

BASES ADMINISTRATIVAS 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

SIMBOLOGÍA UTILIZADA:

Nº	Símbolo	Descripción
1	[ABC] / [.....]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / [.....]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	<div>Importante</div> <ul style="list-style-type: none"> • Abc 	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	<div>Advertencia</div> <ul style="list-style-type: none"> • Abc 	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	<div>Importante para la Entidad</div> <ul style="list-style-type: none"> • Xyz 	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

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

Nº	Características	Parámetros
1	Márgenes	Superior : 2.5 cm Inferior: 2.5 cm Izquierda: 2.5 cm Derecha: 2.5 cm
2	Fuente	Arial
3	Estilo de Fuente	Normal: Para el contenido en general Cursiva: Para el encabezado y pie de página Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
4	Color de Fuente	Automático: Para el contenido en general Azul : Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
5	Tamaño de Letra	16 : Para las dos primeras hojas de las Secciones General y Específica 11 : Para el nombre de los Capítulos. 10 : Para el cuerpo del documento en general 9 : Para el encabezado y pie de página Para el contenido de los cuadros, pudiendo variar, según la necesidad 8 : Para las Notas al pie
6	Alineación	Justificada: Para el contenido en general y notas al pie. Centrada : Para la primera página, los títulos de las Secciones y nombres de los Capítulos)
7	Interlineado	Sencillo
8	Espaciado	Anterior : 0 Posterior : 0
9	Subrayado	Para los nombres de las Secciones y para resaltar o hacer hincapié en algún concepto

INSTRUCCIONES DE USO:

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

Elaboradas en enero de 2019

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



Ministerio de Salud

Dirección de Redes
Integradas de Salud
Lima Norte

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

**CONCURSO PÚBLICO N°
01-2025-DIRIS.LN/CS-1**

PRIMERA CONVOCATORIA

**CONTRATACIÓN DE SERVICIO DE SERVICIO DE
TRANSMISIÓN DE DATOS, INTERNET DEDICADO CON
SEGURIDAD VIRTUAL Y TELEFONÍA PARA LA SEDE
CENTRAL Y LOS ESTABLECIMIENTOS DE SALUD DE LA
JURISDICCIÓN DE LA DIRIS LIMA NORTE**

ABRIL, 2025

DEBER DE COLABORACIÓN

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

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

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

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

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

Importante

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

Importante

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

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

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

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

Advertencia

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

Importante

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

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

Importante

- Los formularios electrónicos que se encuentran en el SEACE y que los proveedores deben llenar para presentar sus ofertas, tienen carácter de declaración jurada.

¹ Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>

- *En 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 : DIRECCION DE REDES INTEGRADAS DE SALUD LIMA NORTE

RUC N° : 20602217508

Domicilio legal : Calle A Mz. 02 Lt. 03 Asoc. Víctor Raúl Haya de la Torre - Distrito Independencia - Independencia – Lima.

Teléfono: : (51) 912217181

Correo electrónico: : procesos.dirislimanorte2024@gmail.com

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del **SERVICIO DE TRANSMISIÓN DE DATOS, INTERNET DEDICADO CON SEGURIDAD VIRTUAL Y TELEFONÍA PARA LA SEDE CENTRAL Y LOS ESTABLECIMIENTOS DE SALUD DE LA JURISDICCIÓN DE LA DIRIS LIMA NORTE.**

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante FORMATO N° 02 N° 15-2025-DA-DIRIS.LN de fecha 16 de abril del 2025.

1.4. FUENTE DE FINANCIAMIENTO

00 – RECURSOS ORDINARIOS

Importante

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

1.5. SISTEMA DE CONTRATACIÓN

El presente procedimiento se rige por el sistema de SUMA ALZADA, de acuerdo con lo establecido en el expediente de contratación respectivo.

1.6. DISTRIBUCIÓN DE LA BUENA PRO

NO CORRESPONDE.

1.7. ALCANCES DEL REQUERIMIENTO

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

1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

Los servicios materia de la presente convocatoria se prestarán en el plazo de OCHOCIENTOS VEINTE (820) DIAS CALENDARIO, en concordancia con lo establecido en el expediente de contratación, que comprenden los siguientes plazos:

- a. El plazo de implementación será de **Noventa (90) días calendario**.
- b. El plazo de ejecución del servicio en marcha será brindado por **Setecientos Treinta (730) días calendarios** y deberá iniciar a partir del día siguiente de suscrita el Acta de Conformidad de la implementación de todas las sedes por parte del Área Usuaria.

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/ 10.00 (Diez con 00/100 Soles) en Caja de la Entidad sito en la Calle A Mz. 02 Lt. 03 Asoc. Víctor Raúl Haya de la Torre - Distrito Independencia - Independencia – Lima.

Importante

<i>El costo de entrega de un ejemplar de las bases no puede exceder el costo de su reproducción.</i>
--

1.10. BASE LEGAL

- Ley N° 32185 Ley de Presupuesto del sector público para el año fiscal 2025
- Ley N° 32186 Ley de equilibrio financiero del presupuesto del sector público del año fiscal 2025.
- Ley N° 32187 Ley que aprueba el endeudamiento del sector público para el año fiscal 2025.
- Texto Único Ordenado de la Ley N° 30225 Ley de contrataciones del estado y sus modificatorias.
- Texto Único Ordenado de la Ley N° 27444 Ley del procedimiento administrativo general aprobado mediante decreto supremo N° 004-2019-JUS.
- Texto Único Ordenado de la Ley N° 27806 Ley de Transparencia y acceso a la información pública, aprobada mediante decreto supremo N° 043-2003-PCM.
- Ley N° 26842 Ley general de salud.
- Directivas del Organismo Supervisor de las Contrataciones del Estado.
- Opiniones del Organismo Supervisor de las Contrataciones del Estado.
- Pronunciamientos del Organismo Supervisor de las Contrataciones del Estado.
- Resoluciones del Tribunal de Contrataciones del Estado.
- Cualquier otra disposición legal vigente que permita desarrollar el objeto de la convocatoria, que no contravenga lo regulado por la Ley de Contrataciones del Estado.

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

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de 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.

2.2.2. Documentación de presentación facultativa:

- a) *Incorporar en la oferta los documentos que acreditan los "Factores de Evaluación" establecidos en el Capítulo IV de la presente sección de las bases, a efectos de obtener el puntaje previsto en dicho Capítulo para cada factor.*

Advertencia

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

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

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

Advertencia

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.

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

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación⁶ (Anexo N° 12).
- i) Detalle de los precios unitarios del precio ofertado⁷.
- j) Estructura de costos⁸.

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.*

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

⁶ 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 en mesa de partes de la Dirección de Redes Integradas de Salud Lima Norte, sito en la Calle A Mz. 02 Lt. 03 Asoc. Víctor Raúl Haya de la Torre - Distrito Independencia - Independencia - Lima.

Importante

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

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista FROMA MENSUAL, previa conformidad de la Coordinación de Comunicación, Redes y Soporte Informático de la Oficina de Tecnologías de la Información, quienes verificarán el cumplimiento del servicio de acuerdo a lo solicitado en los términos de referencia.

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

- Informe de conformidad del funcionario responsable de la Coordinación de Comunicación, Redes y Soporte Informático de la Oficina de Tecnologías de la Información, emitiendo la conformidad de la prestación efectuada.
- Comprobante de Pago Electrónico respectivo y expresado en soles.
- Acta de conformidad emitida por la Oficina de Gestión de tecnología de Información.

Dicha documentación se debe presentar en mesa de partes de la Dirección de Redes Integradas de Salud Lima Norte, sito en la Calle A Mz. 02 Lt. 03 Asoc. Víctor Raúl Haya de la Torre - Distrito Independencia - Independencia - Lima.

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

TÉRMINOS DE REFERENCIA DE CONTRATACIÓN DE SERVICIO DE TRANSMISION DE DATOS, INTERNET DEDICADO CON SEGURIDAD VIRTUAL Y TELEFONIA PARA LA SEDE CENTRAL Y LOS ESTABLECIMIENTOS DE SALUD DE LA JURISDICCIÓN DE LA DIRIS LIMA NORTE

1. DEPENDENCIA QUE REQUIERE EL SERVICIO

Oficina de Gestión de Tecnología de la Información

2. OBJETIVO DE LA CONTRATACIÓN

Realizar la contratación de una persona jurídica que brinde el TRANSMISION DE DATOS, SERVICIO DE INTERNET DEDICADO CON SEGURIDAD VIRTUAL, Y TELEFONIA para la Sede Central y establecimientos de salud, de conformidad a los términos de referencia del presente documento.

3. FINALIDAD PÚBLICA

Los servicios por contratar permitirán interconectar todas las sedes, brindar servicio de telefonía IP (SIP trunk) y tener acceso a internet con seguridad, a velocidades adecuadas para las distintas sedes administrativas, optimizando de esta manera los servicios informáticos en beneficio directo a los administrados y colaboradores de la institución.

4. REQUISITOS GENERALES PARA LOS SERVICIOS DE TRANSMISION

- a. Para los servicios de transmisión de datos e internet todos los servicios deben brindarse con enlaces de fibra óptica (última milla).
- b. Los servicios de transmisión de datos e internet debe brindarse sobre una Red MPLS, no se aceptarán Redes con tecnologías ADSL, GPON, HFC, FTTH o similares.
- c. Debe contar con DNS IPv4 e IPv6 redundantes. El contratista debe contar con DNS redundantes que permita el registro de dominios en IPv4 e IPv6.
- d. El servicio será brindado sobre una Red MPLS asegurando calidad de servicio.
- e. Deberá contar en su Red con una arquitectura de protección contra ataques DDoS la cual debe de estar implementada en el Centro de Datos del postor, además de cumplir con:
 - Estar alojada en la Red del Contratista
 - Estar conformada por equipos de propósito específica No Firewalls, No balanceadores, No UTM, No Gateways ni NGFW
 - Se brindará informe en caso de eventos de ataque. El informe sobre los eventos de ataque se podrá brindar como parte del Informe mensual del servicio.
 - Se debe mitigar ataques del tipo volumétrico para un máximo de 10Gbps.
- f. Tanto para la plataforma de Seguridad Perimetral para los EESS (Establecimientos de Salud) como de Telefonía solicitada debe brindar un alto nivel de disponibilidad (mayor al 99,95%), para lo cual éstas soluciones deberán de encontrarse implementada en la red del contratista y dentro de una infraestructura de Datacenter, la cual deberá contar con certificación en diseño

y/o construcción y/o sostenibilidad TIER 3 emitido por el UPTIME INSTITUTE como mínimo. El postor deberá presentar la documentación sustentatoria del datacenter que garantice el cumplimiento de este requisito en la firma del contrato.

5. DESCRIPCIÓN DEL REQUERIMIENTO

5.1. SERVICIO DE TRANSMISIÓN DE DATOS

- a) Se requiere un servicio de Transmisión de Datos para la Sede Principal y para los Establecimientos de Salud (EESS), según TABLA N°1 en Anexo N°1.
- b) El servicio debe brindarse con enlaces de fibra óptica (última milla).
- c) El servicio debe brindarse sobre una Red MPLS, no se aceptarán Redes con tecnologías ADSL, GPON, HFC, FTTH o similares.
- d) El servicio será brindado sobre una Red MPLS asegurando calidad de servicio
- e) Para la sede Principal se deberá implementar una cabecera de datos de un ancho de banda de 3 Gbps que se debe proporcionar mediante dos enlaces por medio de fibra óptica canalizada subterránea o aérea que provengan de dos nodos diferentes del Contratista. Los enlaces se comportarán como activo – pasivo.

Para la Sede Central el contratista deberá brindar dos (02) equipos routers configurados en alta disponibilidad. Las características mínimas de los router a proponer para la Sede Central son:

- Deben ser equipos de propósito específico (no firewalls, no Gateway no UTMs o similares)
 - Deben ser equipos nuevos y de primer uso, y no deberán tener anuncio de fin de venta o fin de soporte. Esto deberá acreditarse con una carta de fabricante en la etapa de presentación de oferta.
 - Contar con 16 interfaces LAN ethernet RJ45 10/100/1000, seis (06) puertos 10Gbps SFP+, memoria RAM de 1GB, memoria FLASH de 1GB
 - Tener como mínimo 1 puerto de consola RJ45, un puerto USB 2.0, doble fuente redundante.
 - Contar con un throughput mínimo de 3 Gbps simétrico 1:1 IMIX y deberá tener la capacidad de soportar un 100% de aumento de ancho de banda.
 - Deberán soportar como mínimo enrutamiento estático, dinámico (RIPv1,v2, OSPFv2, EIGRP, BGP, IS-IS, ruteo dinámico IPv6 (RIPng, OSPFv3, IS-ISv6, BGP4+), deberá soportar Multicast IGMPv1/v2/v3, PIM-DM, PIM-SM, MBGP, MSDP e IPv6 multicas: MLDv1/v2, PIM-DM, PIM-SM) y Netflow y/o sflow y/o Netstream sobre IPv4 y IPv6. Se da como opcional los siguientes protocolos: EIGRP,IS-IS,IS-ISv6,MSDP,MBGP,MLD v1 / v2,PIM-BIDIR,NetStream
- f) Para los Establecimientos de Salud (EESS) cada establecimiento será atendido con un enlace físico de fibra óptica como medio de acceso a la red. No se aceptará el uso de medios como cable de cobre o coaxial o radioenlaces. El tendido de fibra

óptica podrá ser canalizado subterráneo y/o aéreo. El ancho de banda por cada EESS distinta a la Sede Principal será de 40Mbps. La relación de sedes se indica en la Tabla N°1.

En caso que, por la ubicación de la Sede no se cuente con facilidades de cobertura por fibra óptica por parte del contratista, se permitirá hasta para un máximo de 10 sedes, la implementación del servicio por medios alternativos de baja latencia (no mayor a 80ms) como radioenlaces punto a punto, también se permitirá medios satelitales de acceso a internet de tecnología LEO (de órbita terrestre baja) en cuyo caso el contratista será responsable de suministrar e implementar lo necesario para la comunicación segura entre las sedes del proyecto.

Para cada uno de los EESS el contratista deberá brindar un (01) equipo router. Las características mínimas de los router a proponer para la Sede Central son:

- Deben ser equipos de propósito específico (no firewalls, no Gateway no UTMs o similares)
- Deben ser equipos nuevos y de primer uso, y no deberán tener anuncio de fin de venta o fin de soporte. Esto deberá acreditarse con una carta de fabricante en la etapa de presentación de oferta.
- Contar con 04 puertos LAN RJ45 10/100/1000 Ethernet y 1 puerto WAN SFP 10/100/1000 y 1 puerto WAN RJ45 10/100/1000 (no se aceptarán puertos combo), memoria RAM de 1GB, memoria FLASH de 256 MB
- Tener como mínimo 1 puerto de consola RJ45, un puerto USB 2.0 y una fuente interna o externa.
- Contar con un throughput mínimo de 100Mbps simétrico 1:1
- Los equipos deberán ser rackeable, no se aceptarán equipos instalados en bandejas
- Deberán soportar como mínimo enrutamiento estático, dinámico (RIPv1,v2, OSPFv2, EIGRP, BGP, IS-IS, ruteo dinámico IPv6 (RIPng, OSPFv3, IS-ISv6, BGP4+), deberá soportar Multicast IGMPv1/v2/v3, PIM-DM, PIM-SM, MBGP, MSDP e IPv6 multicas: MLDv1/v2, PIM-DM, PIM-SM) y Netflow y/o sflow y/o Netstream sobre IPv4 y IPv6
- Los equipos deberán poder ser rackeables, no se aceptarán equipos instalados en bandejas.
- Los routers deberá soportar como mínimo enrutamiento estático, dinámico (RIPv1,v2, OSPFv2, EIGRP, BGP, IS-IS, ruteo dinámico IPv6 (RIPng, OSPFv3, IS-ISv6, BGP4+), deberá soportar Multicast IGMPv1/v2/v3, PIM-DM, PIM-SM, MBGP, MSDP e IPv6 multicas: MLDv1/v2, PIM-DM, PIM-SM) y Netflow y/o sflow y/o Netstream sobre IPv4 y IPv6. Se da como opcional los siguientes protocolos: EIGRP,IS-IS,IS-ISv6,MSDP,MBGP,MLD v1 / v2,PIM-BIDIR,NetStream

- g) Se requiere Servicio de transmisión de datos entre los establecimientos de salud (EESS) y la sede principal de la Diris Lima Norte con porcentaje de disponibilidad de los enlaces de transmisión para cada EESS de 99.5% y para la Sede Central

de 99.95%. El prestador del servicio presentará un procedimiento para la atención a averías en la etapa de perfeccionamiento de contrato.

- h) El contratista deberá brindar una herramienta de monitoreo que permita visualizar estadísticas de estado de salud de los equipos para todos los enlaces (Establecimientos de salud y Sede Central). El acceso debe ser vía web http o https. La herramienta debe permitir acceder a un histórico de 6 meses como mínimo. Esta herramienta deberá encontrarse alojada en la red del contratista y deberá contar con un acceso para el personal de la entidad, esta herramienta deberá ser capaz de efectuar descubrimiento de los equipos propuestos a través de descubrimiento de red, programado y de capa 2. Así mismo deberá permitir el monitoreo de disponibilidad de los routers entregados por el contratista, monitoreo de interfaces, monitoreo SNMP, monitoreo de syslog (activarse solo para casos de pruebas y/o Troubleshooting), estadísticas de estado de salud del equipo como memoria, temperatura, cpu, disponibilidad,

El contratista deberá crear un dashboard personalizado con los "widgets" que tenga disponible la herramienta para realizar un monitoreo global. La herramienta debe brindar alertas de estado de equipos, interfaces y enviar notificaciones por medio de correo, SMS (opcional la implementación, pero la herramienta debe soportarla) y debe generar informes y/o reportes programados y deberá permitir la automatización de ciertas tareas, flujos de trabajo que faciliten las acciones cuando ocurre una incidencia, como supresión de alarma, generar una alarma, agregar una nota a la alarma, hacer un ping y trace route. Así mismo esta herramienta deberá poder monitorear el ancho de banda de las interfaces WAN de cada centro de salud y sede principal y mostrar las conversaciones, top de IPs y top de aplicaciones como mínimo, permitiendo generar alarmas si el ancho de banda pasa ciertos umbrales preconfigurados.

- i) El contratista deberá efectuar test de velocidad a solicitud de la entidad de manera automatizada en una frecuencia que podrá ser diario, semanal o mensual, hacia los routers de cada sede ya sea a través de la herramienta de monitoreo o de forma independiente mediante otra aplicación o herramienta, permitiendo visualizar los test ejecutados en la herramienta de monitoreo.
- j) Por cada año se debe considerar 08 traslados de gabinete dentro de la jurisdicción de la DIRIS LIMA NORTE Este sin costo alguno.

5.2. - ACCESO DEDICADO A INTERNET PARA LA SEDE CENTRAL CON SEGURIDAD GESTIONADA

- a) El servicio de Acceso a Internet para la Sede Central deberá contar con las siguientes características

N°	Tipo	Ancho de Banda	Medio de Transmisión
----	------	----------------	----------------------

1	Enlace de internet Principal	300Mbps	Fibra óptica
2	Enlace de internet de Contingencia	300Mbps	Fibra óptica

- b) El contratista deberá implementar un servicio de Internet de 300Mbps de ancho de banda en configuración de alta disponibilidad para lo cual implementará dos enlaces por fibra óptica en configuración activo- pasivo.
- c) El enlace de contingencia deberá implementarse por una ruta distinta, así como deberá atenderse de un nodo diferente de la red del contratista, diferente al enlace Principal para asegurar una disponibilidad de servicio de 99.97%. Para la firma del contrato se adjuntará el plano o esquema con el detalle de las dos rutas a implementar.
- d) El CONTRATISTA deberá proporcionar un pool de 16 IPs públicas IPv4, dentro de las cuales se considera la IP de red, la IP de broadcast y la IP para el Gateway.
- e) El medio de acceso deberá ser de fibra óptica al 100% desde los nodos de atención hasta el Datacenter de la Entidad, donde se alojarán los equipos en el local de la entidad.
- f) El servicio de Internet ofrecido por el POSTOR deberá contar con varios niveles de contingencia tanto en su backbone local, así como también en la salida internacional de ingreso al Backbone de Internet. El contratista deberá contar como mínimo con 2 Proveedores TIER 1 para su salida a Internet. Se adjuntará a la propuesta una topología con los dos proveedores y sus capacidades.
- g) El contratista deberá contar con conexión directa y propia al "NAP Perú", con una capacidad mínima de 2x100Gbps, para lo cual el postor deberá presentar una carta para la etapa de firma del contrato que lo demuestre
- h) Para la Sede Central el contratista deberá brindar dos (02) equipos routers configurados en alta disponibilidad. Las características mínimas de los router a proponer para la Sede Central son:
- Deben ser equipos de propósito específico (no firewalls, no Gateway no UTMs o similares)
 - Deben ser equipos nuevos y de primer uso, y no deberán tener anuncio de fin de venta o fin de soporte. Esto deberá acreditarse con una carta de fabricante en la etapa de presentación de oferta.
 - Contar con 16 interfaces LAN ethernet RJ45 10/100/1000, seis (06) puertos 10Gbps SFP+, memoria RAM de 1GB, memoria FLASH de 1GB.
 - Tener como mínimo 1 puerto de consola RJ45, un puerto USB 2.0, doble fuente redundante.
 - Contar con un throughput mínimo de 1 Gbps simétrico 1:1 IMIX y deberá tener la capacidad de soportar un 100% de aumento de ancho de banda.
 - Deberán soportar como mínimo enrutamiento estático, dinámico (RIPv1,v2, OSPFv2, EIGRP, BGP, IS-IS, ruteo dinámico IPv6 (RIPng, OSPFv3, IS-ISv6, BGP4+), deberá soportar Multicast IGMPv1/v2/v3, PIM-DM, PIM-SM, MBGP, MSDP e IPv6 multicas: MLDv1/v2, PIM-DM, PIM-SM) y Netflow y/o sflow y/o Netstream sobre IPv4 y IPv6.

- i) El contratista deberá brindar el servicio de internet sobre equipos diferentes a los utilizados para el servicio de transmisión de datos a fin de mantener los servicios diferenciados y segmentar la red adecuadamente.
- j) El contratista deberá comprometerse a realizar la instalación, configuración y pruebas hasta dejar operativos los servicios y equipos ofrecidos de acuerdo a las condiciones y disposiciones contenidas en las presentes bases.
- k) El CONTRATISTA debe poseer NOC Local y Propio para garantizar la gestión del servicio de Internet, el mismo que será acreditado con documentación que acredite poseer el NOC Local para la presentación de ofertas
- l) El contratista deberá contar al menos para un segundo nivel de atención con un SOC local con estándares avanzados de procesos, tecnología, personal, gestión y mejora continua en ciberseguridad, lo cual permitirá garantizar una adecuada gestión del servicio de seguridad. Para acreditarlo el Postor deberá presentar para la presentación de ofertas un certificado vigente emitido por una entidad reconocida que acredite que el Centro de Operaciones de Seguridad (SOC) ha alcanzado un nivel de madurez de al menos 2.2 según el modelo de referencia SOC- CMM (Security Operations Center – Capability Maturity Model).
- m) El servicio deberá contar con un sistema de DNS redundantes.
- n) El contratista deberá contar con el servicio de DNS (Sistema de Nombres de Dominio) de manera auto gestionable, teniendo la entidad el acceso a un entorno web (con usuario y clave) que permitirá la capacidad de crear, actualizar registrar, modificar y eliminar las configuraciones de sus registros DNS, sin la necesidad de asistencia técnica del equipo de soporte. (No se requerirá la instalación de equipos adicionales). En caso de no poseer un sistema para la gestión automática deberá tener un sistema de solicitudes vía correo electrónico con un tiempo de respuesta de 30 minutos
- o) El postor debe contar con un sistema de monitoreo vía web que permita visualizar el tráfico del enlace que se contrate, este sistema de monitoreo debe ser accesible para LA ENTIDAD sin que esto represente costo adicional. La ENTIDAD podrá monitorear el tráfico en línea de forma permanente en ambos sentidos para lo cual el contratista brindará un usuario y contraseña. El tiempo de información histórica disponible en la herramienta de monitoreo será de los últimos 3 meses como mínimo.
- p) El contratista debe contar con una línea para el servicio de atención al cliente y soporte técnico 24x7. La línea es exclusiva para clientes corporativos y el horario es de lunes a domingo las 24 horas del día.
- q) El contratista debe contar con un centro de soporte y servicio de Postventa propio y especializado para el segmento corporativo.
- r) El contratista debe implementar lo solicitado en el presente proceso, en coordinación con la entidad.
- s) El contratista tiene la obligación de ejecutar los servicios de acuerdo a lo establecido en los términos de referencia, teniendo responsabilidad total sobre la instalación, implementación, pruebas y puesta en marcha de los servicios contratados.

- t) El contratista asumirá todos los gastos de transporte del contratista hacia la Entidad necesarios para instalación de los equipos, así como de los materiales y demás componentes necesarios para la instalación, implementación, pruebas y puesta en marcha de los servicios.
- u) No se aceptarán enlaces o conexiones con medio de transmisiones inalámbricas, microondas o satelitales.
- v) Todas las infraestructuras de fibra óptica deberán de instalarse con materiales nuevos, no se aceptará reutilizar infraestructura existente, esto para asegurarse que se no se brindará el servicio con materiales con posible daño físico o deteriorado, esto será verificado al finalizar la implementación al momento de brindar la conformidad.

5.2.1. SEGURIDAD GESTIONADA PARA LA SEDE CENTRAL

Los Servicios de Seguridad solicitados para la Sede Central serán tres:

- Seguridad Perimetral
- Protección AntiDDoS
- Protección Antimalware (EDR)

5.2.1.1 Seguridad Perimetral

El Contratista durante el período del servicio deberá proporcionar e implementar en la Sede de la Entidad una solución de seguridad perimetral que incluirá la instalación de dos equipos en formato appliance físicos NGFW.

El equipamiento proporcionado podrá ser nuevo, no deberán encontrarse en situación de fin de venta o fin de soporte al momento de la presentación de propuestas, así mismo el Contratista es responsable de mantener el licenciamiento activo de los equipos durante el período del servicio.

Los equipos de seguridad gestionada en formato appliance físicos NGFW deberán tener una ADMINISTRACIÓN COMPARTIDA con usuarios ADMINISTRADOR por parte del CONTRATISTA y de la ENTIDAD DIRIS LIMA NORTE, en casos de: creación de reglas, publicación de servicios, filtros de seguridad, entre otros. Hasta el término del contrato.

Los equipos y/o solución propuesta deben incluir las siguientes características y capacidades como mínimo:

a) Características Generales:

- La solución debe consistir en una plataforma de protección de Red, basada en dispositivos con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.
- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.
- Las funcionalidades de protección de red que conforman la plataforma de seguridad, pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;

- La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;
- Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19", incluyendo un rail kit (si sea necesario) y los cables de alimentación;
- La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;
- Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
- Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
- Los dispositivos de protección de red deben soportar Policy based routing o policy based forwarding;
- Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
- Los dispositivos de protección de red deben soportar DHCP Relay y DHCP Server
- Los dispositivos de protección de red deben soportar sFlow;
- Los dispositivos de protección de red deben soportar Jumbo Frames;
- Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
- Debe ser compatible con NAT dinámica (varios-a-1);
- Debe ser compatible con NAT dinámica (muchos-a-muchos);
- Debe soportar NAT estática (1-a-1);
- Debe admitir NAT estática (muchos-a-muchos);
- Debe ser compatible con NAT estático bidireccional 1-a-1;
- Debe ser compatible con la traducción de puertos (PAT);
- Debe ser compatible con NAT Origen;
- Debe ser compatible con NAT de destino;
- Debe soportar NAT de origen y NAT de destino de forma simultánea;
- Debe soportar NAT de origen y NAT de destino en la misma política
- Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
- Debe ser compatible con NAT64 y NAT46;
- Debe implementar el protocolo ECMP;
- La solución debe incluir capacidades de SD-WAN durante la vigencia del contrato.
- Las capacidades de SD-WAN de la solución deben permitir monitorear el tráfico de aplicaciones desde un servicio en nube del fabricante.
- Debe soportar el balanceo de enlace por hash de IP de origen y destino;

- Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;
- Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;
- Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;
- Enviar logs a sistemas de gestión externos simultáneamente;
- Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
- Debe soportar protección contra la suplantación de identidad (anti-spoofing);
- Implementar la optimización del tráfico entre dos dispositivos;
- Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
- Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
- Soportar OSPF graceful restart
- Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
- Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
- Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
- Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
- Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
- Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
- Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
- La configuración de alta disponibilidad debe sincronizar: Sesiones, asociaciones de seguridad VPN y ablas FIB;
- La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
- En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
- Debe soportar la creación de sistemas virtuales en el mismo equipo;
- La consola de administración debe soportar como mínimo, ingles, español y Portugues.
- La solución debe incluir la capacidad de detectar al menos los siguientes valores dentro del tráfico analizado: nombre del host y sistema operativo.



- La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas

b) Características de Rendimiento :

- Soportar al menos 3.4 Gbps de throughput de NGFW, medido en Enterprise Mix.
- Soportar al menos 4.9 Gbps de throughput de IPS, medido en Enterprise Mix.
- Soportar al menos 2.9 Gbps de throughput de Threat Protection, medido en Enterprise Mix.
- Soporte a por lo menos 2.9 millones conexiones simultáneas TCP o conexiones concurrentes.
- Soporte a por lo menos 270 000 nuevas conexiones por segundo TCP
- Throughput de al menos 12 Gbps de VPN IPSec, medido con paquetes de 512 bytes
- Estar licenciado para, o soportar sin necesidad de licencia, 1900 túneles de VPN IPSec site-to-site simultáneos o Gateway to Gateway.
- Estar licenciado para, o soportar sin necesidad de licencia, 15000 túneles de clientes VPN IPSec simultáneos
- Throughput de al menos 1.9 Gbps de VPN SSL
- Soportar al menos 500 clientes de VPN SSL simultáneos
- Soportar al menos 3.9 Gbps de throughput de Inspección SSL, medido con conexiones HTTPS
- Soportar al menos 12 Gbps de throughput de Application Control, medido en HTTP 64 KB
- Tener al menos 16 interfaces 1 Gbps RJ45, las cuales serán utilizadas exclusivamente para tráfico de red
- Tener al menos 8 slots de 1Gbps SFP, las cuales serán utilizadas exclusivamente para tráfico de red
- Tener al menos 2 slots de 10Gbps SFP+, las cuales serán utilizadas exclusivamente para tráfico de red
- Tener al menos 1 interfaz dedicada para gestión
- Tener al menos 1 interfaz dedicada para HA
- Tener al menos 1 puerto de consola
- Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) o dominios virtuales por appliance

c) Control por Políticas de Firewall :

- Debe soportar controles de zona de seguridad;
- Debe contar con políticas de control por puerto y protocolo;

- Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
- Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
- Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
- Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- Debe soportar el protocolo estándar de la industria VXLAN;
- La solución debe permitir la implementación sin asistencia de SD-WAN
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
- La solución debe soportar la integración nativa con una solución de sandboxing.

d) Control de Aplicación :

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
- Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
- Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
- Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;
- Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;
- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
- Actualización de la base de firmas de la aplicación de forma automática;
- Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos
- Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
- Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;

- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video;
- Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones, nivel de riesgo de la aplicación y categoría de aplicación.
- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

e) Prevención de Amenazas :

- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
- Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
- Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
- Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
- Debe soportar granularidad en las políticas de IPS, Antivirus y Anti- Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;
- Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
- Debe incluir la protección contra ataques de denegación de servicio;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, análisis para detectar anomalías de protocolo, desfragmentación IP, reensamblado de paquetes TCP y bloqueo de paquetes con formato incorrecto (malformed packets);
- Debe ser capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.;
- Detectar y bloquear los escaneos de puertos de origen;
- Bloquear ataques realizados por gusanos (worms) conocidos
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
- Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- Identificar y bloquear la comunicación con redes de bots;

- Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;
- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
- La capacidad de filtro de DNS debe ser alimentada por un servicio de inteligencia de amenazas de la propia marca.
- Debe permitir la translación en el firewall de una consulta de DNS, a fin de redirigir la resolución hacia otro destino diferente del original.
- Los eventos deben identificar el país que origino la amenaza;
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
- Debe incluir la protección contra ataques de día cero a través de una estrecha integración con análisis Sandbox en nube

f) Filtrado de URL :

- Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);
- Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;
- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;
- Tener por lo menos 75 categorías de URL;
- Debe tener la funcionalidad de exclusión de URLs por categoría; Permitir página de bloqueo personalizada;
- Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio)

g) Identificación de Usuarios :

- Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con
- los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
- Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios;
- Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;
- Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios;
- Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios;
- Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autenticación residente en el equipo de seguridad (portal cautivo);
- Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
- Debe incluir al menos dos tokens dentro del servicio, permitiendo la autenticación de dos factores para los usuarios administradores del firewall;

h) QoS Traffic Shaping :

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o
- denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda
- máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen, dirección de destino, por usuario y grupo.

- Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado, con máximo ancho de banda y colas de prioridad.
- Soportar marcación de paquetes DiffServ, incluso por aplicación;
- Soportar la modificación de los valores de DSCP para Diffserv;
- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
- Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes

i) Filtro de Datos :

- Permite la creación de filtros para archivos y datos predefinidos;
- Los archivos deben ser identificados por tamaño y tipo;
- Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;
- Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
- Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
- Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares

j) Gestión Centralizada :

- El contratista deberá realizar la implementación de una plataforma de gestión centralizada, reportes, monitoreo y centralización de logs.
- La plataforma de gestión (consola), podrá ser entregada en formato Appliance o virtual o en la nube del Contratista.
- El Contratista deberá garantizar que los eventos y/o logs sean almacenados por un periodo de 30 días.

5.2.1.2 Protección AntiDDoS

El Contratista deberá proporcionar un servicio que permita a la Entidad resistir ataques de denegación de servicio (DDoS), protegiendo a la Entidad de situaciones donde su dirección IP de sus servidores críticos reciben con intenciones maliciosas y de manera coordinada, información masiva de todo el mundo con el propósito de sobrecargar y hacer caer los servidores y servicios de la DIRIS LIMA NORTE. El servicio deberá cumplir con las siguientes especificaciones:

- a) Se solicita una solución de AntiDDoS con un alto nivel de disponibilidad (mayor al 99,97%), para lo cual esta solución deberá encontrarse implementada en la

red del contratista y dentro de una infraestructura de Datacenter, el cual deberá contar con certificación en diseño y/o construcción y/o sostenibilidad TIER 3 emitido por el UPTIME INSTITUTE como mínimo. El postor deberá presentar la documentación sustentatoria del datacenter que garantice el cumplimiento de este requisito en la firma del contrato.

- b) Protección ataques volumétricos para los servicios expuestos en el internet.
- c) Detección integral de amenazas, la solución deberá aprender continuamente y adaptarse en tiempo real, alertando a los operadores de ataques, así como de cambios inusuales en la demanda.
- d) Mitigación eficaz con capacidad de identificar y bloquear el tráfico de ataques volumétricos y, al mismo tiempo, permitir que el tráfico que no es de ataques volumétricos fluya hacia su destino previsto.
- e) La solución de limpieza de tráfico Anti-DDoS deberá ser un servicio de seguridad de red que defiende las direcciones IP contra ataques de denegación de servicio distribuido (DDoS) del tipo Volumétrico, hasta una capacidad de 10 Gbps.
- f) La solución Anti-DDoS deberá monitorear el tráfico dirigido a direcciones IP específicas en tiempo real y deberá detectar el tráfico de acceso en los puntos de salida de la red para identificar cualquier ataque DDoS del tipo volumétrico lo antes posible. A continuación, deberá limpiar el tráfico anormal según las políticas de defensa configuradas por la DIRIS LIMA NORTE sin afectar los servicios normales.
- g) Eliminar automáticamente solo el tráfico de ataque sin interrumpir el flujo de no ataque al tráfico comercial.
- h) Brindar una lista completa de contramedidas de ataques protegiendo su infraestructura de los más grandes ataques volumétrico.
- i) Detección integral de amenazas, nuestra solución aprende continuamente y se adapta en tiempo real, alertando, así como de cambios inusuales en la demanda.
- j) Mitigación eficaz con capacidad de identificar y bloquear el tráfico de ataque y, al mismo tiempo, permitir que el tráfico que no es de ataque fluya hacia su destino previsto.
- k) Aislar y eliminar el tráfico de ataque sin afectar a otros usuarios, en tan solo unos segundos.
- l) Permitir Bloquear hosts maliciosos conocidos utilizando listas blancas y negras. La lista blanca contiene hosts autorizados, mientras que la lista negra contiene zombies o comprometidos hosts cuyo tráfico será bloqueado.
- m) Mitigación basada en la ubicación de IP, filtrado basado en anomalías de protocolo, eliminación de paquetes y limitación de velocidad (para gestionar de forma adecuada los picos de demanda no maliciosos).
- n) El fabricante de la solución ofertada por el postor deberá encontrarse en el Top 8 Distributed Denial of Service (DDoS) Protection Tools de PeerSport o Líder en el Forrester Wave 2021 y/o 2022 DDoS Mitigations Solutions. El postor adjudicado deberá adjuntar una carta del fabricante confirmándolo para la firma del contrato.
- o) Proteger los servicios DNS críticos por envenenamiento de caché, agotamiento de recursos y ataques de amplificación. Agregue mayor visibilidad a Servicios de DNS.
- p) Almacenar información para reportes de gestión y entrega de visibilidad sobre los ataques.
- q) El contratista del servicio brindará reportes mensuales dentro de los 10 primeros días calendarios del siguiente mes sobre el servicio de protección de DDoS

5.2.1.3 Protección Anti Malware (EDR)

Generalidades

- a) Se requiere que el Contratista proporcione una solución de seguridad antimalware tipo EDR basada en gestión y despliegue a través de servicios de nube (SaaS) del propio fabricante, en modalidad de suscripción.

- b) Debe estar licenciada para 30 dispositivos servidores por un periodo de VEINTICUATRO(24) meses. La Entidad será responsable de que los servidores cumplan con los requisitos de licenciamiento que sean necesarios.
- c) Deben de brindar una capacitación de la solución ofertada de 2 horas.
- d) Debe soportar los siguientes sistemas operativos:
 - Windows 7 SP1, Windows 8.1, Windows 10 y Windows 11.
 - Windows Server: 2008R2, 2012, 2012R2, 2016, 2019 y 2022.
 - Mac OS (Sonoma 14, Ventura 13, Monterey 12, BigSur 11 y Catalina 10).
 - Distribuciones Linux (Ubuntu, Debian, RHEL, CentOS, OpenSUSE, SLES y Oracle Linux).
- e) La solución debe incluir como mínimo las siguientes funcionalidades:
 - Firewall (Endpoint Firewall).
 - Control de Aplicaciones (Application Control).
 - Cumplimiento (Endpoint Compliance)
 - Anti-Virus
 - Anti-Ransomware
 - Anti-Bot (Protección contra máquinas infectadas de malware)
 - Anti-Exploit
 - Protección de Puertos (Port Protection)
 - Filtrado de Acceso a Internet (URL Filtering)
 - Protección contra Phishing de Día-Cero
 - Protección de contraseñas corporativas.
 - Análisis Forense
 - Emulación de Amenazas de Día-Cero (Sandboxing)
 - Extracción de Amenazas (Threat Extraction)
 - Mapa de Captura de Amenazas (Threat Hunting) basado en MITRE ATT&CK.
- f) La instalación de las licencias será realizada por personal de la Entidad para lo cual el contratista proporcionará una guía de instalación y configuración, adicionalmente El Contratista realizará una implementación típica en un uno de los "end points" que la Entidad indique para validar la guía entregada.

Firewall

- a) Debe proporcionar la capacidad de implementar políticas de firewall sobre el Endpoint y gestionarlo de forma centralizada, controlando tráfico entrante, saliente y los servicios asociados, y registrando los eventos sobre cada regla implementada
- b) Debe permitir la creación de zonas de seguridad (redes confiables) a través de diferentes objetos como: hosts, rango de direcciones IP, redes, grupos de redes y dominio, con diferentes permisos controlando accesos no autorizados.
- c) Capacidad de permitir o no en los equipos de usuario final, conectarse a redes Wireless cuando se encuentra conectado a redes LAN.
- d) Debe controlar si los usuarios pueden conectarse a su red desde puntos de acceso en lugares públicos, como hoteles o aeropuertos.

Control de aplicaciones

- a) Debe permitir el control de aplicaciones por política (grupos de equipos) o de forma global.
- b) El control de aplicaciones debe restringir el acceso a la red de aplicaciones específicas, para lo cual el administrador podrá definir políticas y reglas con acciones de: permitir, bloquear y finalizar las aplicaciones y procesos. También se debe poder configurar, que una aplicación finalice cuando intente acceder a la red, o evitar que una aplicación se inicie al intentar ejecutarla.

- c) Debe permitir configurar reglas detalladas para programas de software, y tomar acción como permitir o bloquear versiones específicas de un mismo software. Cada versión de aplicación debe ser identificado con un hash único y entidad firma (certificado).
- d) Debe tener capacidad de realizar un inventario detallado de las aplicaciones pre-existentes en los equipos de usuario final y sobre la base de dicho inventario, realizar políticas y reglas de control.
- e) Los usuarios administradores deben tener la opción de terminar un proceso potencialmente peligroso.
- f) La solución debe permitir personalizar listas negras y blancas de aplicaciones.

Cumplimiento

- a) Debe poder establecer una política de cumplimiento en las estaciones de usuario final, sobre la base de diversos controles de cumplimiento que deben ser verificados en los equipos.
- b) Las acciones de cumplimiento por cada política infringida (no cumplimiento) deberá ser: observar (solo registra actividad), alertar y restringir (en ambos casos notifica y permite acciones de remediación).
- c) Las etapas de cumplimiento deberán ser como mínimo: en cumplimiento, próximo a ser restringido y restringido.
- d) A través de las políticas de cumplimiento se debe poder restringir al equipo, si se encuentra que la política no está siendo cumplida.
- e) Los controles de cumplimiento deben ser personalizables por grupos de equipos, que permita identificar si las aplicaciones, los archivos, las claves de registro y los nombres de procesos específicos que se definan, deben o no ser permitidos en las estaciones de trabajo.
- f) En el caso de claves de registro de Windows, debe validar si la llave (key) y el valor (value) están presentes o no. Para el caso de los archivos, debe validar si el archivo existe, si el archivo no existe, si el archivo no se está ejecutando y si el archivo se está ejecutando.
- g) Adicionalmente, para la validación de archivo o aplicaciones como parte de la política de cumplimiento, debe validar la versión y el hash MD5 correspondiente.
- h) Se puede configurar para que la política cumpla con todas las variables de cumplimiento para ser dado como válido, o solo una de las variables requeridas.
- i) Las reglas de cumplimiento pueden evitar que los usuarios accedan a los recursos de red requeridos cuando no cumplen con las políticas.
- j) El control de remediación debe ser personalizables por cada control de cumplimiento, es decir cada control de cumplimiento puede tener asociado una acción de remediación. Las acciones de remediación deben poder ejecutar un programa o script en particular que puede ser descargado de una ruta URL específica, y tener la capacidad de ejecutar la remediación empleando los permisos de cuenta del sistema local o la del usuario.
- k) Los mensajes de alerta de incumplimiento deben ser personalizables por cada control de cumplimiento, es decir cada control de cumplimiento puede tener asociado un mensaje de alerta.
- l) Debe validar también controles tales como, service pack en sistema operativo, Anti-Virus/Anti-Malware tanto propias como de terceros instalados y actualizadas.
- m) Debe validar que todos los componentes de la solución de seguridad asignados al usuario y/o equipo final, están instalados y en ejecución en el Endpoint

Anti-virus

- a) Debe trabajar con base de firmas de archivos, para prevenir toda clase de malware, gusanos, troyanos, adware, capturado de teclado (keystroke loggers).
- b) Anti-Malware debe proteger contra malware dentro de archivos comprimidos tales como: ZIP, Z, ISO, 7Z, RAR, JAR, TAR y CAB.
- c) Debe proporcionar una manera de informar a los usuarios finales con alertas o informes de análisis locales relacionados con la actividad del Antimalware.
- d) Debe permitir las siguientes opciones de tratamiento de sobre antivirus o antispyware; reparación, cuarentena y eliminado.
- e) Debe tener capacidad de utilizar métodos de detección de comportamiento para proteger las computadoras de nuevas amenazas cuya información aún no se agregó a las bases de datos.
- f) Debe tener capacidad de usar tecnologías en la nube del propio fabricante, para mejorar la precisión de las funciones de escaneo y monitoreo.
- g) Debe evitar el acceso a sitios sospechosos y la ejecución de scripts maliciosos y ejecutables empaquetados transferidos a través de Web HTTP y alertar a los usuarios si se encuentra contenido malicioso.
- h) Debe tener capacidad de análisis de los mensajes de correo electrónico cuando pasan como archivos a través del sistema de archivos de Sistema Operativo.
- i) Debe tener capacidad desde la consola de enviar operaciones hacia los agentes, tales como: escanear malware, actualizar la base de datos de malware, restaurar archivo de cuarentena.

Anti-ransomware

- a) Debe tener protección específica contra malware del tipo ransomware que posea detección automática, bloqueo y eliminación de este tipo de amenazas.
- b) Debe tener capacidad de monitorear actividad de los archivos y la red, sobre comportamiento sospechosos. Debe detener el ataque inmediatamente cuando detecta que el ransomware modifica los archivos.
- c) Debe poseer la capacidad de restaurar archivos que fueron cifrados por el ransomware, como parte de la recuperación automática (remediación).
- d) Debe ser posible definir un límite de espacio para el resguardo de los archivos.
- e) Debe proteger contra ataques de Ransomware basado en el uso de herramientas de cifrado de volumen en bloque (tales como BitLocker y herramientas similares).
- f) Debe tener capacidad de protección de ransomware en carpetas compartidas en la red. Todas las carpetas compartidas están protegidas, independientemente del protocolo.
- g) Debe analizar el correo electrónico (a través de un complemento de Microsoft Outlook o similar) para incluir los detalles en el informe forense en caso de un ataque malicioso de ransomware a través de un correo electrónico.

Protección contra máquinas infectadas de malware

- a) Debe identificar las direcciones de C&C utilizadas por los delincuentes para controlar los bots.
- b) Debe bloquear la comunicación del bot hacia sitios de C&C; para asegurar de que no se robe ni se envíe información confidencial fuera de la organización.
- c) Debe utilizar el repositorio de amenazas en la nube del propio fabricante, para recibir actualizaciones y consultar el repositorio para clasificar los recursos de IP, URL y DNS no identificados.

Prevención contra exploits

- a) Debe detectar ataques desconocidos y de día cero, y brindar protección a los procesos vulnerables contra la explotación. Los archivos de la computadora se

envían a un área de prueba local, para la emulación y poder detectar archivos y contenido maliciosos.

- b) Identificar manipulaciones sospechosas de memoria en tiempo de ejecución. Al detectarse, el Anti-Exploit deberá terminar todos los procesos de Exploit, corregir la cadena de ataque completamente y desencadenar una Informe forense.

Protección de puertos

- a) Controla en base a políticas, el acceso del dispositivo a todos los puertos disponibles (USB, Bluetooth, entre otros)
- b) Las políticas definen los derechos de acceso para cada tipo de dispositivo de almacenamiento extraíble y los puertos a los que se pueden conectar. La política también evita que los usuarios conecten dispositivos no autorizados a las computadoras.
- c) Debe controlar (permitir o bloquear) la entrada y salida en todos los puertos de conexión, específicamente:
- Medios de almacenamiento USB, unidades CD/DVD, tarjetas SD y discos externos.
 - Dispositivos de audio y video a través de USB y Firewire
 - Dispositivos tales como teclados, adaptadores de red, modem, mouse y lectores de tarjetas (Smart Card Readers).
- d) Debe poder crear listas blancas (permitido) para control de medios
- e) Debe poder gestionar medios extraíbles por su número de serie, tipo de conexión, Device ID (device category class), lo que permite la creación de políticas para dispositivos únicos y específicos.

Url filtering

- a) Debe tener capacidad controlar la navegación en Internet a las que acceden los usuarios a través de los navegadores de internet.
- b) Debe contar con por lo menos 70 categorías de URL Filtering, con capacidad de protección de categorías de riesgo tales como: Anonymizer, botnets, phishing, spam, spyware, sitios maliciosos, sitios inactivos y sitios de alto riesgo.
- c) Debe tener la capacidad de crear listas negras (denegar) sobre sitios, dominios y direcciones IP específicas de Internet.
- d) Debe tener la capacidad de permitir al usuario acceder al sitio restringido (configurable por política).
- e) Debe analizar todas las descargas de archivos sobre canal HTTP, HTTPS y ser integrado con los navegadores MS Edge, Firefox, Google Chrome y Brave. Los archivos en descarga se deben enviar a una Sandbox para su emulación y detectar ataques evasivos de día cero.
- f) El tamaño de los archivos a ser emulados y los entornos de emulación, deberán ser configurables por política.
- g) La protección de navegación debe ser posible aun si el usuario emplea el modo incognito o private-mode en el navegador.
- h) Debe tener capacidad de realizar búsqueda segura, identificando los resultados de la búsqueda basada en reputación de la URL. Debe soportar al menos los motores de búsqueda Google, Bing y Yahoo.
- i) Debe tener capacidad de personalizar el mensaje de la pantalla de bloqueo.

Protección contra phishing de día-cero

- a) Debe contar con capacidad de prevención de Phishing de día cero, debe tener la capacidad de detectar y prevenir. Si se determina que el sitio es un sitio de phishing, los usuarios no pueden acceder al sitio.
- b) La prevención debe verificar diferentes características de un sitio web para asegurarse de que un sitio no pretenda ser un sitio diferente y use información personal de manera maliciosa.

- c) Debe poner analizar phishing de día-cero en archivo HTML locales en el computador, que son abiertos en navegadores basados en Chromium (Edge, Chrome y Brave).
- d) Debe ser compatible con los navegadores actuales de Edge, Firefox, Chrome y Brave.
- e) Debe poder configurar la página de bloqueo que advierte al usuario final que es un sitio de phishing y, por lo tanto, no puede proporcionar credenciales allí.

. Protección de contraseñas corporativas

- a) Debe proteger las credenciales (contraseña) corporativas, debe tener la capacidad de detectar y prevenir.
- b) Debe alertar y prevenir a los usuarios para que no utilicen su contraseña corporativa en dominios no corporativos. (Ej. Redes sociales). La capacidad de prevención impide que el usuario ingrese la contraseña corporativa y abre la página de bloqueo en una nueva pestaña.
- c) Se debe poder configurar que dominios internos y/o corporativos debe ser protegidos por esta protección de reutilización de contraseñas.
- d) Debe ser compatible con los navegadores actuales de Edge, Firefox, Chrome y Brave.

Análisis forense

- a) Debe construir automáticamente informes forenses, entregando visibilidad completa del alcance, daño o severidad y vectores del ataque, incluyendo:
- b) Actividades sospechosas (conexiones y procesos relacionados al ataque).
- c) Actividades de Remediación (procesos terminados, archivos en cuarentena o eliminados, archivos restaurados en el caso de Ransomware)
- d) Impacto al negocio del incidente, como archivo exfiltrados o cifrados por ransomware.
- e) Detalle de la línea de tiempo del Incidente para determinar si es una infección.
- f) Debe mostrar un reporte forense detallado, que incluya el mapa o matriz del Framework MITRE ATT&CK, el cual mostrara las tácticas y técnicas de compromiso que fueron ejecutadas por el atacante.
- g) Debe mostrar los elementos maliciosos que fueron remediados (cuarentena).
- h) Debe indicar el punto de entrada del ataque (ej. Navegador, puerto USB, red interna, etc.)
- i) Debe tener capacidad desde la consola de enviar operaciones hacia los agentes, tales como: analizar en base a un IoC, remediar en base a un archivo y aislar el equipo.

Emulación de amenazas de día-cero

- a) Debe tener capacidad de detección y prevención de malware no conocido. Para ello, el software deberá realizar la emulación del malware en la nube del propio fabricante, en donde se analiza y detecta amenazas no conocidas o de día cero.
- b) Debe proteger contra los ataques de múltiples vectores de amenazas que llegan a través de descargas de la web, contenido copiado de medios de almacenamientos extraíbles, enlaces o archivos adjuntos en mensajes de correo electrónico, movimiento lateral de datos y malware entre segmentos de red e infecciones a través de contenido cifrado.
- c) Debe permitir combinación de capacidades avanzadas de machine learning, análisis de comportamiento dinámico de Sistema Operativo, identificación de

comportamientos maliciosos y sospechosos, tácticas de hacking y técnicas de ingeniería social, análisis de comunicaciones de C&C durante el análisis de Sandboxing

- d) El Sandboxing debe soportar al menos 60 tipos de archivos, incluyendo: Adobe PDF, Microsoft Word, Excel, PowerPoint (incluido plantillas), ejecutables (EXE, COM, SCR, SWF, BAT, DLL, MSI) y comprimidos (Zip, 7z, Tar, Tgz).
- e) Debe ser posible realizar emulación a nivel sistema operativo y a nivel CPU.
- f) Debe ser posible analizar las amenazas evitando las técnicas de evasión como VM Detection, Time Delays, Interacción Humana, etc.
- g) Debe utilizar Machine Learning, análisis de Macros y ambientes de emulación Windows XP, Windows 7, Windows 8.1 y Windows 10.

Extracción de amenazas

- a) Protege proactivamente a los usuarios del contenido malicioso. Para todas las descargas de internet entrega archivos seguros mientras se inspeccionan los archivos originales en busca de posibles amenazas.
- b) Para todas las descargas de archivos de internet, se debe tener las siguientes capacidades:
 - Extracción y Prevención. - El usuario final recibe una versión limpia del archivo (se retiran los elementos activos de riesgo). El administrador puede seleccionar qué partes maliciosas extraer del archivo basado en nivel de riesgo. Por ejemplo, Macros, Java Scripts, etc.
 - Debe poder transformar el archivo en PDF y se obtienen una versión benigna del archivo en formato PDF, en tanto el archivo original es emulado. Cuando la emulación termina el usuario recibe el archivo original. También se puede determinar que se suspenda la descarga hasta que termine con la emulación.
 - Detección. - Se emula el archivo sin detener la descarga del archivo original.

Captura de amenazas

- a) Debe proveer una herramienta de investigación que permite realizar consultas avanzadas sobre todos los eventos forenses maliciosos y benignos recopilados de los terminales que cuenta con el software de seguridad instalado.
- b) La información recopilada debe permitir:
 - Investigue el alcance completo de un ataque.
 - Descubrir un ataque sigiloso mediante la observación de una actividad sospechosa.
 - Reparar el ataque antes de que cause más daño.
 - Busque de forma proactiva ataques avanzados mediante la búsqueda de anomalías y el uso de pistas de búsqueda.
- c) La caza de amenazas debe permitir:
 - Recopilación y enriquecimiento de datos: todos los eventos se recopilan a través de múltiples sensores en agente, se envían a un repositorio unificado y se complementan con información de inteligencia de amenazas, mapa de MITRE ATT&CK y alertas de todos los motores de prevención de amenazas.
 - Consultas predefinidas y un panel de MITRE ATT&CK que mapean toda la actividad y permite el inicio rápido a la búsqueda proactiva de amenazas.
 - Acciones de remediación por cada resultado o de manera masiva, para tomar acciones como la cuarentena de archivos, terminar procesos, iniciar análisis forense y aislar equipos.

- d) Los datos del mapa de captura de amenazas se deben tener una retención mínima de 30 días.

Consola de administración & eventos

- a) La consola de administración deberá ser provista en modo SaaS (Software como servicio) provista por el fabricante y debe proporcionar una consola centralizada para gestionar los servicios, simplificando la gestión de la seguridad y mejora la visibilidad.
- b) La consola de administración debe proveer principalmente:
- Visibilidad en tiempo real de los incidentes y alertas de seguridad, para responder rápidamente a las amenazas y prevenir violaciones de seguridad.
 - Proporciona capacidades detalladas de análisis e informes forenses, que permite monitorear el desempeño de la seguridad e identificar áreas de mejora.
- c) El acceso a consola de administración en nube debe soportar doble factor de autenticación (2FA o MFA) a través de Google Authenticator y Microsoft Authenticator.
- d) El acceso a consola de administración en nube debe soportar integración con contratistas de identidad (IdP) tales como Microsoft ADFS, Microsoft Entra ID (Azure AD), Google Workspace, Okta, DUO y otros basados en SAML.
- e) Debe tener capacidad de gestión de equipos finales, integrado con el Directorio Activo Microsoft existente on-premise, a través de agentes que realicen la función de scanner, para importar el árbol de equipos internos en red LAN.
- f) La solución debe ser capaz de crear log de seguridad, de tal forma que se tenga información ante un incidente de seguridad.
- g) Debe contar con un módulo que permita ver en forma general cual es el estado de los puntos finales, así como las alertas que están activas.
- h) Debe permitir la configuración de políticas de todos los módulos para los equipos de usuario final.
- i) Debe tener un módulo que permita hacer seguimiento de cada módulo de seguridad instalado en los puntos finales, de tal forma que podamos tener información relevante de los usuarios y PC por módulo de seguridad instalado en los agentes.
- j) Debe contar con un módulo que permita configurar todo lo relacionado al modo de implementación o despliegue de los agentes. El despliegue se podrá realizar mediante archivo MSI o paquetes completos pre-configurados.
- k) La consola debe tener capacidad enviar operaciones hacia los agentes, tales como: desplegar nuevos agentes, reparar los agentes, apagar el equipo, reiniciar el equipo, desinstalar el agente, kill (matar) procesos y recolectar logs de los agentes.
- l) La consola debe tener capacidad de gestionar los indicadores de compromiso (IoC) en los agentes.
- m) Los IoC a gestionar deben ser como mínimo: dominio, dirección IP, URL, Hash (MD5 y SHA1). Los IoC puede ser cargados manualmente desde un archivo CSV.
- n) Se debe poder definir desde la consola una contraseña para la desinstalación del agente, para evitar la desinstalación no autorizada.
- o) Debe contar con un módulo de vista operacional, que permita mostrar la siguiente información:
- El tipo de Endpoint sea desktop o laptop.
 - El tipo del SO en el Endpoint (Windows, MacOS, Linux).
 - Versión del producto (agente) desplegado.
 - El resumen de estado del despliegue de cada agente.
 - Versiones del Sistema Operativo empleado.
 - Esta de las actualizaciones de las firmas antimalware, de emulación, de comportamiento entre otras que presentan algún desfase en la actualización

- p) Debe contar con un módulo de reportes que permite mostrar la siguiente información:
- Reporte análisis de amenazas.
 - Cyber Ataques de alto riesgo
 - Actividad Web (Internet)
 - Reporte de Emulación de Amenazas
 - Reporte de Extracción de Amenazas
 - Reporte de Cumplimiento
 - Reporte de Despliegue de Producto
 - Reporte de Políticas de seguridad
- q) Debe contar con un módulo de vista de seguridad que permita mostrar la siguiente información:
- Hosts bajo ataque y ataques activos.
 - Ataques limpiados y bloqueados.
 - Hosts infectados.
 - Línea de Tiempo de los ataques.

5.3. SERVICIO DE ACCESO CENTRALIZADO A INTERNET PARA LOS ESTABLECIMIENTOS DE SALUD CON SEGURIDAD VIRTUAL EN LA RED DEL CONTRATISTA

- a. Se requiere un servicio centralizado de Acceso a Internet con un ancho de banda de 3 Gbps implementado en la Red del contratista, cuyo ancho de banda será compartido ser usado por todos los Establecimientos de Salud según Tabla N°1 del Anexo N°1.
- b. En cada Establecimiento el mismo enlace para transmisión de datos permitirá al EESS acceso a internet a través del Servicio Centralizado de Acceso del contratista.
- c. El servicio de Acceso debe proporcionar un pool de 32 direcciones IP (IPv4) públicas que podrán distribuirse para algún servicio específico.
- d. El servicio de Internet ofrecido por el POSTOR deberá contar con varios niveles de contingencia tanto en su backbone local, así como también en la salida internacional de ingreso al Backbone de Internet. El contratista deberá contar como mínimo con 2 Proveedores TIER 1 para su salida a Internet. Se adjuntará a la propuesta una topología con los dos proveedores y sus capacidades.
- e. El contratista deberá contar con conexión directa y propia al "NAP Perú", con una capacidad mínima de 2x100Gbps, para lo cual el postor deberá presentar una carta para la etapa de firma del contrato que lo demuestre
- f. El CONTRATISTA debe poseer NOC Local y Propio para garantizar la gestión del servicio de Internet, el mismo que será acreditado con documentación que acredite poseer el NOC Local para la presentación de ofertas.
- g. El servicio deberá contar con un sistema de DNS redundantes
- h. El postor deberá contar con el servicio de DNS (Sistema de Nombres de Dominio) de manera auto gestionable, teniendo la entidad el acceso a un entorno web (con usuario y clave) que permitirá la capacidad de crear,

actualizar registrar, modificar y eliminar las configuraciones de sus registros DNS, sin la necesidad de asistencia técnica del equipo de soporte. (No se requerirá la instalación de equipos adicionales). En caso de no poseer un sistema para la gestión automática deberá tener un sistema de solicitudes vía correo electrónico con un tiempo de respuesta de 30 minutos.

- i. El contratista debe contar con un sistema de monitoreo vía web que permita visualizar el tráfico del enlace que se contrate, este sistema de monitoreo debe ser accesible para LA ENTIDAD sin que esto represente costo adicional. La ENTIDAD podrá monitorear el tráfico en línea de forma permanente en ambos sentidos para lo cual el contratista brindará un usuario y contraseña. El tiempo de información histórica disponible en la herramienta de monitoreo será de los últimos 3 meses como mínimo.
- j. El contratista debe contar con una línea para el servicio de atención al cliente y soporte técnico 24x7. La línea es exclusiva para clientes corporativos y el horario es de lunes a domingo las 24 horas del día
- k. El SLA será de 99.5% mensual como mínimo para el Acceso a Internet ubicado en el Centro de Datos del contratista, el tiempo de atención de cualquier tipo de avería será computado a partir de una llamada telefónica y/o mensaje de correo electrónico, luego de producido el incidente, para de este modo facilitar el seguimiento de la falla reportada.
- i. El servicio de Acceso Centralizado a Internet debe incluir una plataforma de seguridad perimetral instalado en la infraestructura del datacenter del contratista propio o alquilado, donde se implemente la traslación de direccionamiento y adicionalmente se pueda establecer políticas específicas para la protección de la navegación de las EESS. Este servicio de seguridad perimetral debe contar con las siguientes características
- Debe ser brindado con equipamiento instalado en el Centro de Datos del contratista que puede ser propio o tercerizado.
 - Debe ser equipamiento de propósito específico y la plataforma tecnológica debe encontrarse en el cuadrante de líderes del reporte Gartner de Network Firewalls o similar.
 - Debe soportar una concurrencia, de al menos 1200 usuarios
 - Debe brindar las funcionalidades de filtrado web, Antivirus, Control de aplicaciones y VPN IP-Sec.
 - Debe permitir almacenar un histórico mínimo de 1 mes
 - Se brindará un reporte mensual y generar reportes.
 - Se deberá brindar un usuario y contraseña de modo lectura y escritura (Nivel Administrador) para la Entidad ya que la administración será compartida
- j. Para brindar este servicio el contratista debe contar, por lo menos para un segundo nivel de atención con un SOC local propio o tercerizado, con estándares avanzados de procesos, tecnología, personal, gestión y mejora continua en ciberseguridad, lo cual debe permitir garantizar una adecuada gestión del servicio de seguridad. Para acreditarlo el Postor deberá presentar un certificado vigente emitido por una entidad reconocida que acredite que el Centro de Operaciones de Seguridad (SOC) propuesto ha alcanzado un nivel de madurez de 2.3 según el modelo de referencia SOC- CMM (Security Operations Center – Capability Maturity Model).

- k. La plataforma de Seguridad Perimetral Solicitada debe brindar un alto nivel de disponibilidad (mayor al 99,95%), para lo cual esta solución deberá encontrarse implementada en la red del contratista y dentro de una infraestructura apropiada de Datacenter, la cual deberá contar con certificación en diseño y/o construcción y/o sostenibilidad TIER 3 emitido por el UPTIME INSTITUTE como mínimo. El postor deberá presentar la documentación sustentatoria del datacenter que garantice el cumplimiento de este requisito en la firma del contrato.
- l. Adicionalmente el contratista deberá brindar un servicio que permita la Administración y Optimización de Ancho de Banda del Acceso Centralizado a Internet, a través de una solución de propósito específico que cumpla como mínimo con:
- El equipo debe estar alojado en la misma infraestructura de Datacenter del Equipamiento de Seguridad Perimetral.
 - Debe ser un equipo dedicado y de propósito específico (no UTM, no Firewalls, no Balanceadores, no servidores, etc).
 - Debe contar con al menos 2 pares de interfaces bridge-bypass, velocidad 10Gbps
 - Deberá tener capacidad de crecimiento de al menos 1 par de interfaces bridge-bypass
 - Contar con almacenamiento interno que le permita al equipo tener la capacidad necesaria para que brinde información y/o reportes del tiempo de contrato como también que tenga características de redundancia que garantice los datos en el tiempo solicitado.
 - Estar licenciado para soportar el ancho de banda total de todas las sedes remotas, de tipo full duplex.
 - Deberá soportar al menos 10,000,000 flujos concurrentes que permita soportar los usuarios de la entidad y cargas adicionales.
 - El equipo debe tener capacidades redundantes en el hardware a fin de garantizar su disponibilidad de funcionamiento en el tiempo, donde mínimamente tenga fuente de poder, ventiladores y almacenamiento redundante.
 - Debe permitir priorización de tráfico, definir un mínimo de ancho de banda garantizado y un máximo de ancho de banda permitido.
 - Deberá medir de forma nativa, métricas de rendimiento que permita monitorear el tráfico de la red, donde se tengan métricas TCP, tráfico web, tráfico VoIP entre otros.
 - Deberá considerar una consola de administración gráfica en el mismo equipo que permita administrar, configurar y generar reportes del equipo Administrador de Ancho de Banda. Se debe indicar en su Oferta la marca y modelo del equipo considerado.
 - La consola de administración debe tener capacidades de multiusuario el cual permita generar roles y permisos específicos para usuarios administradores de la entidad que le permita tener acceso a la información específica a la sede que pertenece y de administradores globales que sí podrían ver todas las sedes.

5.4. SEDE PRINCIPAL Y ESTABLECIMIENTOS DE SALUD : SERVICIO DE TELEFONIA

- a. Se debe brindar el servicio de telefonía para la Sede Central y los Establecimientos de Salud según Tabla N°1 del Anexo N°1, a través de una plataforma instalada en un Datacenter propio o tercerizado del contratista y que incluya : Central de Conmutación de llamadas (PBX IP), Controlador de Sesiones (SBC) y Troncal SIP.
- b. La solución de Central de Conmutación de llamadas (PBX) debe brindarse a través de equipamiento de hardware de propósito específico en alta disponibilidad. No se aceptarán plataformas virtualizadas o que estén basadas en servidores y software de código abierto.
- c. Adicionalmente se deberán instalar un total de 794 anexos telefónicos o teléfonos IP distribuidos según se indica en la TABLA N°1 en Anexo N°1, en las Sedes de la Diris Lima Norte.
- d. Los teléfonos IP deben ser de la misma marca que la central telefónica a fin de usar al máximo sus funcionalidades y no tener inconvenientes con la integración.
- e. La plataforma se debe incluir la implementación de una Troncal SIP de 120 canales , A través de esta troncal SIP se realizarán llamadas desde y hacia la Sede Principal y los EESS
- f. El contratista facilitará 03 números fijos.
- g. Debe permitir vía web la gestión de usuarios, anexos, colas, llamadas y reporte de llamadas
- h. Se requiere se brinden 150 DDI
- i. La Entidad brindará el cableado de datos necesario para la operación de los aparatos telefónico o anexos en cada una de las Sedes de la Diris Lima Norte
- j. El sistema deberá contar con una operadora automática que permita presentar un mensaje de bienvenida a nivel de audio y poder distribuir la llamada de acuerdo al número de extensión requerido (tonos DTMF-dual-tone multifrequency) en su defecto enviar la comunicación a una operadora.
- k. La central telefónica deberá tener las siguientes características:
 - o Configurada en alta disponibilidad sea en arquitectura 2N o N+1.
 - o Deberá tener la capacidad de soportar al menos 2500 usuarios (contabilizando las conexiones simultáneas a una misma extensión, extensiones físicas y softphones)
 - o Soporte de al menos 500 llamadas simultáneas (internas y externas)
 - o Soporte y activación de 100 softphones por el tiempo de contrato los cuales se usarán a través de la red privada de la entidad y el operador. Los softphones deberán ser compatibles con la solución de central telefónica propuesta.
 - o Cada central telefónica deberá contar como mínimo con tres (3) puertos GigabitEthernet
 - o Cada central telefónica deberá contar con doble fuente de energía redundante
 - o Las centrales telefónicas deberán tener factor de forma 1RU.
 - o Códecs de voz: Opus, G.711 A-law/U-law, G.722, G722.1 G722.1C, G.723.1, G.729A/B, iLBC, GSM; T.38,
 - o Códes de video: H.264, H.263, H263+, VP8
 - o El IVR multinivel de hasta 5 niveles.

- Direccionamiento de llamadas de acuerdo a distintos horarios establecidos por la entidad
- Soporte de IPv4 así como IPv6
- Grabación de llamadas internas y externas
- Música en espera personalizada
- Soportar funcionalidades de:
 - Transferencia de llamada.
 - Call Routing
 - Llamada en espera.
 - Paginación (Perifoneo interno a través de teléfonos IP)
 - Monitoreo de la PBX
 - DND.
 - Audio Conferencias.
 - BLF Support.
 - DISA.
 - Audio de Bienvenida (IVR)
 - Llamar lista de permitida / bloquear
 - Transferencia sin consulta.
 - Registro de detalles de Llamada.
 - Transferencia de llamada bajo consulta.
 - Captura de Llamada.
 - Grabaciones de llamadas
 - Registros concurrentes para Teléfonos IP
 - Avisos personalizados
 - Tono de llamada distintivo
 - Enrutamiento de llamadas (DID).
 - Identificación de Llamada
 - Envío de Fax a Email.
 - Correo de voz grupal
 - Auto Provisionamiento.
 - Monitoreo de llamadas (Listen/Whisper/Barge-in).
 - Lista de PIN
 - Número de emergencia
 - Notificaciones de emergencia
 - Desvío de llamadas.
 - Extensión de movilidad
 - Extensiones remotas
 - Marcación rápida
 - Grupo de timbrado.
 - Grupo de cola de atención.
 - Sistema de Backup.
 - Reporte de llamadas.
 - voicemail
 - Mensajes del Buzón de Voz a Email.
 - Llamada de audio WebRTC
 - AMI
 - Web-based GUI
 - Dashboard

l. Los terminales IP deberán contar con al menos las siguientes características:

- El teléfono propuesto deberá ser de la misma marca de la central telefónica
- Pantalla a color LCD como mínimo de 2.7" 320x240 con retroiluminación
- 02 puertos Ethernet 10/100/1000 Mbps con PoE integrado
- Soporte de códecs de voz: G.729A/B, G.711µ/a-law, G.726, G.722 (banda ancha), G.723, iLBC, OPUS
- DTMF en banda y fuera de banda (audio de entrada, RFC2833, SIP INFO), VAD, CNG, AEC, PLC, AJB, AGC.
- Soporte de 3 cuentas SIP y 3 líneas
- Conferencias de audio de 5 participantes
- Directorio telefónico de al menos 1900 contactos (internos y externos)
- Registro de las últimas 800 llamadas
- 2 teclas de línea, 4 teclas programables XML sensibles al contexto, 5 teclas de navegación/menú y 8 teclas de función dedicadas para: MENSAJE (con indicador LED), TRANSFERENCIA, AURICULAR, SILENCIAR, ENVÍO/REMARCACIÓN, ALTA VOZ, VOL+, VOL-
- Contraseñas a nivel de usuario y administrador
- Autenticación basada en MD5 y MD5-sess
- Archivo de configuración cifrado con AES de 256 bits
- SRTP, TLS
- Control de acceso a medios 802.1x.
- Actualización de firmware por medio de FTP, TFTP, TFTP/HTTPS, HTTP y HTTPS
- Power-over-Ethernet integrado (802.3af) y IEEE 802.3az, protocolo usado para garantizar la eficiencia de energía
- Los teléfonos deben contar con fuente de energía
- Funciones soportadas:
 - Retención de llamada
 - Transferencia de llamada
 - Desvío de llamada
 - Conferencia mínima de 5 participantes
 - Parqueo de llamadas
 - Captura de llamadas (Pick-up)
 - Estado de línea compartida (SCA)/estado de línea en puente (BLA)
 - Llamada en espera
 - Personalización de la pantalla
 - Marcación automática al descolgar
 - Contestación automática
 - Clic para marcar (click-to-dial)
 - Plan de marcación flexible
 - Hot-desking
 - arranque seguro
 - Tonos de llamada personalizados y música de espera
 - Redundancia de servidor y tolerancia frente a fallos

m. El contratista deberá proveer una solución de Controlador de Sesiones o equipo Session Border Controller físico o virtual que soporte la cantidad total de llamadas concurrentes requeridas.

- n. La Solución SBC deberá contar con estándares y/o protocolos para calidad de Voz como: Limite el número y la tasa de sesiones y registros simultáneos por par para direcciones entrantes y salientes, Etiquetado VLAN 802.1p/Q, DiffServ, TOS.
- o. La solución SBC debe integrar un sistema de monitoreo de troncales SIP, el cual genere alarmas en caso haya alguna incidencia en las troncales, permitiendo realizar un troubleshooting de manera efectiva. Esta herramienta deberá ser parte del servicio ofertado y deberá ser de tipo cloud. Este sistema de monitoreo debe medir QoS de las troncales SIP con indicadores de MOS, Jitter, Delay, echo y generar alarmas cuando estos parámetros no tengan una buena calidad.
- p. Tanto los equipos SBC como el sistema de Monitoreo deberá ser de la misma marca de los SBC propuestos para asegurar una adecuada integración.
- q. La bolsa de minutos mensual para el servicio de telefonía fija será de:
 - i. 75,000 minutos a fijos locales mensuales
 - ii. 40,000 minutos a celulares nacionales mensuales.
- r. En caso de exceder la cantidad de la bolsa de minutos esta deberá restringirse hasta el mes siguiente en la cual se vuelve a recargar los minutos

5.5. SERVICIO DE INFRAESTRUCTURA DE NUBE PRIVADA

- a. El contratista deberá brindar de un servicio de infraestructura de nube privada local para replicar algunas de las aplicaciones críticas que puedan accederse desde los establecimientos de salud en caso de generarse una indisponibilidad de los sistemas principales instalados en la Sede Central
- b. El servicio debe prestarse desde una plataforma hiperconvergente de alta disponibilidad instalado en un Infraestructura de Data Center Certi se desde un datacenter de la Se debe brindar el servicio de telefonía para la Sede Central y los Establecimientos de Salud
- c. El servicio de almacenamiento de información en nube incluirá el acceso de forma segura, por lo que el postor debe contar con el ISO/IEC 27001:2013 relacionado a los Servicios Cloud y/o Centro de Datos. El postor deberá presentar a la presentación de la propuesta, la documentación sustentatoria que garantice el cumplimiento de este requisito.
- d. Los servidores virtuales deben soportar agregar en caliente vCPU, RAM, vNIC y disco virtual siempre que el Sistema Operativo de la máquina virtual lo soporte.
- e. El contratista deberá proporcionar discos all flash para la capacidad de disco contratada para el servicio de alojamiento de información que requiere la entidad, estos discos deberán estar desplegados en un esquema de hiperconvergencia con recursos de procesamiento y memoria RAM.
- f. El contratista deberá proporcionar 30 CPU, 128 GB RAM y 2 TB de disco de estado sólido, donde la entidad podrá desplegar los sistemas que designe como críticos.
- g. La Entidad será responsable del soporte del sistema operativo y las aplicaciones que se implemente sobre estos.
- h. Se requiere una conexión privada entre la Sede Principal y la plataforma de nube privada local de 200Mbps

- i. La plataforma de nube privada local deberá encontrarse implementada dentro de una infraestructura apropiada de Datacenter, la cual deberá contar con certificación en diseño y/o construcción y/o sostenibilidad TIER 3 emitido por el UPTIME INSTITUTE como mínimo. El postor deberá presentar la documentación sustentatoria del datacenter que garantice el cumplimiento de este requisito en la firma del contrato.
- j. El contratista deberá proporcionar el servicio de backup de la información de los servidores, con una retención de hasta 15 días en un esquema de 01 full backup cada 15 días y 14 backups incrementales diarios, por lo que para el espacio de los backups se debe considerar una capacidad independiente de 2 TB.

6. GESTIÓN Y SOPORTE DEL SERVICIO

- a. Disponibilidad del servicio mínimo: SLA de 99.97 % de disponibilidad mensual como mínimo para el Servicio de Transmisión de Datos e internet para Sede Central.
- b. Disponibilidad del servicio mínima: SLA de 99.5 % de disponibilidad mensual como mínimo para el Servicio de Transmisión de Datos de los EESS
- c. Disponibilidad del servicio mínima: SLA de 99.97 % de disponibilidad mensual como mínimo para el Servicio Centralizado a Internet para las EESS
- d. Disponibilidad del servicio mínima: SLA de 99.97 % de disponibilidad mensual como mínimo para el Servicio de Telefonía e Infraestructura de Nube Privada.
- e. Disponibilidad del servicio mínima: SLA de 99.95 % de disponibilidad mensual como mínimo. para el Servicio de Troncal SIP y PBX en nube.
- f. La Entidad brindará todas las facilidades de acceso para realizar la instalación del servicio, brindando un ambiente adecuado para la colocación de los equipos, energía estabilizada, baja temperatura, pozo a tierra y a la vez la protección del equipamiento; de ser necesario se brindará la conexión del equipo a un UPS,
- g. El Postor debe contar con un Centro de Atención que monitorea y supervisa la integridad del enlace las 24 horas del día, los 7 días de la semana, los 365 días del año. El tiempo de atención por averías será computado a partir de la generación de un ticket de atención y/o reporte de incidencia. El área usuaria, evaluará previamente si las averías reportadas corresponden por responsabilidad del contratista, en cuyo caso, deberá aplicar las penalidades correspondientes y determinadas en los términos de referencias, por otro lado, si la avería fue ocasionada por caso fortuito o de fuerza mayor, debidamente sustentada por el contratista, y evaluada por el área usuaria y de ser conforme, no se generará ningún tipo de penalidad en contra del contratista ni se le imputará ningún incumplimiento.
- h. El contratista monitoreará permanentemente el servicio en tiempo real. El Centro de Gestión de Red del contratista estará en capacidad de realizar detección temprana de fallas, acciones de control preventivo, correctivo y pruebas técnicas.
- i. Se elaborarán reportes de fallas en la red; si la hubiera, considerando las causas de las mismas. Del mismo modo, mensualmente se enviará a la Entidad el reporte de servicio.
- j. El Soporte técnico deberá ser realizado en un plazo no mayor a 04 horas (resolución de avería). Las averías de Planta Externa tendrán un tiempo de resolución de 8 horas, salvo en situaciones donde el contratista demuestre que el hecho fue generado por un tercero. En los casos de avería por degradación el contratista tendrá un plazo máximo para resolver de 12 horas, asimismo; el contratista deberá presentar un

informe técnico sustentatorio, dirigido al área usuaria, el cual se evaluará, y de corresponder la causal de avería por degradación, no se le imputará la degradación.

- k. El tiempo de solicitud de asistencia técnica se contará a partir de una llamada telefónica y/o correo electrónico generada al postor.

7. CAPACITACIÓN

a. Las capacitaciones podrán ser realizadas desde el día siguiente de la firma del Acta de Inicio del Servicio, hasta un plazo máximo de tres (03) meses. Las fechas, horarios u otra coordinación deberán realizarse con la Oficina de Gestión de Tecnologías de la Información.

b. La empresa adjudicada brindará capacitación técnica bajo el siguiente detalle:

- Capacitación de 20 horas como mínimo y para 4 participantes sobre el equipamiento de Seguridad Perimetral propuesto como parte del Servicio de Internet.
- Capacitación de 20 horas como mínimo y para 4 participantes sobre curso de Ethical Hacking.
- Capacitación de 12 horas como mínimo en el Software de Monitoreo propuesto
- Todas las capacitaciones deben incluir certificado indicando la cantidad de horas.
- La capacitación será dictada de manera virtual o presencial.

8. PLAZO DE EJECUCIÓN DEL SERVICIO

El plazo de ejecución del servicio será de 820 días calendario a partir de suscrito el contrato por la empresa adjudicada

- a. El plazo de implementación será de 90 días calendario
- b. El plazo de ejecución del servicio en marcha será brindado por 730 días calendarios y deberá iniciar a partir del día siguiente de suscrita el Acta de Conformidad de la implementación de todas las sedes por parte del Área Usuaria.

9. RESPONSABILIDADES

Responsabilidad de la Entidad:

- La Entidad dará las facilidades al contratista dentro de sus instalaciones (indicadas en ANEXO 01 CONSOLIDADO DE EESS Y SEDE ADMINISTRATIVA CON SUS RESPECTIVAS DIRECCIONES Y COORDENADAS DE LA DIRIS LN), previa solicitud y coordinación con el área técnica, OFICINA DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.
- La Entidad brindará todos los puertos LAN y puntos de red que resulten necesarios para la implementación del servicio

Por ello se confirma que la entidad proporcionará los siguientes equipos/accesorios:

- Tomacorrientes
- Energía Estabilizada
- Puertos disponibles en sus switches LAN
- Tendido de cableado eléctrico
- Pozos de Tierra

- Cualquier trabajo de cableado estructurado interno

Responsabilidad del contratista:

- Cableado de fibra óptica externa para la última milla
- Gabinetes y Equipos routers
- La ruta de cableado será efectuada siguiendo las mejores prácticas de implementación y buscando el menor impacto posible en la infraestructura interna del local de la Entidad (uso de canaletas y ductos existentes, falso techo, etc.).
- Provisión e implementación de materiales diversos como ODF de rack o pared, cables jumper de fibra, cable jumper UTP y ductos flexibles corrugados, necesarios para la correcta puesta en servicio de la WAN.
- Provisión del(los) cable(s) jumper(s) UTP de conexión entre el(los) router(s) WAN provisto(s), propiedad del contratista.
- Cableado y conectorización de tierra eléctrica, desde cada equipo de comunicaciones provisto, hacia la plancha o varilla de cobre disponible.
- Asimismo, es responsabilidad del contratista realizar los trámites y permisos correspondientes ante las autoridades que correspondan para la implementación del servicio. El contratista únicamente podrá solicitar ampliación de plazo, siempre y cuando haya realizados los trámites y/o permisos correspondientes, dentro de los 15 días calendarios posteriores a la suscripción del contrato.

10. GARANTÍA

Cubre la reparación de averías que se produzcan como consecuencia de falla de fábrica del producto. En consecuencia, se encuentran excluidas aquellas averías originadas por:

- Uso indebido o errores de manipulación en los equipos por DIRIS Lima Norte.
- Daños surgidos por reparaciones o modificaciones no efectuadas por el contratista u otra empresa autorizada por ella.
- Fallas en la operatividad del servicio debido a la reconfiguración de los equipos sin autorización del contratista.
- Traslados de los equipos sin conocimiento ni autorización por el contratista.
- Fallos en los equipos producidos por operación en condiciones que no cumplan con las especificaciones indicadas por el fabricante. El contratista será responsable de la correcta operatividad de los equipos instalados para la prestación del servicio, en caso surja desperfectos y/o averías que dañen los equipos propios de la Entidad, y que se evidencien a través de la evaluación técnica realizada por el área usuaria, el contratista deberá asumir los gastos correspondientes.

11. CONFORMIDAD DEL SERVICIO

La conformidad por el servicio será mensual y emitida por la Oficina de Gestión de Tecnologías de la Información de la Dirección de Redes Integradas de Salud Lima Norte.

12. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en forma mensual, previa conformidad de la Coordinación de Comunicación, Redes y

Soporte Informático de la Oficina de Tecnologías de la Información, quienes verificarán el cumplimiento del servicio de acuerdo a lo solicitado en los términos de referencia.

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

- Informe de conformidad del funcionario responsable de la Coordinación de Comunicación, Redes y Soporte Informático de la Oficina de Tecnologías de la Información, emitiendo la conformidad de la prestación efectuada.
- Comprobante de Pago Electrónico respectivo y expresado en soles.
- Acta de conformidad emitida por la Oficina de Gestión de tecnología de Información.

13. RESPONSABILIDAD DE VICIOS OCULTOS

El contratista es responsable por la calidad ofrecida y por los vicios ocultos de los servicios ofertados por un plazo no menor de un (01) año contado a partir de la conformidad otorgada por la entidad.

14. PENALIDADES

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.

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

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

Donde F tiene los siguientes valores:

Fx plazo en días

a) Para plazos mayores a sesenta (60) días.

a.1) Para bienes, servicios en general y consultorías: $F = 0.25$

Tanto el monto como el plazo se refieren, según corresponda, a la ejecución total del servicio o a la obligación parcial, de ser el caso, que fuera materia de retraso.

Se considera justificado el retraso, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable.

Esta calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.

15. OTRAS PENALIDADES

Durante la ejecución del servicio se aplicarán otras penalidades por incumplimiento en la disponibilidad del servicio comprometida, así como por demora en los tiempos de atención según el cuadro siguiente:

Penalidad por Incumplimiento del Nivel de Servicio de Interconexión de Datos en las EESS

El nivel de servicio esperado de 99,5% en la disponibilidad del Servicio de Interconexión de Datos en las EESS se medirá de manera mensual y para efectos de calculo sólo se considerará indisponibilidad en caso de pérdida total del servicio (servicios principal y de contingencia con avería). Asimismo la penalidad aplicará sobre el pago mensual correspondiente del servicio de la siguiente forma:

Disponibilidad	Penalidad (% deducible de la facturación mensual del servicio)
Mayor o igual al 99.5%	0%
≥ 99.3 y < 99.5	10%
≥ 99.0 y < 99.3	20%
< 99.0	30%

Penalidad por Incumplimiento del Nivel de Servicio de Internet Centralizado

El nivel de servicio esperado de 99,97% en la disponibilidad del Servicio de Internet Centralizado y se medirá de manera mensual y para efectos de calculo sólo se considerará indisponibilidad en caso de pérdida total del servicio (servicios principal y de contingencia con avería). Asimismo la penalidad aplicará sobre el pago mensual correspondiente del servicio de la siguiente forma:

Disponibilidad	Penalidad (% deducible de la facturación mensual del servicio)
Mayor o igual al 99.95%	0%
≥ 99.93 y < 99.95	10%
≥ 99.90 y < 99.93	20%
< 99.90	30%

Importante

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

ANEXO 01

TABLA N°1

Relación de Sedes consideradas para el servicio

N°	DISTRITO	CATEGORÍA	ESTABLECIMIENTO	TÓNICOS	LATITUD	LONGITUD
1	ANCON	I-4	CSMI ANCON	8	-11.7747191	-77.1727247
2	ANCON	I-3	CS VILLA ESTELA	4	-11.814635	-77.132218
3	ANCON	I-3	CS SAN JOSÉ	4	-11.7782373	-77.162575
4	ANCON	I-2	PS VILLAS DE ANCON	4	-11.7339705	-77.1459659
5	ANCON	I-3	CSMC RIJCHARY (DESPERTAR)	8	-11.8141858	-77.1336187
6	CARABAYLLO	I-4	CSMI EL PROGRESO	8	-11.87554	-77.0167279
7	CARABAYLLO	I-3	CS LA FLOR	4	-11.8961113	-77.0271114
8	CARABAYLLO	I-3	CS RAUL PORRAS BARRENECHEA	4	-11.8934379	-77.0244019
9	CARABAYLLO	I-3	CS VILLA ESPERANZA	4	-11.88614	-77.022109
10	CARABAYLLO	I-2	PS CHOCAS	4	-11.7667755	-76.9771577
11	CARABAYLLO	I-2	PS PUNCHAUCA	4	-11.8345612	-77.000102
12	CARABAYLLO	I-2	PS JORGE LINGAN	4	-11.8839462	-77.0201549
13	CARABAYLLO	I-2	PS LUIS ENRIQUE	4	-11.8770066	-77.0095277
14	CARABAYLLO	I-2	PS SU MAJESTAD HIROITO	4	-11.881205	-77.003039
15	CARABAYLLO	I-3	CSMC CARABAYLLO	4	-11.9008135	-77.0342341
16	CARABAYLLO	I-3	CS JUAN PABLO II	4	-11.8283581	-77.0691136
17	CARABAYLLO	I-3	CS SAN PEDRO DE CARABAYLLO	4	-11.854034	-77.037398
18	CARABAYLLO	I-3	CS SAN BENITO	4	-11.8184648	-77.0471714
19	CARABAYLLO	I-3	CSMC ASIRI (SONRISA)	4	-11.8787874	-76.9982302
20	COMAS	I-4	CSMI SANTA LUZMILA II	8	-11.9470252	-77.0587122
21	COMAS	I-3	CS SANTA LUZMILA I	4	-11.9416876	-77.0636501
22	COMAS	I-3	CS CARLOS PHILLIPS	4	-11.959672	-77.057458
23	COMAS	I-3	CS HUSARES DE JUNIN	4	-11.9361947	-77.0518657
24	COMAS	I-3	CS EL ALAMO	4	-11.9347565	-77.0656999
25	COMAS	I-3	CS CLORINDA MÁLAGA	4	-11.9661638	-77.0541862
26	COMAS	I-3	CS CARLOS A. PROTZEL	4	-11.9402602	-77.0471573
27	COMAS	I-3	CS COMAS	4	-11.9535459	-77.0495129
28	COMAS	I-3	CS SANTIAGO APOSTOL	4	-11.9569237	-77.0433316
29	COMAS	I-3	CS CARMEN MEDIO	4	-11.9412286	-77.0401638
30	COMAS	I-3	CS CARMEN ALTO	4	-11.945087	-77.0308479
31	COMAS	I-2	PS SEÑOR DE LOS MILAGROS	4	-11.9415104	-77.0452168
32	COMAS	I-4	CSMI LAURA RODRÍGUEZ DULANTO DUKSIL	8	-11.9160503	-77.0553621
33	COMAS	I-3	CS COLIQUE III ZONA	4	-11.9147365	-77.026223
34	COMAS	I-3	CS AÑO NUEVO	4	-11.9231023	-77.0401525
	COMAS	I-3	CS GUSTAVO LANATTA	4	-11.9146878	-77.0113278
	COMAS	I-2	PS 11 DE JULIO	4	-11.930841	-77.037336
	COMAS	I-2	PS MILAGRO DE JESÚS	4	-11.9186782	-77.0258283

DIRECCIÓN DE REDES INTEGRADAS DE SALUD LIMA NORTE
CONCURSO PUBLICO N° 01-2025-DIRIS.LN/CS-1

38	COMAS	I-2	PS SAN CARLOS	4	-11.9086992	-77.041319
39	COMAS	I-3	CS SANGARARA	4	-11.9187627	-77.0436659
40	COMAS	I-2	PS PRIMAVERA	4	-11.9231604	-77.0563885
41	COMAS	I-2	PS LOS GERANIOS	4	-11.8961278	-77.0434893
42	COMAS	I-2	PS LUIS ALBERTO BAZAGOITIA CARDENAS	4	-11.9230139	-77.0215085
43	COMAS	I-3	CSMC WIRAY (CRECIENDO)	4	-11.96821	-77.05743
44	COMAS	I-3	CSMC- AMACHAY (SALUD)	4	-11.92432724	-77.05436658
45	INDEPENDENCIA	I-4	CSMI TAHUANTINSUYO BAJO	8	-11.9784658	-77.0529828
46	INDEPENDENCIA	I-3	CS TAHUANTINSUYO ALTO	4	-11.979306	-77.0396598
47	INDEPENDENCIA	I-3	CS TUPAC AMARU	4	-11.9722396	-77.045511
48	INDEPENDENCIA	I-2	PS JOSÉ OLAYA	4	-11.9674774	-77.0391282
49	INDEPENDENCIA	I-2	PS LAS AMERICAS	4	-11.9876035	-77.0542211
50	INDEPENDENCIA	I-2	PS VÍCTOR RAÚL HAYA DE LA TORRE	4	-11.9774977	-77.0574234
51	INDEPENDENCIA	I-3	CS ERMITAÑO BAJO	4	-11.9977277	-77.0546443
52	INDEPENDENCIA	I-3	CS ERMITAÑO ALTO	4	-11.9992218	-77.0449556
53	INDEPENDENCIA	I-2	PS EL CARMEN	4	-12.0171219	-77.0476186
54	INDEPENDENCIA	I-2	PS LOS QUECHUAS	4	-11.990486	-77.0422114
55	INDEPENDENCIA	I-3	CS MILAGRO DE LA FRATERNIDAD	4	-12.0115856	-77.0490816
56	INDEPENDENCIA	NO	SEDE ADMINISTRATIVA 1 (PRINCIPAL)	260	-11.9774977	-77.0574234
57	INDEPENDENCIA	I-3	CSMC KAWSAY (VIDA)	4	-11.97728011	-77.05179928
58	LOS OLIVOS	I-3	CS VILLA DEL NORTE	4	-11.9710213	-77.0694925
59	LOS OLIVOS	I-3	CS LOS OLIVOS	4	-11.9929462	-77.0655621
60	LOS OLIVOS	I-3	CS CARLOS CUETO FERNANDINI	4	-11.9816146	-77.0719764
61	LOS OLIVOS	I-3	CS PRIMAVERA	4	-12.0092839	-77.07378
62	LOS OLIVOS	I-3	CS SAN MARTIN DE PORRES CONFRATERNIDAD	4	-11.9597024	-77.0802984
63	LOS OLIVOS	I-3	CS LAURA CALLER	4	-11.970078	-77.0776032
64	LOS OLIVOS	I-4	CSMI JUAN PABLO II	8	-11.9532122	-77.0788909
65	LOS OLIVOS	I-3	CS ENRIQUE MILLA OCHOA	4	-11.9565532	-77.0822282
66	LOS OLIVOS	I-3	CS SAGRADO CORAZÓN DE JESÚS	4	-11.9821913	-77.0762076
67	LOS OLIVOS	I-3	CS LOS OLIVOS DE PRO	4	-11.9510556	-77.0843759
68	LOS OLIVOS	I-3	CS RIO SANTA	4	-11.948639	-77.077903
69	LOS OLIVOS	I-3	CSMC ILLARIMUN (AMANECE)	4	-11.9774102	-77.0809391
70	LOS OLIVOS	I-3	CSMC QHALI KAY (SALUD)	4	-11.94335522	-77.07580486
71	PUENTE PIEDRA	I-4	CSMI DR ENRIQUE MARTIN ALTUNA	8	-11.8376114	-77.1090997
72	PUENTE PIEDRA	I-3	CS JERUSALEN	4	-11.8279251	-77.1174256
73	PUENTE PIEDRA	I-3	CS LA ENSENADA	4	-11.9316287	-77.095554
74	PUENTE PIEDRA	I-3	CS LADERAS DE CHILLÓN	4	-11.9203551	-77.0845349
75	PUENTE PIEDRA	I-4	CSMI LOS SUREÑOS	8	-11.8875316	-77.0697014
76	PUENTE PIEDRA	I-4	CSMI SANTA ROSA	8	-11.8748274	-77.0816932
77	PUENTE PIEDRA	I-2	PS SAGRADO CORAZÓN DE JESUS	4	-11.9084111	-77.0777749
	PUENTE PIEDRA	I-2	PS JESUS OROPEZA CHONTA	4	-11.8261347	-77.1123214
	PUENTE PIEDRA	I-3	CSMC RENATO CASTRO LA MATA	4	-11.9316287	-77.095554
	PUENTE PIEDRA	I-3	CSMC QISPIKAY	4	-11.8679905	-77.0754382

DIRECCIÓN DE REDES INTEGRADAS DE SALUD LIMA NORTE
CONCURSO PUBLICO N° 01-2025-DIRIS.LN/CS-1

81	PUENTE PIEDRA	I-2	SERVICIOS MEDICOS DE APOYO ESPERANZA Y FORTALEZA	2	11°51'17.3"S	77°05'18.3"W
82	RIMAC	I-3	CS CIUDAD Y CAMPO	4	-12.0243191	-77.0282412
83	RIMAC	I-3	CS LEONCIO PRADO	4	-12.0316958	-77.0302538
84	RIMAC	I-4	CSMI RIMAC	8	-12.0343399	-77.0336606
85	RIMAC	I-3	CS SAN JUAN DE AMANCAES	4	-12.0168446	-77.0294195
86	RIMAC	I-3	CS FLOR DE AMANCAES	4	-12.008182	-77.0354478
87	RIMAC	I-3	CS CAQUETA	4	-12.031063	-77.0433946
88	RIMAC	I-3	CS VILLA LOS ÁNGELES	4	-12.023599	-77.0242347
89	RIMAC	I-3	CS MARISCAL CASTILLA	4	-12.0178541	-77.0320255
90	RIMAC	I-4	CSMI PIEDRA LIZA	8	-12.0325307	-77.0129107
91	RIMAC	I-3	CSMC SAMAY	4	-12.0285622	-77.0302406
92	RIMAC	NO	SEDE ADMINISTRATIVA 3 (CENTRO DE ALIMENTACION)	4	-12.0364307	-77.0355843
93	SMP	I-3	CS LOS LIBERTADORES	4	-12.006979	-77.0890663
94	SMP	I-3	CS VALDIVIEZO	4	-12.0233352	-77.0660911
95	SMP	I-4	CSMI MÉXICO	8	-12.0252261	-77.0850499
96	SMP	I-3	CS SAN MARTIN DE PORRES	4	-12.0345295	-77.0549341
97	SMP	I-3	CS PERU III ZONA	4	-12.028589	-77.0764106
98	SMP	I-3	CS PERU IV ZONA	4	-12.030943	-77.0861791
99	SMP	I-3	CS CONDEVILLA	4	-12.021281	-77.0814067
100	SMP	I-3	CS AMAXELLA	4	-12.0179051	-77.0785731
101	SMP	I-2	PS CERRO LA REGLA (DAVID TEJADA RIVERO)	4	-11.984054	-77.101534
102	SMP	I-3	CS GUSTAVO LANATTA LUJAN	4	-12.0242216	-77.0732396
103	SMP	I-3	CS SAN JUAN DE SALINAS	4	-11.9841531	-77.0853237
104	SMP	I-2	PS CERRO CANDELA	4	-11.972234	-77.106448
105	SMP	I-3	CS MESA REDONDA	4	-12.0043022	-77.0575097
106	SMP	I-3	CS EX FUNDO NARANJAL	4	-11.9669636	-77.0873748
107	SMP	I-3	CS VIRGEN DEL PILAR DE NARANJAL	4	-11.9838236	-77.062838
108	SMP	I-3	CS INFANTAS	4	-11.9479208	-77.0682998
109	SMP	I-2	PS NUEVA JERUSALEN	4	-11.944476	-77.124673
110	SMP	I-3	CSMC JOSEPH GERARD RUY	4	-11.984054	-77.101534
111	SMP	I-3	CSMC MUNAY KAWAY (VIVIR EN ARMONIA)	4	-11.99107839	-77.09201515
112	SANTA ROSA	I-2	PS VIRGEN DE LAS MERCEDES	4	-11.7848411	-77.1569533
113	SANTA ROSA	I-2	PS PROFAM	4	-11.8173266	-77.1591282
114	SANTA ROSA	I-2	PS LA ARBOLEDA	4	-11.8056717	-77.1582659
115	COMAS	I-3	CSMC SAN GABRIEL	4	-11.941278	-77.059949
116	SAN MARTIN DE PORRES	I-3	CSMC SAN CARLOS	4	12°00'47.9"S	77°03'16.6"W
117	LOS OLIVOS	I-3	CSMC SAN JOSE	4	-11.961440	-77.079187
118	INDEPENDENCIA	I-3	CSMC SAN RAFAEL	4		
119	PUENTE PIEDRA	I-3	CSMC PUENTE PIEDRA	4		
120	CARABAYLLO	I-3	CSMC CARABAYLLO	4		
121	SANTA ROSA	I-3	CSMC SANTA ROSA	4		
122	SMP	I-3	CSMC SMP	4		

3.2. REQUISITOS DE CALIFICACIÓN

A.	CAPACIDAD LEGAL
	HABILITACION
	<u>Requisito:</u> El postor debe constar: <ul style="list-style-type: none">• Certificado de inscripción en el registro para el servicio de valor añadido para la prestación de servicios de datos por paquetes(internet), emitido por el MTC
	<u>Acreditación:</u> <ul style="list-style-type: none">• Copia del certificado de inscripción en el registro para el servicio de valor añadido para la prestación de servicios de datos por paquetes(internet), emitido por el MTC.

B.	CAPACIDAD TECNICA Y PROFESIONAL
B.1	INFRAESTRUCTURA
	Requisitos: <ul style="list-style-type: none">• Contar con un Call Center Técnico y con números dedicados para reportar los servicios y averías, que atenderá las 24 horas por los 7 días de la semana, durante los 365 días del año.• El postor deberá contar con un Centro de Operaciones de Red (NOC) propio, que se encuentre en la ciudad de Lima Metropolitana.• El postor deberá contar con un Centro de Operaciones de Seguridad (SOC) propio que se encuentre en la ciudad de Lima Metropolitana. Acreditación: <ul style="list-style-type: none">• Copia de documentos que sustenten la propiedad, la posesión el compromiso de compra y venta o alquiler y/o licencia de funcionamiento del inmueble del NOC/SOC donde se acredite la operación e infraestructura propia del NOC/SOC u otro documento que acredite la disponibilidad de la infraestructura estratégica requerido.
B.2	CALIFICACION DEL PERSONAL CLAVE
B.2.1	FORMACION ACADEMICA
	REQUISITOS: <ul style="list-style-type: none">- Un (01) Jefe de Proyecto:<ul style="list-style-type: none">- Ingeniero Titulado profesional en las carreras de Ingeniería informático o Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería de computación o Ingeniería de Redes y Comunicaciones.- Un (01) Especialista certificado en Redes<ul style="list-style-type: none">- Ingeniero Titulado las carreras de Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería Informática o ingeniera de redes y comunicación o Ingeniería en sistemas y computación.- Un (01) Especialista Seguridad perimetral<ul style="list-style-type: none">- Titulado o Bachiller en Ingeniería Electrónica y/o en Telecomunicaciones y/o en, Redes y/o Comunicaciones y/o Sistemas y/o en Tecnologías de la Información y/o en Cómputo y Sistemas y/o Informática y/o de Sistemas de Información o en Software o en TI y/o Sistemas y/o Ingeniería Empresarial y de Sistemas.- Un (01) Especialista en telefonía<ul style="list-style-type: none">- Técnico y/o bachiller y/o titulado en Ingeniería Electrónica y/o Electrónica y/o Telecomunicaciones y/o Sistemas y/o Redes y/o Comunicaciones de Datos y/o Sistemas y/o Informática y/o Computación y/o Sistemas de Información ACREDITACIÓN: <ul style="list-style-type: none">- El TÍTULO PROFESIONAL será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: http://www.titulosinstitutos.pe/, según corresponda.


DIRECCIÓN DE REDES INTEGRADAS
DE SALUD LIMA NORTE
Firmado digitalmente por RAFAEL



B.2.2	CAPACITACIÓN
	<p>REQUISITOS:</p> <ul style="list-style-type: none"> - Un (01) Jefe de Proyecto: <ul style="list-style-type: none"> - Certificación en ITIL. - Deberá contar con certificado PMP Vigente - Un (01) Especialista certificado en Redes <ul style="list-style-type: none"> - Deberá contar con certificado de nivel profesional en redes (routing y switching) de la marca de los equipos enrutadores propuesto por el postor. - Un (01) Especialista Seguridad perimetral <ul style="list-style-type: none"> - Deberá contar con certificado oficial vigente de la marca de seguridad perimetral propuesta a nivel técnico. <p>ACREDITACIÓN:</p> <ul style="list-style-type: none"> - Se acreditará con copia simple de constancia, certificados u otros documentos según corresponda.
B.2.3	EXPERIENCIA DEL PERSONAL CLAVE
	<p>REQUISITOS:</p> <ul style="list-style-type: none"> a) Un (01) Jefe de Proyecto: Tres (03) años de experiencia mínima como Jefe de Proyecto en servicio de telecomunicaciones, servicio TI y/o internet, transmisión de datos. b) Un (01) Especialista certificado en Redes Contar con experiencia mínima de dos (02) años en implementación de internet y/o datos y/o servicios de seguridad perimetral y/o seguridad en redes corporativas. c) Un (01) Especialista Seguridad perimetral Contar con experiencia mínima de dos (02) años en implementación y/o configuración y/o administración y/o gestión de soluciones en ciberseguridad y/o perímetro de la red d) Un (01) Especialista en telefonía Contar con experiencia mínima de dos (02) años en implementación y/o configuración de proyectos de telefonía y/o interconexiones de datos. <p>ACREDITACIÓN:</p> <p>LA EXPERIENCIA se validará mediante constancias y/o certificado de trabajo y/o contratos y su respectiva conformidad u otro documento que acredite fehacientemente la experiencia.</p>

C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p>Requisitos:</p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 5,000,000.00 (CINCO MILLONES Y 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 SERVICIOS DE TELECOMUNICACIONES, SERVICIOS DE INTERNET DEDICADO, INTERNET O DATOS IP O INTERNET Y/O TRANSMISIÓN DE DATOS O SERVICIO DE ACCESO A INTERNET Y/O SERVICIO DE INTERNET EN GENERAL Y/O SERVICIOS DE CONECTIVIDAD Y/O SERVICIO DE INTERCONEXION DE VOZ Y DATOS Y/O SERVICIOS DE TELECOMUNICACIONES EN GENERAL.</p> <p>Acreditación:</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</p>

cancelación en el mismo comprobante de pago¹⁰, correspondientes a un máximo de veinte (20) contrataciones.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

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

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

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

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

Importante

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

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".

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: $P_i = \frac{O_m \times PMP}{O_i}$ i = Oferta P_i = Puntaje de la oferta a evaluar O_i = Precio i O_m = Precio de la oferta más baja PMP = Puntaje máximo del precio [100] puntos

Importante

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

CAPÍTULO V PROFORMA DEL CONTRATO

Importante

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

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

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [.....], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO DE SELECCIÓN]** para la contratación de [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto [CONSIGNAR EL OBJETO DE LA CONTRATACIÓN].

CLÁUSULA TERCERA: MONTO CONTRACTUAL

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

Este monto comprende el costo del servicio, todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre la ejecución del servicio materia del presente contrato.

CLÁUSULA CUARTA: DEL 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.

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

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

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

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

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

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

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

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

CLÁUSULA SÉTIMA: GARANTÍAS

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

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

Importante

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

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

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.

Importante

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

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

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

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

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 32.3 del artículo

32 y artículo 36 de la Ley de Contrataciones del Estado, y el artículo 164 de su Reglamento. De darse el caso, LA ENTIDAD procederá de acuerdo a lo establecido en el artículo 165 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

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

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

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

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

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

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

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

CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO

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

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE 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.

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

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).

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° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.

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.

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 N° 2

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

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 5

PROMESA DE CONSORCIO

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

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO** N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO].

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

a) Integrantes del consorcio

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

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

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

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

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

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

TOTAL OBLIGACIONES

100%²²

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.

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

[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.



Importante para la Entidad

En caso de la prestación de servicios bajo el sistema a suma alzada incluir el siguiente anexo:

Esta nota deberá ser eliminada una vez culminada la elaboración de las bases

ANEXO N° 6

PRECIO DE LA OFERTA

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

Presente.-

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

CONCEPTO	PRECIO TOTAL
TOTAL	

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

Importante para la Entidad

- *En caso de procedimientos según relación de ítems, consignar lo siguiente:
"El postor puede presentar el precio de su oferta en un solo documento o documentos independientes, en los ítems que se presente".*
- *En caso de contrataciones que conllevan la ejecución de prestaciones accesorias, consignar lo siguiente:
"El postor debe detallar en el precio de su oferta, el monto correspondiente a la prestación principal y las prestaciones accesorias".*

Incluir o eliminar, según corresponda

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]
Presente.-

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP 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 período.

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 N° 216-2017/DTN "Considerando que la sociedad matriz y la sucursal constituyen la misma persona jurídica, la sucursal puede acreditar como suya la experiencia de su matriz". Del mismo modo, según lo previsto en la Opinión N° 010-2013/DTN, "... en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad incorporada o absorbida, que se extingue producto de la fusión; asimismo, si en virtud de la escisión se transfiere un bloque patrimonial consistente en una línea de negocio completa, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante podrá emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe".

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.

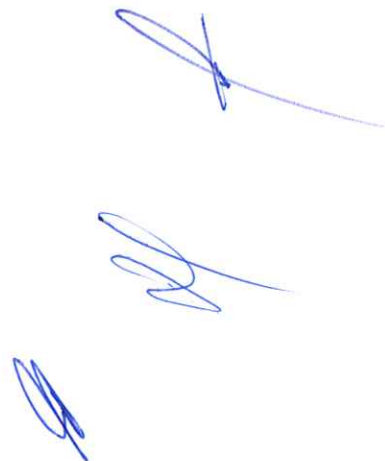
²⁸ Consignar en la moneda establecida en las bases.

DIRECCIÓN DE REDES INTEGRADAS DE SALUD LIMA NORTE
CONCURSO PÚBLICO N° 01-2025-DIRIS.LN/CS-1

N°	CLIENTE	OBJETO DEL CONTRATO	N° 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 N° 9

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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