de algún ataque o alguna otra actividad no autorizada, la solución deberá ser capaz de definir un nivel de severidad y tomar las acciones adecuadas, como mínimo: terminar las solicitudes y respuestas, bloquear la sesión TCP, colocar en

cuarentena temporal o bloquear al usuario de la aplicación, colocar en cuarentena temporal o bloquear la dirección IP de origen, ejecutar un comando a nivel de Sistema Operativo en la solución WAF, notificar vía Email y Syslog.

- La solución deberá tener la capacidad de utilizar los certificados y pares de llaves público/privadas para los servidores web HTTPS.
- La solución de monitoreo de aplicaciones web, deberá validar todos los tipos de datos ingresados, incluyendo URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos HTTP, elementos XML / JSON y acciones SOAP / REST
- La solución deberá tener la capacidad de realizar un parche virtual para proteger las vulnerabilidades detectadas y deberá tener integración con scanners de vulnerabilidades (al menos 5 diferentes soluciones o servicios del mercado) para tomar sus resultados, interpretarlos y sugerir los cambios a aplicar.
- La solución debe soportar la detección de herramientas automáticas de descarga, bots, scripts, etc. por medio de la generación de un requerimiento en JavaScript, a fin de poder bloquear todas las consultas que no poseen un navegador real por detrás.
- Implementar en forma nativa controles anti-scraping.
- Implementar de forma nativa políticas para prevenir el acceso a aplicaciones web utilizando websockets (incluyendo JSON sobre websocket).
- Proporcionar protección para todas las vulnerabilidades expresadas en OWASP y no sólo las Top 10. Respecto a estas vulnerabilidades la solución debe proporcionar protección automatizada con políticas predefinidas de fábrica.
- Debe poder generar excepciones para controlar los falsos positivos.
- La solución debe permitir tomar acciones y alertar ante violaciones de protocolos inferiores al aplicativo, incluyendo inspección de paquetes IP, TCP, UDP y sus encabezados.
- La solución debe soportar la identificación de IP origen en caso de que este pase por un proxy, interpretando el campo X-Forwarded-For de la cabecera HTTP.
- Deberá soportar la integración de un módulo (licenciamiento adicional) de base de datos de reputación de IP maliciosas, geolocalización y firmas en tiempo real (up-to-day) de ataques zero-day.
- Deberá soportar (licenciamiento adicional) una herramienta de análisis de ataques web que realice un análisis de información unificada y contextual pudiendo ser en la nube que permita analizar miles de eventos WAF como tendencias, patrones de amenazas y campañas de ataque en distintos contextos.
- Consola de Administración
 - Todos los componentes que conformen la solución deben poder ser configurados, administrados y monitoreados en su totalidad en forma centralizada con una consola dedicada para ello. La consola de gestión puede ser del tipo appliance o virtual, la entidad proveerá el servidor virtual en caso se requiera.
 - La consola de administración deberá soportar todo tipo de gestión sobre el WAF y personalización de reportes granulares que incluyen: servidor y aplicación web protegidos, tipo de ataque, objeto atacado, URL, método HTTP, IP origen, usuario del aplicativo web, rango de tiempo, entre otros. Con capacidad de automatizar la generación de reportes y su posterior remisión por email.
 - La solución de administración permitirá la visualización centralizada y en tiempo real de los logs de actividad de los equipos de la solución y las modificaciones de configuración que los administradores pudieran efectuar.
 - Generar alarmas ante los siguientes eventos: degradación de la performance, falla de cualquiera de los componentes de la solución, problemas de conectividad.
 - Permitir la generación de reportes de forma manual, automática y periódica, de todas las alertas de seguridad, en los formatos PDF y CSV. Los reportes podrán ser enviados de forma automática a un correo electrónico
 - La plataforma deberá ser implementada por especialista certificado de la marca propuesta, dicha certificación se presentará para la firma del contrato
 - Documento de Garantía del Fabricante por el HW a través de RMA durante el periodo de contrato, el cual será presentado previo a la instalación y configuración del o los equipos a instalar e implementar. Además, el contratista deberá contar con una unidad

similar o superior para reemplazo en modalidad 24x7x8.

Se precisa que la entidad requiere equipos de repuesto dedicados en caso de falla de los equipos principales que deberán instalarse en nuestro centro de datos, los cuales se deben de configurar como los equipos principales.

✓ **SOLUCIÓN ANTI-RANSOMWARE (1 o 2 equipos de acuerdo a lo que disponga el contratista)**

Se deberá adjuntar, previo a la instalación y configuración del o los equipos a instalar e implementar, una carta del fabricante confirmando que los equipos son nuevos, de primer uso y no tienen anuncio de "End-of-Life" ni "End-of-Sale", indicando el modelo del equipo que están ofreciendo para esta solución. La solución deberá cumplir con las siguientes características mínimas:

- La solución deberá permitir realizar detección y bloqueos de amenazas persistentes, por lo que el Contratista podrá presentar un (01) equipo de 2UR como máximo, ó en su defecto, dos (02) equipos de igual o distinta marca con una altura máxima de cada equipo de 1UR. En caso de proveer un equipo deberá contar con fuentes redundantes y 02 discos duros en RAID1.
- El proceso de detección de amenazas desconocidas o conocidas no deberá ser intrusivo y deberá permitir notificar automáticamente al servicio de bloqueo, es decir, la plataforma a ofertar deberá realizar el envío de los análisis de las amenazas vía web, correo, trap, syslog y/o snmp para su notificación.
- No se aceptarán soluciones de seguridad que no sean dedicadas a la tecnología requerida.
- No se aceptarán soluciones de NGFW, UTM u otras que no sean dedicadas a la tecnología requerida.
- Deberá tener una lista de vigilancia que ayude a proteger a los dispositivos de mayor riesgo en la red.
- Deberá tener una consola de gestión para administrar la herramienta en modo appliance o embebida en el equipo.
- La solución deberá instalarse en línea con el tráfico de la red, por lo que deberá contar con características de alta disponibilidad para evitar interrupción de la comunicación, como es la característica de bypass de tráfico por corte de energía.
- Inspección de tráfico de Red
 - La Inspección deberá incluir máquinas virtuales permitan el análisis de los siguientes tipos de archivos maliciosos:
 - ✓ 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
 - Contar con una consola de información en tiempo real, que permita dar visibilidad en cualquier momento, de lo que sucede en la red. Deberá contar con mecanismo que permita identificar los orígenes de la comunicación maliciosa.
 - Permitir acceso a un portal de información sobre amenazas del fabricante para conseguir más datos sobre un ataque o malware específico y acceder a recomendaciones de contención y solución de amenazas.
 - Deberá ser capaz de monitorear aplicaciones no aprobadas dentro de las políticas internas del usuario (P2P, chat en IRC, multimedia, etc) y/o deberá registrar toda la actividad que un objeto malicioso trate de ejecutar, registrando las modificaciones del sistema operativo/aplicación que logre modificar, tales como: Registro de Windows,

Registro de la aplicación, Registro de procesos, Registro de Archivos, Registro de comportamiento y Registro de comunicaciones.

- La solución no deberá ser disruptiva ante ningún servicio informático que la institución brinde, es decir; deberá soportar el modo inline de monitoreo, o el modo inline con bloqueo activo.
- La recepción y análisis del tráfico de red deberá ser posible mediante la lectura y recepción de puertos de monitoreo (port mirror o port span) que envíen la totalidad del tráfico de red a analizar.
- La recepción y análisis del tráfico de red deberá ser posible sin la necesidad de integración con ningún servicio o infraestructura de la institución, y sin la necesidad de instalar agentes de software en ningún dispositivo a monitorear.
- Deberá poder identificar amenazas que son evasivas a la seguridad tradicional de firewalls, detectores de intrusos y antivirus.
- Sandboxing
 - La solución deberá permitir hacer sandboxing para poder reflejar un entorno específico del lado usuario. El sandboxing debe estar integrado de forma local a la solución implementada para realizar el servicio.
 - El sistema de protección de malware deberá tener la capacidad de bloquear llamadas a servidores remotos (callbacks). En el caso de ataques de día cero, deberá bloquear la habilidad del Malware para realizar llamadas C&C (comando & control), de esa manera dejándolo inerte y previniendo pérdida de información. Esto significa que deberá detectar y prevenir malware avanzado, ataques del tipo Zero Day y Amenazas persistentes avanzadas dirigidas sin necesidad de haber sido reconocidas previamente por una base de firmas.
 - La solución **podrá** soportar al menos 16 instancias de Sandboxing o ambientes de simulación simultáneos dentro del mismo componente, con versiones de Sistema operativo diferentes. Las 16 instancias podrán ofrecerse en 12 máquinas virtuales en el mismo equipo 04 máquinas virtuales en la nube del fabricante.
 - Deberá tener una tecnología en la nube del fabricante, que permita analizar la reputación del tráfico y correlacionar las amenazas que afecten el servicio.
 - La solución deberá 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
 - Deberá ser capaz de detectar y bloquear tráfico C&C y actividad Backdoor.
 - Deberá poder detectar y controlar amenazas en la red del tipo Ransomware, ataques de día cero y vulnerabilidades, deberá bloquear los programas maliciosos para evitar que afecten una aplicación
 - Capacidad de detectar y bloquear paquetes "exploit" que atacan vulnerabilidades de sistemas operativos Windows, aplicaciones comunes y bases de datos.
 - Capacidad para detener zero-day exploits o detectar, frenar, bloquear actividad maliciosa cuando se configure en modo en línea.
 - Capacidad para detectar y bloquear malware conocido y desconocido
 - Monitoreo de tráfico, incluyendo tráfico encriptado SSL
 - Deberá permitir integración con soluciones SIEM.
 - Capacidad de detección y protección o informar ante las siguientes amenazas
 - ✓ Ataques dirigidos y Amenazas avanzadas
 - ✓ Zero-day malware y document o object exploits
 - ✓ Attacker behavior o comportamiento malicioso and other network activity
 - ✓ Amenazas Web, incluyendo exploits y drive-by-downloads
 - ✓ Exfiltración o robo de Datos
- Consola de Gestión y Reportes.
 - Deberá ser una consola de gestión embebida en el mismo equipo o en formato appliance del mismo fabricante que presente reportes de las amenazas encontradas por los equipos de bloqueos y de sandboxing.
- Bloqueo de las amenazas detectadas
 - Detectar y mitigar ataques
 - Deberá permitir el detectar y exploit kits o root kits en tiempo real.

- Deberá permitir bloquear ataques dirigidos y amenazas persistentes avanzadas que pueden haber pasado por las defensas existentes, proporcionando un enfoque de defensa en profundidad.
- Deberá ser capaz de detectar vulnerabilidades, sin necesidad de conocer la firma, es decir, a través del comportamiento de la amenaza
- Deberá trabajar como un mecanismo de defensa frente a los ataques conocidos que intentan explotar una falla particular de algún software de la red interna o detectar, entender y comprender los tres estados del ciclo de vida de los ataques modernos: Exploit, Dropper y Data Exfiltration.
- La solución deberá permitir extraer la información de reportes a través de una memoria flash o tener la capacidad de exportar sus informes en formato CSV y PDF de manera automática (programada) o manual.
- Características del appliance de bloqueo de amenazas avanzadas
 - Capacidad de throughput de 1Gbps y licenciada al menos con 100Mbps
 - Sesiones concurrentes de al menos 250,000 o soportar al menos 1,500 usuarios concurrentes.
 - Se precisa que el postor podrá ofrecer capacidades mayores siempre y cuando no se tengan costos adicionales para la entidad
 - Puerto de gestión: Puerto ethernet de 01 Gbps.
 - Puerto de red: 04 puertos de cobre (04 x 1G) RJ-45 Soporte Bypass integrado y 04 de fibra SFP+ (4x10G SFP+), que incluya los 04 módulos transceiver SFP+.
 - Ranura para insertar memoria flash de 8GB o 04 puertos USB tipo A.
- Características del appliance para la detección de amenazas avanzadas
 - Capacidad de throughput de 1Gbps y licenciada al menos con 100Mbps
 - Un puerto de gestión 1Gbps RJ45.
 - Puertos de datos: 04 puertos 01 Gbps, RJ45 con soporte bypass.
- La plataforma deberá ser implementada por especialista certificado de la marca propuesta.
- Documento de Garantía del Fabricante por el HW a través de RMA durante el periodo de contrato, el cual será presentado previo a la instalación y configuración del o los equipos a instalar e implementar. Además, el contratista deberá contar con una unidad similar o superior para reemplazo en modalidad 24x7x365.

✓ **SERVICIO DE CIBERDEFENSA**

El CONTRATISTA, deberá entregar un servicio de ciberdefensa propio o de un tercero, este servicio debe ser alojado en un centro de datos [opcionalmente](#) certificado RATED II propio o de tercero y operado por su CyberSOC en gestión de incidentes, gestión de cambios y ciberseguridad. Este servicio deberá permitir mediante el análisis de logs de la solución de seguridad propuesta y al menos 20 servidores Windows, permita realizar investigaciones y escalar incidentes con las siguientes características

Se precisa que el cliente brindará el espacio de rack y energizado necesario dentro de su infraestructura para el despliegue de la solución de SIEM para el servicio de monitoreo, esto con el fin de garantizar que los logs a monitorear no salgan de su infraestructura y que el monitoreo se realice a través de una conexión VPN Site to Site.

Se requiere que la retención de Logs sea de al menos 3 meses

- Capas adicionales como analítica de comportamiento de 300 usuarios ([UEBA](#)), orquestación, automatización y respuesta de seguridad (SOAR), para procesar múltiples eventos de seguridad.
- Se precisa que se requiere al menos 2 playbooks
- Con el objetivo de validar y dar seguimiento a las investigaciones de ciberseguridad, el CONTRATISTA deberá entregar un Portal web seguro con doble factor de autenticación para revisar las investigaciones.
- El portal debe actuar como una interfaz gráfica de usuario (GUI) que muestre investigaciones que fueron realizadas por los componentes (SIEM, [UEBA](#), SOAR, inteligencia de amenazas), es decir que la herramienta cuenta con la auditoría de usuarios que realizaron cambios en la misma.

- Capas adicionales al SIEM como analítica de comportamiento de usuarios (**UEBA**), orquestación, automatización y respuesta de seguridad (SOAR), para procesar múltiples eventos de seguridad y mecanismos de detección propietarios basados en Inteligencia artificial totalmente integrados al servicio.
- Monitoreo 24x7 identificando amenazas cibernéticas que puedan afectar la operación.
- Inteligencia de amenazas mediante actualizaciones de indicadores de compromiso (IOC) de múltiples fuentes que incluyen indicadores internos extraídos de eventos, comunidades de código abierto, redes sociales, inteligencia técnica y/o inteligencia procedente de la Deep and Dark Web. Las fuentes de inteligencia de amenazas deberán ser enviadas al gestor de eventos de la seguridad de la información para correlacionar y generar detecciones.
Estos IOC se refiere a todos los equipos de seguridad a proponer como parte del servicio
- Caza de amenazas sobre el gestor de eventos de seguridad, identificando, evaluando y mejorando la capacidad de detección mediante búsqueda exhaustiva de ciber-amenazas y actividades maliciosas.
- Respuesta y mitigación de incidentes en tiempo real ante ciber- amenazas.
- Optimización de procesos consistentes de desarrollo y aprendizaje que incluyan optimización de reglas, actualizaciones y sugerencias de implementación de nuevas tecnologías de detección de amenazas cibernéticas.
- La Inteligencia de amenazas debe comprobar todas las comunicaciones salientes; alertar sobre la comunicación con la IP, dominios y URL maliciosos; y finalizar la conexión inmediatamente, todo esto sucede en tiempo real. La Inteligencia de amenazas debe comprobar todas las comunicaciones salientes(**LAN-WAN**); alertar sobre la comunicación con la IP, dominios y URL maliciosos; y finalizar la conexión inmediatamente, todo esto sucede en tiempo real.
- Investigación forense de procesos en curso de presuntas actividades maliciosas y amenazas cibernéticas incluyendo el análisis post mortem de incidentes verificados, identificando el origen del ataque, la causa raíz y proporcionar información sobre quién inició el ataque. Mínimo de 4 horas mensuales de ser requerido y un máximo de 08 horas.
- El servicio deberá tener la capacidad de integrarse a cualquier solución de seguridad, fuente de registro y Endpoint.
- Configuración personalizable de notificaciones vía email (notificaciones, recomendaciones, acciones pendientes, nuevas investigaciones, escalamiento de una investigación en curso, modificación del estado de una investigación en curso)
- Este servicio debe tener la capacidad de ser retroalimentado por un emisor externo de incidentes para que de esta manera no sea juez ni parte en la emisión de investigaciones, a fin de asegurar la imparcialidad y permitir que la entidad pueda dar seguimiento de los tiempos de resolución y atención del contratista.

5. CONSIDERACIONES ADICIONALES para el ITEM A y el ITEM B

- A. El Contratista del servicio deberá poner a disposición de SERNANP, las 24 horas del día, un sistema de Monitoreo On Line del estado del enlace del servicio. El acceso a este sistema (software) deberá ser vía Web con usuario y contraseña. La información histórica deberá conservarse en línea y deberá poder ser consultada en cualquier momento debiendo guardar la información hasta un mínimo de 90 días.
Se precisa que el postor debe implementar el sistema de monitoreo en el centro de datos de la entidad considerando todo el software y hardware necesario, siendo responsabilidad de la entidad sólo brindar el espacio y energía en los gabinetes correspondientes.
- El contratista deberá incluir una herramienta web (HTTP o HTTPS) de monitoreo de los enlaces de Internet y Datos.
 - Debe permitir el monitoreo del desempeño de cada router, debe mostrar en una pantalla resumen: alarmas recientes, pérdida de paquetes. Asimismo, deberá presentar gráficas de utilización de CPU, utilización de memoria.
 - Debe permitir Reportes de la salud del Router. Reportes con intervalo de tiempo configurables del uso del CPU, memoria, temperatura y otros de los dispositivos

- monitoreados. Gráficos interactivos en pie, barras, tabular.
- Capacidad para seleccionar las interfaces físicas o virtuales a monitorear.
- Soporte NetFlow (version 5, 7 y 9), jFlow, sFlow, cFlow.
- Ancho de Banda del transmisor y receptor configurable.
- Deberá permitir la generación de alarmas que serán enviadas vía correo electrónico.
- Debe permitir Reportes de Tráfico (Entrada y Salida): en Kbps y Paquetes por segundo, Errores y Descartes (Entrada y Salida).
- Permitir tener la cantidad de tráfico en Megabits por segundo y Porcentaje mostrándolo en un gráfico tipo pastel o barras.
- Filtros configurables, personalización de reportes en archivos pdf, csv y creación de alarmas.
- Reportes ejecutivos personalizados y gráficos interactivos.
- Permite la configuración de reportes automáticos para ser generados mensualmente y a petición.
- Permite la configuración de alertas basado en violaciones de los umbrales.
- Envío de notificaciones vía correo electrónico
- B. El contratista deberá contar con al menos un centro de operaciones de Seguridad (SOC) propio o tercerizado y ubicado dentro del territorio nacional, dicha certificación se presentará para la firma del contrato. Asimismo, el contratista deberá contar con una solución SIEM (Security Information and Event Management) como parte del servicio y se requiere del acceso al mismo.
- C. La administración de todos los equipos que conformen la implementación de la solución planteada para el presente servicio debe ser en forma compartida, es decir la UOF TIC del SERNANP debe contar con un usuario cuyo perfil permita administrar las reglas del Firewall, WAF y solución Anti-Ransomware.
- D. Se aclara que la entidad será responsable por la actuación de sus dependientes a quienes se les otorgo credenciales.
- E. EL CONTRATISTA deberá garantizar que la solución completa quede operativa y en óptimas condiciones de seguridad y performance, y de activar un plan de contingencia cuando una falla se produzca asegurando que todos los servicios solicitados queden de la misma manera hasta superar la falla
- F. La implementación de todas las configuraciones y reglas solicitadas en el presente documento, será de entera responsabilidad del contratista, dejando todo completamente operativo puesto que se trata de un servicio llave en mano
- G. Una vez terminado el vínculo contractual con el contratista, este se verá obligado a desmontar y retirar todos los equipos así como el cableado que este dentro de los locales de la entidad a nivel nacional y que hayan sido instalados para el funcionamiento de dicho servicio. El tiempo que tiene para realizar esta actividad a nivel nacional es de máximo 60 días calendarios.
- H. En caso sea necesario, el contratista deberá incluir a todo costo el trabajo de ducterías y/o canalizaciones para ingresar el medio de conexión hasta la ubicación final del Router. De ser necesario realizar picados y/o resanes, y otras obras de construcción civil relacionadas, este será asumido a todo costo por el contratista
Se precisa que el proveedor será responsable de las ducterías, canalizaciones y cableado por donde deberá pasar la fibra óptica, las rutas serán definidas y coordinadas por la entidad.
Se aclara que, en caso de ofrecer el servicio por medio inalámbrico, la entidad será responsable de brindar un espacio físico.
La adquisición y /o instalación del sistema inalámbrico, de ser necesaria algún tipo de estructura (torre o mástil), será enteramente responsabilidad del contratista asumiendo los costos que sean necesarios.
Se aclara que la entidad brindará las facilidades de acceso en sus locales, indicando la cámara de acceso a su local o punto de acceso aéreo.
- I. Todos los equipos deben contar con la última versión estable del sistema operativo recomendado por el fabricante
- J. Los routers deben contar con la capacidad necesaria para soportar hasta un 50 % más del tráfico generado por las distintas sedes remotas y sede central, que forman parte de la solución.

Se precisa que todo aumento de ancho de banda, estará sujeto a adenda adicional y a facilidades técnicas.

- K. Los siguientes equipos/accesorios, de ser requeridos, NO forman parte de la presente convocatoria y por lo tanto serán proporcionados por el SERNANP:
- ☐ Tomacorrientes.
 - ☐ Energía estabilizada.
 - ☐ Switch y sus respectivos puertos disponibles (donde se conectará el router). Este punto es solo para las sedes de provincia
 - ☐ Tendido de cableado eléctrico.
 - ☐ Sistema de Alimentación Ininterrumpida (UPS).
 - ☐ Armarios los Racks
 - ☐ Pozos de tierra
- L. Se deberá dejar configurar las cabeceras para que cuando se llame sernanp.gob.pe la conexión sea directa a la hacia la sede central del SERNANP (ida y vuelta).

6. GARANTÍA DE LOS EQUIPOS para el ITEM A y el ITEM B

El contratista deberá asegurar a la entidad (SERNANP) que, si alguno de los equipos que nos entregan como parte del servicio, a nivel nacional, fallara y se necesita su cambio, este deberá ser en un plazo máximo de 24 horas. Se aclara que estos días no incluye sábados y domingos. Se precisa que el postor deberá considerar todo lo necesario para cumplir con los tiempos de reposición del servicio

Se aclara que la solución que tenga que realizar el contratista para el cumplimiento de este punto será de su entera responsabilidad.

En caso del supuesto de que los equipos se encuentren en algún supuesto de pérdida de garantía indicado por el CONTRATISTA, la reparación y/o reposición de los equipos tendrá un costo que será asumido por la Entidad.

Se entiende por supuesto de pérdida de garantía cuando presenten lo siguientes: Golpes, quiebres, ingreso de líquido, y/o cualquier afectación al equipo imputable al usuario o manipulación del equipo por tercero

Dicho monto inicial no debe exceder del monto de compra del equipo el cual debe estar sustentado con el documento de compra del equipo.

Para el caso del supuesto de pérdida de garantía, se deberá remitir un informe del FABRICANTE fundamentando dicha pérdida de garantía e indicar cuál es el paso para seguir: reparación y/o reposición

7. GESTIÓN DE SERVICIO para el ITEM A y el ITEM B

✓ Niveles de Servicio

El contratista deberá garantizar los siguientes niveles mínimos de servicio:

Servicio	Disponibilidad mínima Mensual garantizada
Internet Sede central	99.90% (Con al menos dos enlaces redundantes provenientes de POPs o nodos distintos)
Internet Sedes remotas	Disponibilidad diferenciada de acuerdo a sus ubicaciones:

Cuadro de atención de averías diferenciado por sedes:

Tiempo de subsanación de averías no imputadas al contratista	Disponibilidad Mensual (incógnita X que se usará para las penalidades)	Ubicación	Dirección
04 horas	99.5%	Lima-almacen	Sede Av. José Gálvez Barrenechea 165 San Isidro
		Lima- OCI	Sede Av. José Gálvez Barrenechea 696 San Isidro
		Lima- Al frente	Calle diecisiete 438 San Isidro
			Huanuco - Jr. Elías Mabama N°290-PP.JJ. Túpac Amaru
		Ancash	Federico Sal y Rosas N° 555, Huaraz
		Junin	Av. Huancavelica N° 3113 El Tambo Huancayo
		Apurimac	Urbanización Santa Martha Mz. M - Lote 02, Abancay
		Lambayeque	Calle Los Laureles N° 330, Urb. Salaverry - Chiclayo
		Piura	Av. Los Cocos Mz. H-23 Urb. Club Grau-Piura
		Puno	PASAJE 2 DE FEBRERO N° 154,
		San Martín	Jr. Angel Delgado Morey 565, Barrio Partido Alto - Tarapoto, San Martín
		Tumbes	Av. Panamericana Norte N° 1739, Tumbes
		Cusco	URB. SANTA MARTHA E-12 APROVITE SAN JERONIMO
08 horas	98.8%	Ayacucho	Mz k-Lote 12 Centro Poblado Pucallma-Distrito de Quinua
		ICA	Car. Punta Pejerrey Km. 27 Paracas-Pisco-Ica
		Junin	Jr. San Martín N° 138 Lado Oeste, Junín
		San Martín	Carretera a Pósc-KM 01 Mz -47 LT-11, Sector Nueva Rioja – Rioja
		Huanuco	Jr. Elías Mabama N°290-PP.JJ. Túpac Amaru
13 horas	98.2%	Cajamarca	Av. San Juan N° 724 - Cutervo Cutervo - Cajamarca
		Cajamarca	Jr. Jose Olaya N° 518, San Ignacio, Cajamarca
		Cusco	JR. SABAS SARAZOLA K-17, SANTA ANA, LA CONVENCION
		Arequipa	Urb. Pampas de Aymaña F-12, Cotahuasi, La Unión - Arequipa
		Junin	Av. Antonio Raymondi Mz. A, Lote 3, 4, 5 en Urbanización Juan Ramon, San Ramón.
		Pasco	Av. Ernesto de Souza S/N, Cahchacucho - Huallay
		Ucayali	Av. Túpac Amaru - Mz G Lote 10, Calleria - Ucayali
24 horas	96.6%	Loreto	Calle Tacna N° 432, Iquitos - Maynas

Nota: Los tiempos de subsanación e avería se han calculado a través de la página:

<https://uptime.is/>

✓ **Soporte Técnico**

El contratista debe contar con un Centro de Operaciones para el servicio de Soporte Técnico 24x7x365 con línea de comunicación vía telefónica, **opcionalmente** correo electrónico y Portal Web de Mesa de Ayuda alineada **opcionalmente** a las mejores prácticas de ITIL para la atención de todas las solicitudes de soporte respecto al servicio solicitado a nivel nacional y los cambios de configuraciones de políticas en los dispositivos de seguridad perimetral, WAF y antirransomware.

Asimismo, para seguimiento de tickets se debe brindar las siguientes opciones: **(Se precisa que será suficiente que se cumpla al menos una de las dos opciones para el seguimiento de tickets)**

- Un Portal Web de Mesa de Ayuda para el seguimiento de los tickets de incidentes y cambios, este Portal debe estar alojado en el centro de datos propio o tercerizado certificado y ubicado en territorio nacional e integrarse con la herramienta de monitoreo. Para ello el contratista deberá otorgar una cuenta para el registro de tickets.
- Brindar un Service Manager dedicado exclusivamente a la entidad para la atención en horario de oficina y número celular dedicado para la atención, fuera de horario de atención se requiere: número gratuito 0800 con atención 24x7 para seguimiento de ticket de incidentes y cambios, así como envío de reportes de reportes de subsanación de averías indicando el tiempo de origen y finalización de la generación del ticket de atención para realizar la contabilización correspondiente en caso de aplicarse alguna penalidad.

Se aclara que el contratista debe contar con un NOC propio y un SOC propio o tercerizado. En caso de ser el SOC tercerizado, será obligación y responsabilidad del contratista mantener un contrato vigente con el propietario del SOC por el servicio correspondiente y durante toda la vigencia del contrato con la entidad. En caso el contratista decida cambiar el SOC tercerizado, deberá avisar a la entidad con una anticipación mínima de 60 días y confirmar el cumplimiento de todos los requisitos solicitados.

- El contratista deberá asignar un especialista residente que estará en el SOC del contratista y dedicado para la atención directa de los incidentes y requerimientos de la entidad durante el horario de oficina. **Se precisa que la documentación del especialista residente será presentada al finalizar la implementación junto con el informe final**
- La ENTIDAD podrá abrir casos directamente con el fabricante, de requerirlo, por lo que el contratista deberá brindarle los accesos correspondientes. Se aclara que el contratista podrá ser el encargado de escalar los casos a nivel interno y/o con el fabricante siempre y cuando el contratista mantenga informada de la entidad con el número de caso del fabricante.
- El servicio de soporte técnico comprenderá la solución de cualquier tipo de incidente que cause una interrupción parcial o total del servicio a nivel nacional solicitado por la entidad, así como a la pérdida de la calidad o degradación del mismo. Se aclara que todo tipo de incidente debe ser atendido por el SOC del contratista, pudiendo considerar los niveles de severidad para cada tipo que deberá estar claramente establecido en el Informe Final y según las mejores prácticas de ITIL.
- El servicio de soporte técnico comprenderá consultas, solicitudes de reportes, y solicitudes de análisis de auditoría. A todo ello se le denominará "requerimiento". Se aclara que el análisis de auditoría se refiere a una revisión sobre los servicios y/o equipos parte del servicio. Los reportes mínimos solicitados serán mensuales y a entregarse dentro de los diez (10) días siguientes del mes:
 - ✓ Reportes de tráfico WAN del router
 - ✓ Reportes de análisis del firewall
 - ✓ Reportes del WAF y Anti-ransomware
 - ✓ Reportes de calidad de servicio
- El especialista residente deberá realizar una presentación trimestral del servicio incluyendo

incidentes, requerimientos, desempeño de servicios, las sedes que más consumos presentan (aplicaciones, IPs), eventos de seguridad y proponiendo mejoras, fecha que será coordinada con la entidad. Asimismo, deberá coordinar reuniones con los fabricantes de los equipos a fin de proponer mejoras y nuevas características que desarrollen en beneficio de la entidad.

- El servicio de soporte técnico debe incluir el análisis, actualización, corrección y documentación de los incidentes en la solución implementada. Estos reportes deberán ser presentados dentro de los dos (02) días útiles de solucionado el mismo.
- Deberá brindar soporte técnico In Situ a nivel nacional a cargo de personal técnico del contratista, quien asistirá a la ENTIDAD en forma personal. Se precisa que el soporte técnico in situ se dará en caso de fallas que no puedan ser solucionados de manera remota:
 - Para el caso del soporte técnico In Situ para la sede central estará a cargo del especialista residente, quien asistirá a la ENTIDAD en forma personal.
 - Para el caso del soporte técnico In Situ en las otras sedes será brindado por el personal del contratista sin ser indispensable el requerimiento de experiencia en análisis de seguridad informática pero soportado remotamente por el especialista residente o personal experto del SOC a fin de solucionar las fallas presentadas
- Se precisa que el soporte técnico in situ se dará en caso de fallas que no puedan ser solucionados de manera remota.
- El servicio de soporte técnico se efectuará a través de línea telefónica, correo electrónico y [opcionalmente](#) un Portal Web de Mesa de Ayuda
- [De manera opcional, en caso de brindar un Portal Web de Mesa de Ayuda](#) debe estar implementada en la nube del contratista (centro de datos certificado) y estar alineada al proceso ITIL, para ello debe contar [opcionalmente](#) con al menos con cuatro (04) procesos certificados por PinkVerify.
- Una vez recibida tal notificación, EL CONTRATISTA, registrará el requerimiento y/o falla del servicio y proporcionará a la ENTIDAD un número de seguimiento al pedido.
- Se aclara que todos los tiempos serán contabilizados a partir de la entrega del ticket de atención respectivo.
- Se consideran los siguientes tiempos de respuesta a nivel nacional:

Tiempo máximo de Respuesta e identificación del problema	30 minutos
Tiempo máximo de Resolución de incidente de manera remota	02 horas
Tiempo máximo de Mantenimiento correctivo local	06 horas
Reemplazo de partes o equipos (RMA)	24 horas sin contar sábado y domingo

✓ **Niveles de Escalamiento:**

Cuadro N° 1: Niveles de escalamiento

Nivel de Escalamiento	Descripción	Periodo de atención	Tiempo de respuesta	Tiempo de solución
1	Especialista residente	Lunes a Viernes de 8:00 a.m. hasta las 6:00 p.m.	30 minutos	2 horas
2	Especialista en NOC/SOC	24x7	2 horas	4 horas
3	Fabricante de la solución	24x7	4 horas	24 horas

Se aclara que para el caso de una degradación del servicio que no implique corte total del servicio, y que este tenga que hacerse mediante reparación de algún equipo, el tiempo de resolución será de hasta 24 horas para todas las sedes de Lima y de 48 horas para las sedes de provincias.

El de Tiempo de Resolución de falla o avería (remoto) es 02 horas en la sede central y las otras

sedes será de 08 horas.

Se aclara que la solución que tenga que realizar el contratista para el cumplimiento de este punto será de su entera responsabilidad.

Se indica que el Especialista Residente y el Especialista NOC/SOC, deberán contar con acceso a los equipos y herramientas para las atenciones a la entidad. **El especialista NOC/SOC podrá ser el personal de turno disponible o un personal dedicado para la atención a la entidad**

El especialista residente deberá contar con al menos una certificación técnica (Firewall o WAF, o Anti-Ransomware), las cuales se presentarán como parte del informe cuando se presente alguna incidencia.

El Especialista Residente podrá ser reemplazado eventualmente por el Especialista NOC/SOC. Todos los tiempos indicados como parte del nivel de atención, son contados desde el registro de la solicitud de requerimiento y/o incidente, de la entidad al Contratista, mediante tickets de atención.

Tiempo de respuesta, se define desde que se reporta el requerimiento y/o incidente del servicio por parte de la entidad, mediante llamada telefónica, correo electrónico o Portal Web hasta el instante que el personal designado por el contratista tome contacto con los encargados de la UOF TIC de la entidad.

Tiempo de solución, se define desde que el especialista del contratista registra el incidente mediante un ticket de atención hasta el instante que el servicio ha retomado a su operación normal.

✓ **Procedimiento de solución de incidentes:**

- Al ocurrir una avería o caída del servicio o equipamiento de seguridad, de severidad media o alta, el SOC lo alertará de manera automática con su sistema de monitoreo y gestión y se generará el ticket de manera automática en el ServiceDesk del contratista y que luego será informado a la UOF TIC. Se requiere que la herramienta de monitoreo se encuentre integrada con el ServiceDesk.
O también será válido que al ocurrir una caída de servicio del equipamiento de seguridad, el SOC lo alertará de manera automática con su sistema de monitoreo y gestión y se generará el ticket luego será informado a la UOF TIC
- Al requerir uno o varios cambios en las políticas y/o configuraciones de los equipos de seguridad o reportes a demanda, que la entidad solicite o desee realizar, la UOF TIC de la entidad reportará al Especialista Residente por teléfono o correo electrónico o Portal Web. Cabe indicar que los cambios en las políticas y/o configuraciones y reportes, sin restricción de cantidad de solicitudes y sin costos adicionales. Cabe indicar que los cambios en las políticas y/o configuraciones y reportes, el Contratista los atenderá de manera ilimitada, sin restricción de cantidad de solicitudes y sin costos adicionales.
- Una vez recibida la notificación, el Especialista residente registrará el requerimiento de servicio y proporcionará a la entidad un número de ticket de incidente o requerimiento. Dicho ticket servirá para realizar el seguimiento respectivo y escalamiento que fuera necesario.
- En caso que el Especialista residente no solucione el incidente tendrá que escalar al nivel 2, donde el Especialista en el NOC/SOC de la solución específica atenderá el incidente presentado.
- De no solucionar la problemática el nivel 2, el incidente se escala al nivel 3 donde el fabricante brinda la solución definitiva.
- El ticket será cerrado, cuando se solucione el incidente o se atienda el requerimiento y se obtenga la correspondiente aprobación por parte de la entidad.
- El soporte proporcionado por el contratista será telefónico, remoto y on-site, dependiendo de la severidad del caso

8. CUADRO DE ATENCIÓN DE SOLICITUDES TÉCNICAS SOLO PARA EL ÍTEM A:

Nateo (IP privada vs IP publica) para publicación web de servicios (Firewall) incluida liberación de los puertos	maximo 24 horas de lunes a viernes
--	------------------------------------

solicitados por el SERNANP	
Registro de subdominios asociado a la IP Publica en los DNS que nos brindan al SERNANP	maximo 24 horas de lunes a viernes
Registro y/o anulación de subdominios en los DNS que nos brindan al SERNANP	maximo 24 horas de lunes a viernes
Generación de nuevas cuentas VPN	maximo 24 horas de lunes a viernes
Configurar los filtros de ingreso exclusivo de algunas IP publicas de entidades externas (firewall) para que tengan permisos de consumir los servicios informáticos que indique el SERNANP	maximo 24 horas de lunes a viernes

9. LUGAR DEL SERVICIO

La implementación del servicio para el ITEM A se dará según las direcciones indicadas en el cuadro A

La implementación del servicio para el ITEM B se dará según las direcciones indicadas en el cuadro B

Para el ITEM A y el ITEM B, el contratista deberá considerar que el servicio solicitado incluya la entrega de los bienes necesarios y en calidad de prestamo como parte del servicio y solo por el periodo que dure el contrato.

Se aclara que una vez finalizado el plazo contractual se devolverán los equipos, sin más desgaste que el de su uso normal

10. PLAZO DE IMPLEMENTACIÓN E INICIO DEL SERVICIO

- **Para el ITEM A** el plazo de implementación y activación del servicio será como máximo de **cien (100)** días calendarios contados a partir del día siguiente de la firma del contrato.

Para ello se realizarán las siguientes pruebas:

- 1- Prueba de saturación de enlace que permita garantizar el ancho de banda dedicado de cada sede para el servicio de Internet
- 2- Prueba de descarga de archivos que permita verificar el tiempo que toma la descarga a realizarse desde cada sede hacia páginas Web
- 3- Pruebas de visualización de la disponibilidad del servicio (**el postor debe mostrar un protocolo de pruebas donde se demuestre la disponibilidad del servicio**)

- **Para el ITEM B.** el plazo de implementación se iniciará desde el día siguiente de la firma del contrato hasta máximo 15 días calendarios antes de la culminación del servicio vigente (14 de septiembre del 2023).

Para ello se realizarán las siguientes pruebas:

- 1- Prueba de saturación de enlace que permita garantizar el ancho de banda dedicado de cada sede para el servicio de Internet
- 2- Prueba de Bypass de los equipos WAF y Anti-Ransomware: apagado del equipo y verificar la disponibilidad del servicio.
- 3- Prueba de descarga de archivos que permita verificar el tiempo que toma la descarga a realizarse desde cada sede hacia páginas Web
- 4- Pruebas de visualización de la disponibilidad del servicio (**el postor debe mostrar un protocolo**

[de pruebas donde se demuestre la disponibilidad del servicio.\)](#)

5- Pruebas del servicio (activo pasivo en el local de la sede central)

Tener en cuenta que una vez terminada la implementación, este servicio se activará desde el día siguiente de la culminación del servicio vigente, es decir desde el 15 de septiembre del 2023.

Para el ITEM A y el ITEM B, se aclara que la entidad garantizará al Contratista todas las facilidades técnicas que sean necesarias; así como todos los accesos que correspondan, teniendo a su cargo la responsabilidad de gestionar las autorizaciones de ingreso necesarias, de desocupar los espacios, oficinas y/o pasillos donde vayan a ser ejecutados los respectivos trabajos de instalación, así como la provisión de los servicios correspondientes para la instalación de cualquier equipo.

Para el ITEM A y el ITEM B, se aclara que, en caso de existir atrasos y/o paralizaciones no imputables al contratista, éste podrá solicitar la ampliación de plazo correspondiente de acuerdo a lo señalado en la normativa vigente de la Ley de Contrataciones del Estado y su Reglamento.

11. PLAZO DE PRESTACIÓN DEL SERVICIO

Para el ITEM A y el ITEM B, cada servicio será brindado por un periodo de 24 meses.

Para el ITEM A, el plazo de prestación del servicio será contabilizado a partir del día siguiente que se suscriba por parte del Contratista y la UOF TIC del SERNANP el Acta de Activación del Servicio

Para poder firmar esta Acta de Activación del Servicio se deberá contar previamente con los siguientes actas firmadas y aprobadas:

- ✓ Actas de conformidades operatividad del servicio por parte de cada uno de los jefes o quien ellos designen de cada local en provincia

Para el ITEM B, el plazo de prestación del servicio será contabilizado a partir del día siguiente que se suscriba por parte del Contratista y la UOF TIC del SERNANP el Acta de Activación del Servicio

Para el ITEM A y el ITEM B, se aclara que el plazo de prestación del servicio será computado a partir de la fecha de firma de la respectiva Acta de Activación y no desde la fecha de firma del contrato.

12. REQUISITOS DEL CONTRATISTA Y/O PERSONAL para el ITEM A y EL ITEM B

✓ **REQUISITOS DEL CONTRATISTA para el ITEM A y EL ITEM B**

- Empresa dedicada a la venta del servicio de Internet, servicios VPN, servicio de interconexión de uno o varios locales en general, servicio de Internet en General, servicio de Ciberseguridad, servicio de Transmisión de datos, servicio de Transmisión de Datos.
- Deberá poseer un NETWORK OPERATION CENTER (NOC 7x24x365) propio que asegure la administración de conectividad punto a punto, el monitoreo proactivo, la generación de soluciones flexibles a requerimientos del cliente y brindar soporte y asistencia técnica alineados a los acuerdos de nivel de servicio.
- Deberá contar con un SECURITY OPERATION CENTER (SOC 7x24x365) con personal especializado, el cual será responsable del monitoreo de la salud del servicio contratado, así como la prevención, detección, atención, tratamiento y resolución de incidentes de seguridad asociados al servicio.
- El contratista deberá ser miembro activo y directo del NAP Perú. Deberá presentar un documento que lo acredite a la firma del contrato

Se aclara que la entrega de los informes mensuales se podrá dar por medios digitales a la mesa de partes virtual de la entidad. El plazo de entrega es responsabilidad del contratista ya que de este depende su conformidad y pago correspondiente

Para el ITEM B

- ✓ Plan de implementación, presentada en un plazo no mayor a los veinte (20) días calendario contados a partir del día siguiente de la firma del contrato.
- ✓ Informe Final, a ser presentado en un plazo no mayor de 05 días calendarios contados a partir del día siguiente de la firma del Acta de Activación del Servicio, el cual deberá contener como mínimo:
 - Para el caso de los softwares requeridos serán entregados en DVD o descarga electrónica del sitio web del fabricante, así como el licenciamiento correspondiente.
 - Documentación técnica de los equipos adquiridos, el contratista deberá suministrar en forma impresa y digital.
 - Documentación conteniendo la arquitectura y funcionamiento detallado de toda la solución
 - Planos en Auto CAD a escala (01 juego impreso a colores) donde se visualice la ruta de los enlaces por cada local, desde el ingreso al local hasta los gabinetes de comunicaciones del SERNANP.
 - Planos en Auto CAD (01 juego impreso a colores) donde se visualice el esquema de solución implementada y la distribución de los equipos en los gabinetes de comunicaciones del SERNANP.
 - Un juego impreso a colores del Diagrama de Red de la solución implementada, donde se muestre los routers, y para el caso de la Sede Central incluir los equipos de seguridad perimetral, los switch de core, entre otros que hayan implementado y que estarán a cargo de estos servicios.
 - Diagrama de interconexión a nivel WAN (01 juego impreso a colores), incluyendo la parte de acceso (última milla) y una descripción donde se describirá las soluciones, marca y modelo propuesto.
 - Diagrama de interconexión a nivel de direccionamiento IP (01 juego impreso a colores), el cual deberá incluir las soluciones de seguridad perimetral, routers, switches y Anti-DDoS con las IP finales.
- ✓ El contratista deberá entregar un informe mensual para el pago que contenga la utilización del consumo de ancho de banda por cada local y el reporte mensual de tráfico por reglas configuradas en el firewall.

Este informe debe ser entregado pasado el mes correspondiente del servicio, el cual servirá para la conformidad respectiva y el pago mensual por el servicio prestado.

Se aclara que la entrega de los informes mensuales se podrá dar por medios digitales a la mesa de partes virtual de la entidad. El plazo de entrega es responsabilidad del contratista ya que de este depende su conformidad y pago correspondiente

14. CONFIDENCIALIDAD para el ITEM A y EL ITEM B

EL CONTRATISTA se compromete a mantener en reserva, y no revelar a terceros, sin autorización escrita de la Entidad, la información que le sea suministrada por este último o a la cual tenga acceso, excepto en cuanto resultare estrictamente necesario para el cumplimiento del Contrato, y que restringirá la revelación de dicha información sólo a sus empleados y subcontratistas, sobre la base de "necesidad de conocer".

EL CONTRATISTA se compromete a preservar la privacidad de la información que será transportada por la red contratada.

Se aclara que la obligación de confidencialidad no resulta aplicable en los siguientes supuestos:

1. Cuando la información en cuestión haya sido de difusión o acceso público;
2. Cuando la información en cuestión haya sido publicada antes de haber sido puesta a disposición del contratista;
3. Cuando la información en cuestión ya obre en poder del contratista y no esté sujeta a cualquier otro impedimento o restricción que le haya sido puesto de manifiesto;
4. Cuando la información en cuestión haya sido recibida a través de terceros sin restricciones y sin que implique incumplimiento del Contrato;
5. Cuando la información en cuestión haya sido independientemente desarrollada por el contratista, siempre que no se hubiese utilizado para ello otra información confidencial; o
6. Cuando la información en cuestión deba ser revelada a alguna autoridad autorizada para dar cumplimiento a una orden de naturaleza judicial o administrativa, bastando para ello informar a la Entidad la recepción de dicha orden.

15. CONFORMIDAD DEL SERVICIO para el ITEM A y EL ITEM B

La conformidad del servicio será emitida por la UOF TIC del SERNANP, con la presentación de los entregables correspondientes.

16. FORMA DE PAGO para el ITEM A y EL ITEM B

Los pagos serán mensuales durante el periodo de la prestación del presente servicio, con la presentación de la factura por parte del contratista, su informe mensual con los reportes correspondientes y la conformidad de la UOF de Tecnologías de la Información y Comunicaciones.

Tener en cuenta que solo para el primer pago se deberá presentar el Plan de implementación, el Informe Final y el Informe mensual

Se aclara: en caso que el inicio de la prestación del servicio no coincida con el ciclo de facturación del operador adjudicatario de la buena pro, la facturación incluiría un cargo por el prorrateo del servicio brindado durante los días previos al inicio del correspondiente ciclo de facturación.

Se aclara: que se aceptará el ciclo de facturación que le asigne el proveedor ganador de la Buena Pro, el cuál será el más cercano a la fecha de activación del servicio.

Se aclara: en caso que el inicio de la prestación del servicio no coincida con el ciclo de facturación del operador adjudicatario de la buena pro, la facturación incluiría un cargo por el prorrateo del servicio brindado durante los días previos al inicio del correspondiente ciclo de facturación.

17. PENALIDADES

Se aplicará una penalidad de hasta el 10% del monto contratado en caso de retraso injustificado del contratista, según el artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

✓ **Disponibilidad del Servicio**

En caso de no cumplirse la disponibilidad mínima del servicio, según el tiempo especificado por tipo de incidente, se aplicará la penalidad correspondiente de acuerdo al siguiente cuadro:

Disponibilidad del Servicio de Internet de la Sede central: (Para el ITEM B)

Descripción	Medición	Penalidad	Procedimiento
Disponibilidad Mayor o igual a 99.90%	Mensual	No aplica penalidad	La disponibilidad se verá en el informe mensual que entrega el contratista para el pago, el cual contiene la utilización del consumo de ancho de banda por cada local
Disponibilidad Mayor o igual a 99.50% y Menor al 99.90%	Mensual	50% de la UIT (La penalidad se aplicará por ocurrencia)	
Disponibilidad Mayor o igual a 99.00% y Menor al 99.50%	Mensual	100% de la UIT (La penalidad se aplicará por ocurrencia)	
Disponibilidad menor al 99.00%	Mensual	200% de la UIT (La penalidad se aplicará por ocurrencia)	

Disponibilidad del Servicio de Sedes Remotas (Para el ITEM B)

Descripción	Medición	Penalidad	Procedimiento
Disponibilidad Mayor o igual al % de la incógnita X correspondiente	Mensual	No aplica penalidad	La disponibilidad se verá en el informe mensual que entrega el contratista para el pago, el cual contiene la utilización del consumo de ancho de banda por cada local
Disponibilidad Mayor o igual al % de la incógnita X correspondiente menos 0.40% y Menor al % de la incógnita X correspondiente	Mensual	50% de la UIT (La penalidad se aplicará por ocurrencia)	
Disponibilidad Mayor o igual al % de la incógnita X correspondiente menos 0.90% y Menor al % de la incógnita X correspondiente menos 0.40%	Mensual	100% de la UIT (La penalidad se aplicará por ocurrencia)	
Disponibilidad menor al % de la incógnita X correspondiente menos 0.90%	Mensual	200% de la UIT (La penalidad se aplicará por ocurrencia)	

La incógnita X correspondiente se encuentra en el **Cuadro de atención de averías diferenciado por sedes**.

La indisponibilidad se contará desde que se tiene un ticket del incidente generado telefónicamente o a través del portal del contratista, y a partir de ese momento se contarán los minutos de indisponibilidad hasta que el contratista de servicio brinde la solución del incidente. La indisponibilidad menor al 99.0% se aplicará la penalidad correspondiente según tabla.

Disponibilidad del Servicio de Sedes Remotas (Para el ITEM A)

Descripción	Medición	Penalidad	Procedimiento
Disponibilidad Mayor o igual al % de la incógnita X correspondiente	Mensual	No aplica penalidad	La disponibilidad se verá en el informe mensual que entrega el contratista para el pago, el cual contiene la utilización del consumo de ancho de banda por cada local
Disponibilidad Mayor o igual al % de la incógnita X correspondiente menos 0.40% y Menor al % de la incógnita X correspondiente	Mensual	50% de la UIT (La penalidad se aplicará por ocurrencia)	
Disponibilidad Mayor o igual al % de la incógnita X correspondiente menos 0.90% y Menor al % de la incógnita X correspondiente menos 0.40%	Mensual	100% de la UIT (La penalidad se aplicará por ocurrencia)	
Disponibilidad menor al % de la incógnita X correspondiente menos 0.90%	Mensual	200% de la UIT (La penalidad se aplicará por ocurrencia)	

La indisponibilidad se contará desde que se tiene un ticket del incidente generado telefónicamente

o a través del portal del contratista, y a partir de ese momento se contarán los minutos de indisponibilidad hasta que el contratista de servicio brinde la solución del incidente. La indisponibilidad menor al 99.0% se aplicará la penalidad correspondiente según tabla.

18. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es responsable por la Calidad ofrecida y por los vicios ocultos de los bienes y servicios ofertados por un plazo de un (01) año contado a partir de la conformidad otorgada por la Entidad.

19. FUENTE DE FINANCIAMIENTO

RO

20. META PRESUPUESTAL

0212 (GERENCIA GENERAL)
0050 (OA-UNIDADES OPERATIVAS)

21. ESPECIFICA DE GASTO

2.3.2.2.2.3



REPÚBLICA
DEL PERÚ
Firma Digital

Firmado digitalmente por:
CAMACHO VILLANUEVA Manuel
Francisco FAU 20478053178 soft
Motivo: Soy el autor del documento
Fecha: 27/04/2023 15:45:28-0500

3.2. REQUISITOS DE CALIFICACIÓN PARA AMBOS ITEMS

B.3	CALIFICACIONES DEL PERSONAL CLAVE PARA EL ITEM A Y EL ITEM B
B.3.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>JEFE DE PROYECTO</p> <ul style="list-style-type: none"> - Un (01) Ingeniero titulado en Telecomunicaciones, Sistemas, Redes, Comunicaciones, Electrónica o afines. <p>ESPECIALISTA EN SEGURIDAD</p> <ul style="list-style-type: none"> - Un (01) Ingeniero titulado o Bachiller en Telecomunicaciones, Sistemas, Redes, Comunicaciones, Electrónica o afines. <p>ESPECIALISTA EN INSTALACIÓN</p> <ul style="list-style-type: none"> - Un (01) Ingeniero titulado o Bachiller o Técnico en Telecomunicaciones, Sistemas, Redes, Comunicaciones, Electrónica o afines. <p><u>Acreditación:</u></p> <p>El grado o título 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.</p> <p>En caso el grado o título 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.</p>
B.3.2	CAPACITACIÓN
	<p><u>Requisitos:</u></p> <p>JEFE DE PROYECTO</p> <ul style="list-style-type: none"> - Contar con Certificación PMP (Project Management Professional) <p>ESPECIALISTA EN SEGURIDAD</p> <ul style="list-style-type: none"> - Contar con Certificación en la marca de Firewalls y/o Certificación en Seguridad de Aplicaciones y/o Experto del fabricante WAF de la solución ofertada. <p>ESPECIALISTA EN INSTALACIÓN</p> <ul style="list-style-type: none"> - Contar con Certificación en la marca de router propuestos. <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de constancias, certificado, u otro documento que corresponda.</p> <div> <p>Importante</p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p> </div>

B.4	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>JEFE DE PROYECTO</p> <p>- Mínimo tres (03) años de experiencia en la Gestión de Proyectos de telecomunicaciones, o tres (03) años de experiencia en gestionar y/o supervisar y/o liderar la implementación de proyectos de telecomunicaciones (acceso a internet y/o redes de datos y/o telefonía fija) y/o servicios TI (ciberseguridad y/o gestión de aplicaciones y/o servidores y/o infraestructura Data center y/o cloud) y/o Gestión de los proyectos de implementación de transmisión de datos, internet y/o Comunicaciones Unificadas y/o Telefonía e Infraestructura de Data Center.</p> <p>ESPECIALISTA EN SEGURIDAD</p> <p>- Mínimo dos (02) años de experiencia en la implementación y/o gestión y/o soporte de soluciones de seguridad perimetral y/o soluciones WAF.</p> <p>ESPECIALISTA EN INSTALACIÓN</p> <p>- Mínimo dos (02) años de experiencia en la implementación de servicios de telecomunicaciones.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <div> <p>Importante</p> <ul style="list-style-type: none"> • <i>Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.</i> • <i>En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.</i> • <i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i> • <i>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.</i> </div>

C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 7'920,000.00 (Siete millones novecientos veinte mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran servicios similares a los siguientes: venta del servicio de Internet, servicios VPN, servicio de interconexión de uno o varios locales en general, servicio de Internet en General, servicio de Ciberseguridad, servicio de Transmisión de datos, servicio de Transmisión de Datos.</p> <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 pago¹⁰, 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 presumirá que las obligaciones se ejecutaron en partes iguales.</p> <p>Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.</p> <p>Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.</p> <p>Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.</p>

¹⁰ 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".

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).		La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $P_i = \frac{O_m \times PMP}{O_i}$ <p> <i>i</i> = Oferta P_i = Puntaje de la oferta a evaluar O_i = Precio <i>i</i> O_m = Precio de la oferta más baja PMP = Puntaje máximo del precio </p> <p style="text-align: right;">100 puntos</p>

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 SERVICIO DE ACCESO A INTERNET PARA LAS SEDES DE LAS OFICINAS DE LAS ÁREAS NATURALES PROTEGIDAS Y LA SEDE CENTRAL DEL SERNANP, MEDIANTE LÍNEAS DEDICADAS DE CONEXIÓN PERMANENTE A INTERNET, POR UN PERIODO DE 24 MESES**, que celebra de una parte **[CONSIGNAR EL NOMBRE DE LA ENTIDAD]**, en adelante LA ENTIDAD, con RUC Nº [.....], con domicilio legal en [.....], representada por [.....], identificado con DNI Nº [.....], y de otra parte [.....], con RUC Nº [.....], con domicilio legal en [.....], inscrita en la Ficha Nº [.....] Asiento Nº [.....] del Registro de Personas Jurídicas de la ciudad de [.....], debidamente representado por su Representante Legal, [.....], con DNI Nº [.....], según poder inscrito en la Ficha Nº [.....], Asiento Nº [.....] del Registro de Personas Jurídicas de la ciudad de [.....], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [.....], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO Nº 003-2023-SERNANP**, para **LA CONTRATACIÓN DEL SERVICIO DE SERVICIO DE ACCESO A INTERNET PARA LAS SEDES DE LAS OFICINAS DE LAS ÁREAS NATURALES PROTEGIDAS Y LA SEDE CENTRAL DEL SERNANP, MEDIANTE LÍNEAS DEDICADAS DE CONEXIÓN PERMANENTE A INTERNET, POR UN PERIODO DE 24 MESES**, a **[INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO]**, cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto **LA CONTRATACIÓN DEL SERVICIO DE SERVICIO DE ACCESO A INTERNET PARA LAS SEDES DE LAS OFICINAS DE LAS ÁREAS NATURALES PROTEGIDAS Y LA SEDE CENTRAL DEL SERNANP, MEDIANTE LÍNEAS DEDICADAS DE CONEXIÓN PERMANENTE A INTERNET, POR UN PERIODO DE 24 MESES**.

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 PAGO¹¹

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.

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

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

LA ENTIDAD debe efectuar el pago de las contraprestaciones pactadas a favor del CONTRATISTA dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, 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].

Importante para la Entidad

De preverse en los Términos de Referencia la ejecución de actividades de instalación, implementación u otros que deban realizarse de manera previa al inicio del plazo de ejecución, se debe consignar lo siguiente:

“El plazo para la [CONSIGNAR LAS ACTIVIDADES PREVIAS PREVISTAS EN LOS TÉRMINOS DE REFERENCIA] es de [...], el mismo que se computa desde [INDICAR CONDICIÓN CON LA QUE DICHAS ACTIVIDADES SE INICIAN].”

Incorporar a las bases o eliminar, según corresponda.

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

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

CLÁUSULA SÉTIMA: GARANTÍAS

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

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

Importante

Al amparo de lo dispuesto en el numeral 149.4 del artículo 149 del Reglamento de la Ley de Contrataciones del Estado, en el caso de contratos periódicos de prestación de servicios en general, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato original como garantía de fiel cumplimiento de contrato, debe consignarse lo siguiente:

“De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo.”

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

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

CLÁUSULA DÉCIMA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

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

De existir observaciones, LA ENTIDAD las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (8) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no 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 manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD no otorga la conformidad, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

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

El plazo máximo de responsabilidad del contratista es de [CONSIGNAR TIEMPO EN AÑOS, NO MENOR DE UN (1) AÑO] año(s) contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

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

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

Donde:

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

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

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

OTRAS PENALIDADES

Disponibilidad del Servicio

En caso de no cumplirse la disponibilidad mínima del servicio, según el tiempo especificado por tipo de incidente, se aplicará la penalidad correspondiente de acuerdo al siguiente cuadro:

Disponibilidad del Servicio de Internet de la Sede central: (Para el ITEM B)

Descripción	Medición	Penalidad	Procedimiento
Disponibilidad Mayor o igual a 99.90%	Mensual	No aplica penalidad	La disponibilidad se verá en el informe mensual que entrega el contratista para el pago, el cual contiene la utilización del consumo de ancho de banda por cada local
Disponibilidad Mayor o igual a 99.50% y Menor al 99.90%	Mensual	50% de la UIT (La penalidad se aplicará por ocurrencia)	
Disponibilidad Mayor o igual a 99.00% y Menor al 99.50%	Mensual	100% de la UIT (La penalidad se aplicará por ocurrencia)	
Disponibilidad menor al 99.00%	Mensual	200% de la UIT (La penalidad se aplicará por ocurrencia)	

Disponibilidad del Servicio de Sedes Remotas (Para el ITEM B)

Descripción	Medición	Penalidad	Procedimiento
Disponibilidad Mayor o igual al % de la incógnita X correspondiente	Mensual	No aplica penalidad	La disponibilidad se verá en el informe mensual que entrega el contratista para el pago, el cual contiene la utilización del consumo de ancho de banda por cada local
Disponibilidad Mayor o igual al % de la incógnita X correspondiente menos 0.40% y Menor al % de la incógnita X correspondiente	Mensual	50% de la UIT (La penalidad se aplicará por ocurrencia)	
Disponibilidad Mayor o igual al % de la incógnita X correspondiente menos 0.90% y Menor al % de la incógnita X correspondiente menos 0.40%	Mensual	100% de la UIT (La penalidad se aplicará por ocurrencia)	
Disponibilidad menor al % de la incógnita X correspondiente menos 0.90%	Mensual	200% de la UIT (La penalidad se aplicará por ocurrencia)	

Disponibilidad del Servicio de Sedes Remotas (Para el ITEM A)

Descripción	Medición	Penalidad	Procedimiento
Disponibilidad Mayor o igual al % de la incógnita X correspondiente	Mensual	No aplica penalidad	La disponibilidad se verá en el informe mensual que entrega el contratista para el pago, el cual contiene la utilización del consumo de ancho de banda por cada local
Disponibilidad Mayor o igual al % de la incógnita X correspondiente menos 0.40% y Menor al % de la incógnita X correspondiente	Mensual	50% de la UIT (La penalidad se aplicará por ocurrencia)	
Disponibilidad Mayor o igual al % de la incógnita X correspondiente menos 0.90% y Menor al % de la incógnita X correspondiente menos 0.40%	Mensual	100% de la UIT (La penalidad se aplicará por ocurrencia)	
Disponibilidad menor al % de la incógnita X correspondiente menos 0.90%	Mensual	200% de la UIT (La penalidad se aplicará por ocurrencia)	

La incógnita "X" y la indisponibilidad, se tratan en el numeral 17) de los términos de referencia, referida a las penalidades.

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

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

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

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

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

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

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

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

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

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

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

CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO

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

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS¹²

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

¹² 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).

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

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

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

CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

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

CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

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

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

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

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

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

“LA ENTIDAD”

“EL CONTRATISTA”

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹³.

¹³ Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>

ANEXOS

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 003-2023-SERNANP

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 ¹⁴		Sí	No
Correo electrónico :			

Autorización de notificación por correo electrónico:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios¹⁵

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.

¹⁴ 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.

¹⁵ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

Importante

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

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 003-2023-SERNANP
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 ¹⁶	Sí		No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁷	Sí		No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁸	Sí		No	
Correo electrónico :				

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

¹⁶ 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.

¹⁷ Ibídem.

¹⁸ Ibídem.

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios¹⁹

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.

¹⁹ 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 Nº 2

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 003-2023-SERNANP
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 Nº 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 Nº 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.
- v. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.
- vi. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.
- vii. Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO Nº 003-2023-SERNANP

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° 003-2023-SERNANP

Presente. -

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

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 5

PROMESA DE CONSORCIO

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

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO Nº 003-2023-SERNANP

Presente. -

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO Nº [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] [%]²⁰

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²¹

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

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

²¹ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

TOTAL OBLIGACIONES

100%²²

[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.

²² Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

ANEXO Nº 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 003-2023-SERNANP
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
ITEM A: Servicio de internet en 22 locales a nivel nacional.	
ITEM B: Servicio de internet en la sede central y tres locales en Lima	
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

“El postor puede presentar el precio de su oferta en un solo documento o documentos independientes, en los ítems que se presente”.

ANEXO Nº 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 003-2023-SERNANP
Presente. -

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

Nº	CLIENTE	OBJETO DEL CONTRATO	Nº CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²³	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁴	EXPERIENCIA PROVENIENTE ²⁵ DE:	MONEDA	IMPORTE ²⁶	TIPO DE CAMBIO VENTA ²⁷	MONTO FACTURADO ACUMULADO ²⁸
1										
2										
3										
4										

²³ 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.

²⁴ Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho periodo.

²⁵ 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 Nº 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 Nº 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”.

²⁶ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

²⁷ 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.

²⁸ Consignar en la moneda establecida en las bases.

Nº	CLIENTE	OBJETO DEL CONTRATO	Nº CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²³	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁴	EXPERIENCIA PROVENIENTE ²⁵ DE:	MONEDA	IMPORTE ²⁶	TIPO DE CAMBIO VENTA ²⁷	MONTO FACTURADO ACUMULADO ²⁸
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 9

DECLARACIÓN JURADA (NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO Nº 003-2023-SERNANP

Presente. -

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

ANEXO N° 12

**AUTORIZACIÓN DE NOTIFICACIÓN DE LA DECISIÓN DE LA ENTIDAD SOBRE LA
SOLICITUD DE AMPLIACIÓN DE PLAZO MEDIANTE MEDIOS ELECTRÓNICOS DE
COMUNICACIÓN**

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 003-2023-SERNANP
Presente. –

El que se suscribe, [.....], postor adjudicado y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], autorizo que durante la ejecución del contrato se me notifique al correo electrónico [INDICAR EL CORREO ELECTRÓNICO] lo siguiente:

✓ Notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

La notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo se efectúa por medios electrónicos de comunicación, siempre que se cuente con la autorización correspondiente y sea posible obtener un acuse de recibo a través del mecanismo utilizado.