

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

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



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

### SIMBOLOGÍA UTILIZADA:

N°	Símbolo	Descripción
1	[ABC] / [.....]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / [.....]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	<div>Importante</div> <div>• Abc</div>	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	<div>Advertencia</div> <div>• Abc</div>	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	<div>Importante para la Entidad</div> <div>• Xyz</div>	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

### CARACTERÍSTICAS DEL DOCUMENTO:

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

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

### INSTRUCCIONES DE USO:

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

Elaboradas en enero de 2019

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



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

**CONCURSO PÚBLICO N° 02-2023-UNT/CS**

### **BASES INTEGRADAS**

**“CONTRATACIÓN DE SERVICIO DE INTERNET PARA LA  
UNIVERSIDAD NACIONAL DE TRUJILLO Y FILIALES”**





## 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](http://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 Digitales<sup>1</sup>). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

#### Importante

- Los formularios electrónicos que se encuentran en el SEACE y que los proveedores deben llenar para presentar sus ofertas, tienen carácter de declaración jurada.
- En caso la información contenida en los documentos escaneados que conforman la oferta no

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



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

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

### 1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

#### Importante

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

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

### 1.9. EVALUACIÓN DE LAS OFERTAS

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

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

### 1.10. CALIFICACIÓN DE OFERTAS

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

### 1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

### 1.12. RECHAZO DE LAS OFERTAS

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



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

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

#### **1.13. OTORGAMIENTO DE LA BUENA PRO**

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

#### **1.14. CONSENTIMIENTO DE LA BUENA PRO**

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

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

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

##### **Importante**

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





## CAPÍTULO II SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

### 2.1. RECURSO DE APELACIÓN

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

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

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

#### Importante

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

### 2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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





### CAPÍTULO III DEL CONTRATO

#### 3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

#### 3.2. GARANTÍAS

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

##### 3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

##### 3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

En las contrataciones que conllevan la ejecución de prestaciones accesorias, tales como mantenimiento, reparación o actividades afines, se otorga una garantía adicional por una suma equivalente al diez por ciento (10%) del monto del contrato de la prestación accesoría, 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-emitar-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 : UNIVERSIDAD NACIONAL DE TRUJILLO  
RUC N° : 20172557628  
Domicilio legal : JR. DIEGO DE ALMAGRO NRO. 344 – TRUJILLO – TRUJILLO – LA LIBERTAD  
Teléfono: : 044-233250 / 044-233050  
Correo electrónico: : comitedeseleccion@unitru.edu.pe

### 1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto **LA CONTRATACIÓN DEL SERVICIO DE INTERNET PARA LA UNIVERSIDAD NACIONAL DE TRUJILLO Y FILIALES.**

### 1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante **FORMATO N° 02 SOLICITUD Y APROBACIÓN DEL EXPEDIENTE DE CONTRATACIÓN** con **APROBACIÓN N° 09-2023**, el 12 de junio del 2023.

### 1.4. FUENTE DE FINANCIAMIENTO

RECUSOS DIRECTAMENTE RECAUDADOS y/o 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 APLICA

### 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:

- Plazo de implementación del servicio: el tiempo de implementación de todo lo solicitado

se realizará como máximo en noventa (90) días calendario contados a partir del día siguiente de la firma de contrato.

- El plazo de duración del servicio: es de 730 días calendarios ~~o dos (2) años~~<sup>2</sup>. Contados a partir del día siguiente del acta de activación del servicio. En concordancia con lo establecido en el expediente de contratación.

### 1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/ 10.00 (Diez con 00/100 soles) en la caja de la entidad, sito en Jr. Diego de Almagro N° 344 o en las siguientes cuentas de la entidad

- **Financiera confianza**  
Cuenta de ahorros: 003021000187671001

- **Interbank**  
Cuenta Corriente: 6163001972909.

Y recabar el ejemplar de las bases en la oficina de abastecimiento de la Universidad Nacional de Trujillo, Sito en Jr. Diego de Almagro N° 344-Trujillo.

#### Importante

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

### 1.10. BASE LEGAL

- Ley N° 31638, Ley de Presupuesto del Sector Público para el Año Fiscal 2023.
- Ley N° 31639, Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2023.
- Ley N° 30225, Ley de Contrataciones del Estado.
- Decreto Supremo N° 082-2019-EF, que aprueba el Texto Único Ordenado de la Ley N° 30225, Ley de Contrataciones del Estado.
- Decreto Supremo N° 344-2018-EF, que aprueba el Reglamento de la Ley de Contrataciones del Estado, modificado por el Decreto Supremo N° 168-2020-EF y por el Decreto Supremo N° 162-2021-EF.
- Ley N° 27444, Ley de Procedimiento Administrativo General.
- Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública.
- Ley N° 30220, Ley Universitaria.

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

<sup>2</sup> Texto suprimido en virtud a la consulta y/u observación N° 05; 150, 151, 235 y 260 respectivamente.



## CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

### 2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

#### Importante

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

### 2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos<sup>3</sup>, la siguiente documentación:

#### 2.2.1. Documentación de presentación obligatoria

##### 2.2.1.1. Documentos para la admisión de la oferta

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

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

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

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

#### Advertencia

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

- c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. (**Anexo N° 2**)
- d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo N° 3**)

<sup>3</sup> La omisión del índice no determina la no admisión de la oferta.

<sup>4</sup> 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) DOCUMENTACIÓN QUE SERVIRÁ PARA ACREDITAR EL CUMPLIMIENTO DE ALGÚN COMPONENTE DE LOS TÉRMINOS DE REFERENCIA QUE LA ENTIDAD CONSIDERE PERTINENTE.

- Carta emitida por el Fabricante del Equipo de la Solución de Protección AntiDDoS en nube indicando que se encuentra con soporte activo del fabricante.
- Carta de Acreditación de Vigencia Tecnológica, emitida por el Fabricante del Equipo de la Solución de Seguridad Perimetral contra Intrusos Dedicado.
- Carta de Acreditación de Vigencia Tecnológica y cumplimiento de especificaciones técnicas, emitida por el Fabricante del Equipo de la Solución de Seguridad Perimetral en alta disponibilidad.
- Carta de Acreditación de Vigencia Tecnológica y cumplimiento de especificaciones técnicas, emitida por el Fabricante del Equipo de la Solución de detección y respuesta de red para brechas de amenazas.
- Link de plataforma web que permita administrar los registros DNS o procedimiento de atención de solicitudes de modificación o registros de dominios<sup>5</sup>
- Diagrama topológico y direcciones donde se ubican los servidores DNS.
- Constancia de experiencia en gestión de incidentes de ciberseguridad (Certificado de Membresía emitido por el FIRST para el 2023)<sup>6</sup>.
- Constancia o link público que acredite la conexión igual o superior a 100 Gbps al NAP Perú.
- Carta del fabricante que certifique que los equipos propuestos para la solución de seguridad perimetral en alta disponibilidad no están en end-of-life o end-of-sale o end-of-support o similares<sup>7</sup>

f) Declaración jurada de plazo de prestación del servicio. (Anexo N° 4)<sup>8</sup>

g) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (Anexo N° 5)

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

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

**Importante**

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

**2.2.1.2. Documentos para acreditar los requisitos de calificación**

Incorporar en la oferta los documentos que acreditan los “Requisitos de Calificación” que se detallan en el numeral 3.2 del Capítulo III de la presente sección de las bases.

<sup>5</sup> Texto agregado en virtud a la consulta y/u observación N° 12 y 177 respectivamente.

<sup>6</sup> Texto agregado en virtud a la consulta y/u observación N° 07 y 172 respectivamente.

<sup>7</sup> Texto agregado en virtud a la consulta y/u observación N° 246.

<sup>8</sup> 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.



2.2.2. **Documentación de presentación facultativa:**

**Importante para la Entidad**

- En caso el comité de selección considere evaluar otros factores además del precio, incluir el siguiente literal:
- 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.
- Si durante la fase de actos preparatorios, las Entidades advierten que es posible la participación de proveedores que gozan del beneficio de la exoneración del IGV prevista en la Ley N° 27037, Ley de Promoción de la Inversión en la Amazonía, consignar el siguiente literal:
- b) Los postores que apliquen el beneficio de la exoneración del IGV previsto en la Ley N° 27037, Ley de Promoción de la Inversión en la Amazonía, deben presentar la Declaración Jurada de cumplimiento de condiciones para la aplicación de la exoneración del IGV (Anexo N° 7).
- En el caso de procedimientos por relación de ítems cuando la contratación del servicio en general va a ser prestado fuera de la provincia de Lima y Callao y el monto del valor estimado de algún ítem no supere los doscientos mil Soles (S/ 200,000.00), consignar el siguiente literal:
- c) En el [CONSIGNAR EL ÍTEM O ÍTEMS, SEGÚN CORRESPONDA, EN LOS QUE SE PUEDE SOLICITAR LA BONIFICACIÓN] los postores con domicilio en la provincia donde se prestará el servicio, o en las provincias colindantes, sean o no pertenecientes al mismo departamento o región, pueden presentar la solicitud de bonificación por servicios prestados fuera de la provincia de Lima y Callao, según Anexo N° 10.
- En caso de procedimientos de selección por relación de ítems cuando el monto del valor estimado de algún ítem corresponda al monto de una Adjudicación Simplificada, se incluye el siguiente literal:
- Ítem N° [...]
- d) Solicitud de bonificación del cinco por ciento (5%) por tener la condición de micro y pequeña empresa (Anexo N°11).

Incorporar a las bases o eliminar, según corresponda.

**Advertencia**

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

2.3. **REQUISITOS PARA PERFECCIONAR EL CONTRATO**

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

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



- f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.

#### Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE<sup>9</sup> 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 comunicación <sup>10</sup>(Anexo N° 12).  
i) Detalle de los precios unitarios del precio ofertado<sup>11</sup>.  
j) Estructura de costos<sup>12</sup>.  
k) ~~Detalle del precio de la oferta de cada uno de los servicios que conforman el paquete<sup>13</sup>.~~  
l) Detalle de las opciones de atención de averías o fallas<sup>14</sup>

#### 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.

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/>

<sup>10</sup> En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

<sup>11</sup> Incluir solo en caso de la contratación bajo el sistema a suma alzada.

<sup>12</sup> Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.

<sup>13</sup> Incluir solo en caso de contrataciones por paquete.

<sup>14</sup> Texto agregado en virtud a la consulta y/u observación N° 164



**Importante para la Entidad**

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

- m) [DE ACUERDO AL OBJETO CONTRACTUAL CONVOCADO REQUERIR LA PRESENTACIÓN DE OTROS DOCUMENTOS, SEGÚN CORRESPONDA].

*Incorporar a las bases o eliminar, según corresponda.*

**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 Haya<sup>15</sup>.*
- *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 la **Unidad de Abastecimientos, Sito en Jr. Diego de Almagro N° 344-Trujillo - Trujillo - La Libertad** de lunes a viernes de 07:00 am a 14:45 pm

**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. ADELANTOS<sup>16</sup>**

La entidad no otorgara adelantos.

**2.6. FORMA DE PAGO**

La Entidad realizará el pago de la contraprestación pactada a favor del contratista de manera mensual, luego de la conformidad del servicio por parte de la oficina de tecnologías de información de la UNT.

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

- Informe del funcionario responsable de la oficina de Tecnologías de la Información de la Universidad Nacional de Trujillo emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago remitido a [logistica.mesadepartes@unitru.edu.pe](mailto:logistica.mesadepartes@unitru.edu.pe)

<sup>15</sup> Según lo previsto en la Opinión N° 009-2016/DTN.

<sup>16</sup> Si la Entidad ha previsto la entrega de adelantos, debe prever el plazo en el cual el contratista debe solicitar el adelanto, así como el plazo de entrega del mismo, conforme a lo previsto en el artículo 156 del Reglamento.



Dicha documentación se debe presentar en la **Unidad de Abastecimientos**, sito en **Jr. Diego de Almagro N° 344 – Trujillo – Trujillo – La Libertad**.

### 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. TÉRMINOS DE REFERENCIA

#### TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DEL SERVICIO DE INTERNET PARA LA UNIVERSIDAD NACIONAL DE TRUJILLO Y FILIALES

##### I. TÉRMINOS DE REFERENCIA

##### 1.1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de internet para la universidad nacional de Trujillo y filiales

##### 1.2. FINALIDAD PÚBLICA

El presente proceso busca cumplir con una condición básica de calidad impuesto por La Superintendencia Nacional de Educación Superior Universitaria (SUNEDU) dentro del licenciamiento universitario, el cual se describe dentro del indicador 24: ***“Disponibilidad de Internet en los ambientes que brinden el servicio educativo de todos sus locales. El servicio de Internet debe contar con banda ancha requerida para la educación superior universitaria, conforme a lo establecido por el órgano competente y de acuerdo a la disponibilidad del servicio de telecomunicaciones en la región.”***; del mismo modo se busca brindar el acceso a toda la comunidad universitaria (alumnos, docentes, personal administrativo) a los sistemas de información (investigación, enseñanza, gestión académica y administrativa) a través de la interconexión de las sedes desconcentradas, esto también requerido como una condición básica de calidad por la SUNEDU dentro del indicador número 4.

##### 1.3. ANTECEDENTES

La Oficina de Tecnologías de la Información (Ex Dirección de sistemas y comunicación – DSC) como parte de los órganos de gestión que planifican, organizan, dirigen y controlan los procesos estratégicos de la Universidad; coordinan y toman decisiones orientadas al logro de objetivos institucionales, con criterios de eficiencia y eficacia, para dar soporte a la Alta Dirección de la Universidad; está obligada a garantizar el funcionamiento y la disponibilidad de la plataforma tecnológica, así como al cumplimiento de normativas en cuanto a materia de tecnología emitidas por los organismos del estado peruano, como por ejemplo la Ley N° 30035, que regula el repositorio nacional digital de ciencia, tecnología, e innovación de acceso abierto; las normas técnicas peruanas, ley de gobierno digital, condiciones básicas de calidad para el licenciamiento universitario, entre otras; para esto se hace imprescindible contar con el servicio de internet.

En el año 2018, Oficina de Tecnologías de la Información (Ex Dirección de sistemas y comunicación – DSC), realizó el contrato de servicio de internet, en el cual se adquirió un ancho de banda de 2.5 Gbps, se interconectó mediante fibra oscura el local central y facultad



de medicina; mediante enlaces privados de fibra óptica las sedes de Moche y el valle Jequetepeque, soluciones wifi para la facultad de medicina y la biblioteca central; asimismo, se logró adquirir soluciones de optimización de ancho de banda, Switching capa 3 y seguridad perimetral; donde la solución Switching capa 3 pasó a formar parte de los activos de la universidad.

Por tanto, para este año se espera continuar con una capacidad similar de ancho de banda, con la interconexión de todas las sedes desconcentradas de LA UNIVERSIDAD NACIONAL DE TRUJILLO, y la renovación de la solución de Switching capa 3 que pasará a formar parte de los activos de la universidad, y mejorar algunos servicios para la seguridad informática de nuestro centro de datos.

#### 1.4. OBJETIVOS DE LA CONTRATACIÓN

##### 1.4.1. Objetivo General:

- Contratar el servicio de internet para atender los requerimientos académicos y administrativos de la comunidad universitaria en todas las filiales de la universidad.

##### 1.4.2. Objetivos específicos:

- Cumplir con los requisitos de condición básica de calidad, como parte del licenciamiento universitario, y, de acuerdo a las normas regulatorias vigentes emitidas por el Ministerio de transportes y telecomunicaciones y el OSIPTEL (Decreto ley 26096 – Ley de telecomunicaciones y demás normas vigentes).
- Brindar el acceso a los sistemas de información a toda la comunidad universitaria en las distintas sedes.
- Proveer a los sistemas de información de la universidad, con equipos y herramientas de seguridad a fin de mantener la integridad, disponibilidad, confidencialidad de la información sensible.

#### 1.5. SISTEMA DE CONTRATACIÓN:

- Suma alzada

#### 1.6. ALCANCE Y DESCRIPCIÓN DEL SERVICIO

##### 1.6.1. ALCANCE DEL SERVICIO

##### 1.6.1.1. SERVICIO DE INTERNET

- El contratista deberá brindar Enlace a internet dedicado con un ancho de banda de 2.6 Gbps; este enlace deberá ser simétrico y con un Overbooking 1:1.
- El protocolo de transporte del Backbone del Contratista debe ser MPLS y/o metro Ethernet.
- El contratista deberá contar con salidas internacionales 100% fibra óptica, de al menos dos enlaces de 10 Gbps, con 2 proveedores TIER 1 como mínimo.
- El servicio de acceso dedicado a internet deberá contar con una alta disponibilidad en modo activo – pasivo. El enlace de contingencia se activará en caso de avería física del router o avería en la última milla del enlace principal. El enlace de contingencia deberá tener el mismo ancho de banda del enlace principal. Cabe señalar que se considerará como indisponibilidad del servicio cuando se tenga la afectación en ambos enlaces (enlace principal y contingencia).
- Los enlaces de internet principal y contingencia para el campus universitario deberán venir de puntos de presencia distintos del contratista y a través de rutas diferentes hasta el ingreso de la universidad, donde podrán compartir el mismo recorrido; Tanto para el enlace principal como para el enlace de contingencia el recorrido de la fibra óptica podrá ser canalizado y/o aéreo; Cabe resaltar que en cualquier momento la entidad puede inspeccionar el recorrido de la última milla del proveedor.
- Se entiende por puntos de presencia, al espacio geográfico donde el proveedor cuenta con energía y equipos de comunicaciones.
- El protocolo de comunicación será TCP/IP, deberá tener disponibilidad de protocolo de ruteo IPV4 / IPV6
- Un mínimo de 56 direcciones IPv4 públicas y un mínimo 256 direcciones en IPv6, dentro de las cuales no deberán estar el IP del router, el IP de la red, el IP del broadcast e IP de alta disponibilidad, y serán configuradas en coordinación con el área de Sistemas de Universidad Nacional de Trujillo.





- El contratista debe tener redundancia de servidores DNS en arreglos de alta disponibilidad y en sitios geográficamente diferentes, deben ubicarse en departamentos distintos<sup>17</sup> deberá indicar como parte de la oferta las direcciones donde se ubican los servidores DNS. Para lo cual se deberá presentar un diagrama topológico en la oferta del postor.
- El proveedor deberá proveer de una aplicación o plataforma web que permita administrar los registros DNS de los dominios que la Universidad Nacional de Trujillo administra. En caso el proveedor no permita administrar los registros DNS a través de una aplicación o plataforma web deberá garantizar una atención a las solicitudes de modificación o registro de dominios en un tiempo no mayor a quince (15) minutos desde generado el ticket de atención por el proveedor y se deberá de ver reflejado en los DNS como máximo en un plazo de 6 horas desde la generación del ticket. presentar un procedimiento de atención de estas solicitudes de modificación o registros de dominios y que podrán ser a través de una notificación vía correo electrónico y/o el canal de atención que brinde el postor y la recepción del requerimiento será hasta de 30 minutos en horario de atención de Lunes a Viernes de 08:00 a 16:00 y deberá reflejar los cambios hasta 24 horas después de generado el ticket o notificación vía correo electrónico y/o el canal de atención que brinde el postor<sup>18</sup>.
- Para realizar la conexión el Contratista deberá proveer un equipo router de propósito dedicado, de primer uso y con vigencia tecnológica de una marca de prestigio internacional. El fabricante del equipo router deberá haber estado listado como líder o retador en al menos tres (03) reportes de los últimos tres años del cuadrante mágico de Gartner en la categoría de Edge Routing y/o deberá soportar la integración con una arquitectura SD-WAN del mismo fabricante de manera nativa. El equipo será otorgado en calidad de alquiler y demás accesorios necesarios para realizar la conexión a internet.
- El contratista deberá ser miembro activo del NAP Perú, con conexión igual o superior a los 100 Gbps y con infraestructura propia o arrendada a terceros.
- El contratista deberá contar una base técnica y personal supervisor de planta externa propio en su planilla que pertenezca a la zona con la finalidad de poder cumplir con los SLAs indicados, esto se garantizará a través de una declaración jurada en momento de presentar la oferta.
- El proveedor deberá otorgar una herramienta de monitoreo de red, a la cual se accederá a través de un navegador web, mediante las respectivas credenciales de acceso.
- La Universidad para validar el servicio de internet (principal y contingencia) realizará pruebas de conectividad y navegación a páginas web externas. Complementariamente, el proveedor deberá entregar un informe, al final de la implementación, de saturación de ancho de banda realizado con un equipo generador de tráfico de red, para lo cual la entidad brindará las facilidades para el tiempo que conlleven dichas pruebas, dando conformidad y entregando al contratista el acta de inicio de operaciones mediante un documento formal.
- Los POPs/nodos, última milla y toda la infraestructura de la red core y transporte (equipamiento del Contratista ubicado en sus PoP/nodos, tales como equipos de acceso L3 y transporte) utilizadas para provisionar el servicio de internet por ambos enlaces debe ser de propiedad del postor, es decir no tercerizada o subcontratada.<sup>19</sup>

#### 1.6.1.2. SERVICIO DE TRANSMISIÓN DE DATOS

- El contratista debe brindar el servicio de transmisión de datos Full Mesh entre las sedes de la Universidad Nacional de Trujillo hacia la sede principal, detalladas a continuación:

TABLA N° 01. SEDES UNT

N°	SEDE	DIRECCIÓN	COORDENADAS APROX.	ANCHO DE BANDA MÍNIMO	MEDIO
1	Ciudad Universitaria, Pabellón de matemáticas (Sede principal)	Av. Juan Pablo II S/N Urb. San Andrés I Etapa (Ciudad Universitaria) – Trujillo	8°06'49.3"S 79°02'18.1"W	1150 Mbps	FO

<sup>17</sup> Texto agregado en virtud a la consulta y/u observación N° 175

<sup>18</sup> Texto suprimido y agregado en virtud a la consulta y/u observación N° 12 y 177 respectivamente.

<sup>19</sup> Texto agregado en virtud a la consulta y/u observación N° 173 y 185 respectivamente.



2	Facultad de Medicina	Jr. Salaverry N° 545	8°06'24.4"S 79°02'10.0"W	200 Mbps	FO
3	Local Central	Jr. Diego de Almagro 344	8°06'42.3"S 79°01'49.3"W	400 Mbps	FO
4	Ciudad Universitaria Guadalupe	Carre. Panamericana Norte Km. 693 - Guadalupe	7°14'12.0"S 79°27'29.6"W	200 Mbps	FO
5	Clínica Estomatológica de Moche	Ca. Elias Aguirre 560	8°10'14.0"S 79°00'21.0"W	50 Mbps	FO
6	Dirección de Planificación	Jr. Zepita N° 482	8°6'33.91"S 79°1'26.31"W 8° 6'33.89"S 79° 1'49.95"W <sup>20</sup>	100 Mbps	FO
7	Consultorio jurídico gratuito	Av. España 2122 Trujillo	8°6'33.91"S 79°1'26.31"W 8° 6'49.16"S 79° 1'26.30"W <sup>21</sup>	50 Mbps	FO
8	Campus Universitario Santiago de Chuco	Av. Universitaria S/N	8°08'23.0"S 78°10'24.7"W	50 Mbps	FO
9	Campus Universitario Huamachuco	Centro Poblado Huamachuco – Vía Universitaria	7°49'44.0"S 78°03'14.8"W	100 Mbps	FO

- El contratista del servicio debe garantizar una transmisión segura, íntegra y confiable de la voz, video y datos desde las sedes remotas hacia la sede principal, considerando como factor crítico en el transporte de la información, una trayectoria privada separada de la red pública de internet.
- Los routers a colocar en las sedes remotas deberán ser hardware de propósito dedicado. No se aceptarán firewalls o dispositivos cuya función principal no sea el enrutamiento de paquetes IP. El fabricante del equipo router deberá haber estado listado como líder o retador en al menos tres (03) reportes de los últimos tres años del cuadrante mágico de Gartner en la categoría de Edge Routing y/o deberá soportar la integración con una arquitectura SD-WAN del mismo fabricante de manera nativa.
- El contratista no podrá emplear el internet como medio de transporte para la interconexión de las sedes. No se aceptará una solución basada en túneles a través de internet.
- El protocolo de transporte del Backbone del Contratista debe ser MPLS y/o metro Ethernet.
- Para la sede principal, se requiere un enlace principal y contingencia y deberán venir de puntos de presencia distintos del contratista y a través de rutas diferentes hasta el ingreso de la universidad, donde podrán compartir el mismo recorrido; Tanto para el enlace principal y el enlace de contingencia el recorrido de la fibra óptica podrá ser canalizado y/o aéreo; Cabe resaltar que en cualquier momento la entidad puede inspeccionar el recorrido de la última milla del proveedor.
- Se podrá hacer uso de los mismos recursos de planta externa (Fibra óptica) del enlace de Internet.
- El proveedor deberá otorgar una herramienta de monitoreo de red, a la cual se accederá a través de un navegador web, mediante las respectivas credenciales de acceso.
- Se entiende por puntos de presencia, al espacio geográfico donde el proveedor cuenta con energía y equipos de comunicaciones.
- Para las líneas de transmisión de datos se debe considerar configuración de clases de servicio (CoS) de los equipos. Las clases de servicio se da en el siguiente orden de prioridad:

<sup>20</sup> Texto suprimido y agregado en virtud a la consulta y/u observación N° 496

<sup>21</sup> Texto suprimido y agregado en virtud a la consulta y/u observación N° 496



Voz/Video, Datos Críticos y Datos no Críticos; los valores de ancho de banda por cada tipo de tráfico a priorizar en las configuraciones de CoS se coordinarán conjuntamente con personal encargado de la Universidad Nacional de Trujillo, los cuales deberán soportar y garantizar adecuadamente una comunicación a nivel de Voz, Video y Datos.

- Los circuitos privados no deberán ser filtrados por la empresa contratista del servicio.
- La Universidad Nacional de Trujillo (UNT) proporcionará espacio en los gabinetes de comunicaciones para alojar los equipos que serán instalados por el contratista, así como brindar la energía adecuada (monofásica 220v, estabilizada y con puesta a tierra) para dichos equipos, esto refiriéndonos a las sedes 1, 2, 3, 5, 6 y 9 de la TABLA N° 01. SEDES UNT; para las sedes 4, 7, 8 el contratista deberá instalar un gabinete de 12 RU por sede, y deberá extender la acometida eléctrica más cercana para energizar a los equipos que serán alojados en estos gabinetes, la distancia promedio de la acometida eléctrica más cercana es de 20 metros y la más lejana de 40 metros; la Universidad se encargará de proporcionar los ambientes donde serán instalados estos gabinetes. En caso la estructura no permita realizar obra civil para enterrado de ducterías, se aceptará ducterías/canalizado superpuesto en conformidad con la norma TIA/EIA-569-A. Todos los ambientes son de material de concreto y ladrillo y se encuentran en espacios interiores y estarán libres al realizar la implementación, asimismo mencionar que, la universidad ya cuenta con energía estabilizada y pozo a tierra en cada una de sus sedes y proveerá el sistema de respaldo UPS para cada gabinete.
- Los POPs/nodos, última milla y toda la infraestructura de la red core y transporte (equipamiento del Contratista ubicado en sus PoP/nodos, tales como equipos de acceso L3 y transporte) utilizadas para provisionar el servicio de internet por ambos enlaces debe ser de propiedad del postor, es decir no tercerizada o subcontratada.<sup>22</sup>

#### 1.6.1.3. De la herramienta de monitoreo de enlace de internet y sedes remotas

El postor deberá incluir como parte de su oferta una herramienta web (HTTP) de monitoreo de los enlaces con las siguientes características:

- Debe permitir el monitoreo del desempeño de cada router, debe mostrar en una pantalla resumen: alarmas recientes, disponibilidad, tiempo de respuesta, pérdida de paquetes. Asimismo, deberá presentar gráficas de utilización de CPU, utilización de memoria y buffer.
- Soporte de visualización de la red usando la integración de Google Maps.
- Opcionalmente, deberá incluir el módulo Vista 3D
- Soporte NetFlow (version 5, 7 y 9), jFlow, sFlow, cFlow. Soporte NBAR.
- Tráfico: Presentación del volumen, velocidad, utilización y paquetes, en presentación gráfica de tiempo y permita la generación del Informe de Planificación de Capacidad. Las mediciones deben actualizarse a 1, 5 o 10 minutos y las cuales deben ser configurables por el usuario.
- Aplicaciones: Presentación de la distribución gráfica de las aplicaciones en el tiempo permitiendo tener la visibilidad de hasta 500 aplicaciones por página.
- Visibilidad del Consumo de Ancho de Banda diferenciado por tipo de tráfico (mínimo tres Clases de Servicio) para todos los enlaces de datos.
- La herramienta de Monitoreo debe permitir el almacenamiento de la data histórica durante el periodo de contrato.
- Debe permitir crear diagramas topológicos detallados de la Red en tiempo real, al menos al minuto. La solución debe recopilar la información de los equipos descubiertos por SNMP capturando como mínimo: Dirección IP, Marca, Modelo y debe permitir exportar esta información del inventario de los equipos descubiertos en un archivo Excel/PDF. Asimismo, debe permitir documentar la información recopilada y deberá exportarla en un archivo PDF.
- La solución de monitoreo debe incluir un módulo de Capacity Planning que permita lo siguiente:
  - El Software de Monitoreo debe permitir Reportes en Tiempo Real con granularidad de 1 minuto para muestreos de intervalos de 24 horas a fin de detectar tráfico anómalo, aplicaciones, conversaciones, Top Senders y Top Receivers.

<sup>22</sup> Texto agregado en virtud a la consulta y/u observación N° 173.



- El Software de Monitoreo debe permitir tener granularidad de al menos 1 minuto para la data almacenada en la base de datos que debe ser incluida y para el periodo de al menos de 1 año con el objetivo de tener reportes granulares y realizar comparativos mensuales para el sustento y planificación de la capacidad.

#### 1.6.1.4. SERVICIO CONTRA ATAQUES DE NEGACIÓN DE SERVICIO ANTI-DDoS

El postor debe ofertar una solución en nube o cloud del servicio de Anti-DDoS, es decir desplegada dentro de la red del operador y dentro del territorio nacional, considerando que el ataque debe quedar en la plataforma del operador y no afectar el ancho de banda de internet contratado por la entidad.

Las características que debe cumplir el servicio son:

- La solución deberá ser de tipo appliance, de tecnología específica para la mitigación de ataques de denegación de servicios, no se aceptarán soluciones en las que la protección DDoS sea una funcionalidad adicional de equipos Firewall, Next Generation Firewalls, Application Delivery Controllers, Routers u otros equipos de seguridad o redes
- La solución en la nube desplegada en la red nacional del proveedor de servicios de internet deberá proteger el peer a Internet del proveedor, de manera que el tráfico malicioso sea derivado y mitigado lo más cercano a la entrada de la red del postor se aceptará una arquitectura always on tanto para la mitigación, como para la derivación.<sup>23</sup>
- Opcionalmente<sup>24</sup>, el tráfico debe ser derivado para su limpieza solo cuando se necesite, (es decir, ante un ataque) finalizada la inspección el tráfico limpio debe ser reinyectado a la red del proveedor de internet para continuar con la ruta a la red de la entidad, esto se requiere con el fin evitar congestión de red, puntos de fallo que puedan degradar la performance de la red y servicios de la entidad.
- Capacidad de throughput inspección del 20 Gbps y mitigación incluida debe ser de al menos 5 Gbps de tráfico.
- Capacidad de informar la cantidad de tráfico malicioso bloqueado, en ~~bps~~ kbps o Mbps<sup>25</sup>, durante una mitigación activa en la nube.
- Capacidad de informar la cantidad de tiempo que una mitigación de nube lleva ejecutándose.
- La solución debe incluir la protección contra ataques de denegación de servicio a nivel de aplicación sin estados (stateless), por lo que no deberá tener límite de conexiones ni de sesiones concurrentes para el tráfico total (Incluyendo tráfico atacante). ~~No se aceptarán soluciones "always-on" para este componente.~~<sup>26</sup>
- El proveedor del servicio brindará reportes mensuales dentro de los 10 días del siguiente mes sobre el servicio de protección DDoS.
- El postor deberá indicar en su oferta una descripción del equipamiento asociado a esta solución e incluir una carta del fabricante indicando que la solución implementada para brindar el servicio Anti-DDoS se encuentra con soporte activo del fabricante.

#### 1.6.1.5. SOLUCIÓN DE PROTECCIÓN CONTRA INTRUSOS DEDICADO EN EL PERIMETRO

Adquisición de una solución de protección de contra intrusos dedicado en el perímetro (IPS). La solución tiene que ser ofrecida mediante la instalación de un equipo físico, específico y dedicado.

Para efectos de la propuesta el equipo ofertado deberá ser nuevo, de primer uso, no se admitirán equipos refurbished o de re-uso, asimismo, el equipo ofertado no podrá estar listado ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support o similares al momento de la presentación de la oferta<sup>27</sup>. Se deberá adjuntar el link público o carta del fabricante que verifique que el modelo propuesto no está en ese listado.

<sup>23</sup> Texto agregado en virtud a la consulta y/u observación N° 24.

<sup>24</sup> Texto agregado en virtud a la consulta y/u observación N° 23.

<sup>25</sup> Texto suprimido y agregado a la consulta y/u observación N° 26.

<sup>26</sup> Texto suprimido en virtud a la consulta y/u observación N° 27.

<sup>27</sup> Texto agregado en virtud a la consulta y/u observación N° 190



Características generales de la solución:

- La solución no debe tener chips específicos de aplicación del tipo ASIC que no permitan futuras expansiones de firmware y características en el mismo hardware. La solución debe basarse en una arquitectura de procesamiento paralelo y no debe usar chips ASIC de propiedad exclusiva.
- La solución propuesta debe ser con factor de forma 1U (opcional)<sup>28</sup>.
- La solución propuesta debe tener al menos ~~dos puertos USB~~<sup>29</sup> 01 puerto USB y un 2do puerto USB (opcional)<sup>30</sup>, 1 puerto de administración, 1 puerto de consola y 2 puertos para Alta Disponibilidad.
- La solución propuesta debe tener al menos 8 puertos Gigabit Ethernet fijos de los cuales al menos 2 puertos deben soportar la funcionalidad bypass y 4 x SFP+ 10GE.
- La solución propuesta debe tener al menos dos ranuras para los módulos de IO de extensión.
- La solución propuesta debe soportar puertos 2 x QSFP+ en módulo de extensión.
- La solución deberá incluir los transceivers de la marca, necesarios para la conectividad entre los equipos componentes de la solución.
- La solución propuesta debe soportar al menos 1T de espacio de almacenamiento.
- La solución propuesta debe soportar el rendimiento de 24 Gbps IPS
- La solución propuesta debe admitir sesiones simultáneas de 12M.
- La solución propuesta debe admitir 300,000 nuevas sesiones / segundo bajo tráfico TCP.
- La solución propuesta debe admitir fuente de poder redundante.

SERVICIOS DE RED

- La solución propuesta debe ser capaz de operar en modalidad capa 3 (enrutamiento), modalidad en línea (bridge) y capa 2 (port mirroring) de forma simultánea (sin necesidad de virtualizar el equipo)

CONTROL DE APLICACIONES

- La solución debe admitir la identificación de la IP del EndPoint, la cantidad, el tiempo en línea, el tiempo fuera de línea.
- La solución debe admitir más de 3,000 aplicaciones, debe admitir el filtro de aplicaciones por nombre, categoría, subcategoría, tecnología (opcional)<sup>31</sup> y riesgo (opcional)<sup>32</sup>.
- La solución debe ser compatible para reconocer aplicaciones IPv6.
- La solución debe admitir la identificación de aplicaciones para el tráfico cifrado SSL.
- La solución debe ser compatible para identificar aplicaciones móviles de Android, iOS.
- La solución debe admitir la visualización de la descripción, los factores de riesgo, las dependencias, los puertos típicos utilizados y las URLs para obtener referencias adicionales, y la información para cada aplicación en su WebUI.
- La solución debe ser compatible con el bloqueo, reinicio de sesión, monitoreo y traffic shaping para las aplicaciones.
- La solución debe ser capaz de identificar y controlar las aplicaciones en la nube, debe proporcionar monitoreo y estadísticas multidimensionales para las aplicaciones en la nube, incluyendo la categoría de riesgo y las características.

DETECCION DE INTRUSOS

- La solución debe soportar más de 8000 firmas. Debe admitir firmas personalizadas, actualizaciones automáticas de inserción o extracción de firmas y una enciclopedia de amenazas integrada.
- La solución debe ser compatible con la prevención de intrusiones para el tráfico cifrado SSL.

<sup>28</sup> Texto agregado en virtud a la consulta y/u observación N° 274.

<sup>29</sup> Texto suprimido en virtud a la consulta y/u observación N° 275 y 472 respectivamente.

<sup>30</sup> Texto agregado en virtud a la consulta y/u observación N° 472.

<sup>31</sup> Texto agregado en virtud a la consulta y/u observación N° 32.

<sup>32</sup> Texto agregado en virtud a la consulta y/u observación N° 32.



- La solución debe ser compatible con la protección del entorno IPV6.
- La solución debe ser compatible con la protección de la inyección SQL, los ataques CC y XSS.
- (opcional)<sup>33</sup> la solución debe ser compatible con la verificación de enlace externo (external link check)
- La solución debe ser compatible con la protección contra ataques CC con límite de solicitud, límite de proxy, umbral personalizado, métodos amigables con los rastreadores. Admite 4 métodos de autenticación: JS Cookie, Redirect, Access confirm, CAPCHA
- La solución debe admitir la detección de anomalías de protocolo, la detección basada en la velocidad o Ratio<sup>34</sup>
- La solución debe admitir las siguientes acciones de IPS: predeterminado, monitor, bloqueo, restablecimiento (IP de los atacantes o IP de la víctima, interfaz de entrada) con tiempo de caducidad
- La solución debe ser compatible con la opción de registro de paquetes.
- La solución debe ser compatible con el perfil de seguridad IPS según la gravedad, el destino, el sistema operativo, la aplicación o el protocolo.
- La solución debe ser compatible con la prevención de intrusiones para HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS etc.
- La solución debe ser compatible para verificar protocolos del tipo HTTP Get, Head, Put, Post.
- La solución debe admitir la exención de IP de firmas IPS específicas.
- La solución debe ser compatible con el modo de operación de IDS sniffer.
- La solución debe ser compatible con la configuración predefinida de perfiles IPS.
- La solución debe ser compatible con la creación de firmas IPS definidas por el usuario.
- La solución propuesta debe ser compatible con detección de la reputación de IP y el bloqueo de IP del servidor de botnet con la base de datos de reputación de IP global.
- La solución propuesta debe admitir una descripción detallada de los perfiles IPS predefinidos.
- La solución debe soportar el registro de amenazas IPv6: soporte para capturar y descarga de paquetes IPv6
- Los detalles de amenazas admiten URI y decodificación de datos de ataque
- Admite la detección de anomalías de protocolo para HTTP / DNS / FTP / MSRPC / POP3 / SMTP / SUNRPC y Telnet

#### ALTA DISPONIBILIDAD

- La solución debe ser compatible con los modos Activo / Activo y Activo / Pasivo
- La solución debe admitir interfaces heartbeat redundantes para HA
- La solución debe ser compatible con la conmutación por error de HA:
  - Monitoreo de puertos.
  - Failover de estado
  - Sub-segundo de conmutación por error.
  - Notificación de error.
- La solución debe admitir las siguientes opciones de implementación de HA:
  - HA con agregación de enlaces
  - HA de malla completa
  - HA geográficamente disperso
- La solución debe admitir la funcionalidad Bypass en un entorno de HA de dos capas.
- La solución debe soportar la función de Bypass del hardware de la interfaz.
- La solución debe ser compatible con la sincronización de sesión independiente.
- La solución debe ser compatible con la interfaz de gestión de HA reservada.

#### ADMINISTRACION LOGS Y REPORTES

- La solución debe ser compatible con la interfaz de usuario web integrada (WebUI) y la interfaz de línea de comandos (CLI)

<sup>33</sup> Texto agregado en virtud a la consulta y/u observación N° 280 y 467 respectivamente.

<sup>34</sup> Texto agregado en virtud a la consulta y/u observación N° 193 y 194 respectivamente.



- La solución debe admitir el acceso de administración desde HTTP / HTTPS, SSH, telnet, consola
- La solución debe ser compatible con la administración centralizada.
- La solución debe ser compatible con la autenticación de dos factores: nombre de usuario / contraseña, archivo de certificados HTTPS
- La solución debe ser compatible con la integración del sistema: SNMP, syslog.
- La solución debe admitir al menos 3 roles de administrador, incluidos administrador, operador y auditor (se aceptará roles con diferentes nombres siempre que cumpla con la función de administrador, operador y auditor)<sup>35</sup>
- La solución debe poder proteger el sistema de ataques de fuerza bruta en el nombre de usuario y la contraseña
- La solución debe admitir la política de seguridad de contraseña para las cuentas de administrador.
- La solución debe ser compatible con los servidores Radius, AD y LDAP.
- La solución debe ser compatible con la implementación rápida mediante la instalación automática de USB, la ejecución local y remota de scripts.
- La solución debe ser compatible con el estado dinámico del panel de control en tiempo real y con los widgets de monitoreo detallados
- El dispositivo debe ser compatible con la gestión de dispositivos de almacenamiento: personalización y alarma del umbral de espacio de almacenamiento, superposición de datos antiguos, detener la grabación.
- El dispositivo debe admitir registros de tráfico detallados: reenviados, sesiones violadas, tráfico local, paquetes inválidos
- El dispositivo debe admitir registros de eventos completos: auditorías de actividad administrativa y del sistema, enrutamiento y redes, VPN, autenticaciones de usuarios, y opcionalmente<sup>36</sup> eventos relacionados con WiFi.
- El dispositivo debe admitir la opción de resolución de nombre de puerto de servicio e IPs.
- La solución debe ser compatible para agregar direcciones IP o MAC de hosts a la lista negra para bloquear el acceso a la red por un cierto período de tiempo.
- La solución debe admitir el bloqueo de la cuenta después de varias fallas de inicio de sesión.
- La solución debe admitir la configuración de tareas de captura de paquetes con múltiples condiciones para capturar paquetes al mismo tiempo.
- La solución debe ser compatible para guardar y exportar los archivos de captura.
- El dispositivo debe admitir la opción de formato de registro de tráfico breve
- El dispositivo debe admitir informes granulares con puntos de vista orientados por el usuario
  - Gestión de HA
  - Vista del propietario del sistema
  - Vista del administrador de seguridad de red.
- Opcionalmente<sup>37</sup>, la solución debe ser compatible con SYSLOG estándar y registro de formato binario; el almacenamiento distribuido de registro binario a múltiples servidores de registro, el algoritmo distribuido admite Round robin, Src IP HASH.
- La solución debe admitir el registro en la memoria local y / o los registros de syslog.
- La solución debe admitir el registro para el cambio de la política de seguridad.
- La solución debe ser compatible con el registro confiable utilizando la opción TCP (RFC 3195)
- La solución debe ser compatible para guardar las condiciones del filtro de registro buscado.
- La solución debe admitir informes basados en zona de seguridad, dirección IP, nivel de amenaza y tipo.
- La solución debe admitir informes definidos por el usuario.
- La solución debe soportar el reporte programado.

<sup>35</sup> Texto agregado en virtud a la consulta y/u observación N° 38 y 78 respectivamente.

<sup>36</sup> Texto agregado en virtud a la consulta y/u observación N° 288 y 459 respectivamente.

<sup>37</sup> Texto agrado en virtud a la consulta y/u observación N° 42, 291 y 456 respectivamente.



- El informe se puede exportar en PDF / HTML / WORD por correo electrónico o FTP.
- La solución debe ser compatible para obtener una vista previa de los archivos de informe en formato HTML y PDF.
- La solución debe ser compatible con URI y la decodificación de datos de ataque
- La solución debe ser compatible para configurar direcciones Ipv6 para el servidor NTP.
- La solución debe ser compatible para identificar la fuente de IP real del paquete y mostrar el registro de IP de origen del paquete en el registro de amenazas
- (opcional)<sup>38</sup> la solución debe admitir la función de reparación de la base de datos.

#### POLITICAS DE SEGURIDAD

- La solución propuesta debe ser compatible con el control de acceso para la zona , usuario , servicio, aplicación, IPS, AV en una regla de política.
- La solución propuesta debe admitir objetos de políticas predefinidos y personalizados.
- La solución propuesta debe soportar la verificación de redundancia de la política de seguridad.
- La solución propuesta debe ser compatible con el recuento de hits de políticas en WebUI
- La solución debe admitir la detección de validez basada en el tiempo.
- La solución debe ser compatible con la importación y exportación de políticas.

#### CARACTERÍSTICAS INTELIGENTES DE SEGURIDAD

- La solución debe admitir análisis de correlación de amenazas, correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales. Se aceptará que la solución se encuentre licenciada con la funcionalidad de sandbox en la nube del fabricante<sup>39</sup>
- La solución debe ser compatible con las reglas de análisis de correlación de amenazas multidimensionales, actualización diaria automática desde la nube
- La solución debe admitir la detección avanzada de malware basada en el comportamiento sin firma o con un servicio licenciado de sandbox en la nube del fabricante<sup>40</sup>.
- La solución debe permitir la detección de más de 2000 familias de programas maliciosos conocidos y desconocidos, incluidos virus, gusanos, troyanos, desbordamientos, etc.
- La solución debe ser compatible con la actualización de la base de datos del modelo de comportamiento de malware en línea en tiempo real. Se aceptará un servicio licenciado de sandbox en la nube del fabricante para la actualización de base de datos de firmas.<sup>41</sup>
- La solución debe ser compatible con el modelado de comportamiento basado en el tráfico de línea de base L3-L7 para revelar un comportamiento anómalo de la red, como el escaneo HTTP, Spider, SPAM, SSH / FTP. Se aceptará que la solución se encuentre licenciada con la funcionalidad de sandbox en la nube del fabricante<sup>42</sup>
- (opcional)<sup>43</sup>, la solución debe ser compatible con la detección de DDoS, incluyendo Flood, Sockstress, zip of death, reflejo, consulta de DNS, SSL DDoS y DDoS de aplicaciones basadas en análisis de comportamiento anormal.
- La solución debe admitir la inspección del tráfico de túnel cifrado para aplicaciones desconocidas
- La solución debe ser compatible con la actualización de la base de datos del modelo de comportamiento anormal en línea y en tiempo real.
- La solución debe proporcionar visibilidad de amenazas, incluido el índice de riesgo de la red, los activos críticos y el estado de riesgo del host, la gravedad y la certeza del riesgo del host y la amenaza.

<sup>38</sup> Texto agregado en virtud a la consulta y/u observación N° 292 y 455 respectivamente

<sup>39</sup> Texto agregado en virtud a la consulta y/u observación N° 195 y 201 respectivamente

<sup>40</sup> Texto agregado en virtud a la consulta y/u observación N° 196

<sup>41</sup> Texto agregado en virtud a la consulta y/u observación N° 197

<sup>42</sup> Texto agregado en virtud a la consulta y/u observación N° 198

<sup>43</sup> Texto agregado en virtud a la consulta y/u observación N° 294 y 453 respectivamente



- La solución debe proporcionar el mapeo de cadena de eventos de amenaza en cada host
- La solución debe proporcionar análisis forense, incluido el análisis de amenazas, base de conocimientos, histórico y el PCAP.
- La solución debe admitir reglas de mitigación personalizadas y predefinidas para eventos de seguridad.
- La solución debe ser compatible con la herramienta de captura de paquetes en línea, que se puede utilizar para capturar paquetes en línea según la dirección de origen, la dirección de destino, la aplicación, el protocolo, el puerto de origen, el puerto de destino, el tamaño del archivo, etc.<sup>44</sup>
- La solución debe admitir la captura de paquetes para la base de datos de firmas IPS global o protocolos específicos

#### MONITOREO

- La solución debe ser compatible con el monitor de amenazas completo, incluido el nombre del ataque, la gravedad, el tiempo, la dirección, el protocolo, la solución recomendada, etc.
- La solución debe ser compatible con el monitor de estadísticas multidimensionales para el riesgo de la aplicación, la categoría, las características y la tecnología.
- La solución debe soportar estadísticas y análisis de tráfico en tiempo real.
- La solución debe ser compatible para observar la tasa de reenvío de paquetes ascendente y descendente de la interfaz
- La solución debe ser compatible con el monitoreo de estado de CPU, memoria, temperatura, ventilador, módulos de alimentación, etc.

#### 1.6.1.6. SOLUCIÓN DE SEGURIDAD PERIMETRAL EN ALTA DISPONIBILIDAD

Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red de datos de la entidad.  
La solución tiene que ser ofrecida en alta disponibilidad (Activo – Pasivo), se entiende por alta disponibilidad, es decir por lo menos dos (02) appliances con las mismas características mínimas mencionadas en estas especificaciones.

Para efectos de la propuesta los equipos propuestos deberán ser nuevos de primer uso, no se admitirán soluciones que incluyan equipos refurbished o de re-uso. Asimismo, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support o similares al momento de la presentación de la oferta<sup>45</sup>. Se deberá adjuntar carta del fabricante que certifique que los equipos propuestos no están en end-of-life o end-of-sale o end-of-support o similares<sup>46</sup> y confirme el cumplimiento de las especificaciones técnicas.

#### Características generales:

- La solución no debe tener chips específicos de aplicación del tipo ASIC que no permitan futuras expansiones de firmware y características en el mismo hardware. La solución debe basarse en una arquitectura de procesamiento paralelo y no debe usar chips ASIC de propiedad exclusiva.
- La solución propuesta debe ser capaz de operar en modalidad capa 3 (enrutamiento), modalidad en línea (bridge) y capa 2 (port mirroring) de forma simultánea (sin necesidad de virtualizar el equipo)
- La solución propuesta debe ser un Firewall de Próxima Generación y no un sistema UTM.
- La solución propuesta debe tener al menos un puerto de consola dedicado, un puerto AUX (opcional)<sup>47</sup> y al menos un puerto USB.
- La solución propuesta debe tener al menos 2 puertos Gigabit Ethernet y 8 puertos SFP+; cualquiera de ellos puede ser utilizado como interfaz WAN o LAN.
- La solución deberá incluir los transceivers de la marca, necesarios para la conectividad entre los equipos componentes de la solución.

<sup>44</sup> Texto suprimido en virtud a la consulta y/u observación N° 297 y 450 respectivamente.

<sup>45</sup> Texto agregado en virtud a la consulta y/u observación N° 201

<sup>46</sup> Texto agregado en virtud a la consulta y/u observación N° 201

<sup>47</sup> Texto agregado en virtud a la consulta y/u observación N° 55



- La solución propuesta debe tener un puerto dedicado para alta disponibilidad (HA) en Gigabit Ethernet y un puerto de administración (MGT) en Gigabit Ethernet.
- La solución propuesta debe tener al menos 3 slots para módulos de extensión, pudiendo llegar a tener hasta 18 puertos Gigabit Ethernet ó hasta 16 puertos SFP al agregar dichos módulos.
- La solución propuesta debe ser poseer fuente redundante.
- La solución propuesta debe ser con un factor de forma 2.5-U o 2-U o 3-U<sup>48</sup>.
- La solución propuesta debe ser compatible con Lightning Surge Immunity (certificación IEC 61000-4-5 2005 Surge Immunity)
- La solución propuesta debe admitir 60 Gbps de Firewall Throughput.
- La solución propuesta debe admitir sesiones concurrentes de hasta 20 M.
- La solución propuesta debe soportar 800,000 nuevas sesiones por segundos bajo tráfico TCP.
- La solución propuesta debe admitir Throughput VPN IPSec de 35 Gbps y 20000 túneles VPN IPSec.
- La solución propuesta debe admitir Throughput de AV de 20 Gbps.
- La solución propuesta debe admitir Throughput de IPS de 25 Gbps.
- La solución propuesta debe admitir un máximo de 10000 usuarios SSLVPN concurrentes, y con 8 usuarios SSLVPN de forma gratuita.

#### Servicios de red:

- La solución propuesta debe ser compatible con los protocolos de enrutamiento dinámico OSPF, BGP, RIPv2 y (opcionalmente)<sup>49</sup> IS-IS.
- La solución propuesta debe ser compatible con enrutamiento estático y basado en políticas (PBR).
- La solución propuesta debe ser compatible con enrutamiento basado en aplicaciones, para poder enrutar aplicaciones como P2P, video en línea, etc.<sup>50</sup> con números de puerto dinámicos al enlace WAN seleccionado.
- La solución propuesta debe ser compatible con los servicios de red DHCP, NTP, Servidor DNS y proxy DNS integrados.
- La solución propuesta debe soportar modo de operación routing o NAT.
- La solución propuesta debe poder ser soportada ser<sup>51</sup> configurada en modo TAP.
- La solución propuesta debe ser compatible con el modo de operación transparente (bridge)
- La solución propuesta debe ser compatible con el modo de operación mixto (NAT, routing y bridge)
- La solución propuesta debe admitir los siguientes modos de interfaz: sniffer, puerto agregado, loopback, VLANS (802.1Q y Trunking)
- La solución propuesta debe ser compatible con conmutación y enrutamiento (capa 2 y capa 3).
- (opcional)<sup>52</sup> la solución propuesta debe ser compatible con la función de virtual switch, cada virtual switch tiene su propia tabla de direcciones MAC.
- La solución propuesta debe ser compatible con la función de enrutamiento virtual, cada v-router tiene su propia tabla de enrutamiento.
- La solución propuesta debe ser compatible con la duplicación de tráfico al puerto configurado en el dispositivo para el análisis del tráfico (port mirror), éste puede estar basado en la IP de origen, IP de destino, puerto de origen, puerto de destino, protocolo de red (TCP, UDP o ICMP), etc. El port mirror puede ser configurado para el tráfico de ingreso, el tráfico de egreso o ambos.
- La solución propuesta debe soportar SNAT, DNAT, PAT. Debe admitir por política la configuración de NAT y la configuración central de la tabla de NAT.
- La solución propuesta debe ser compatible con NAT dinámico y NAT estático, multi-a-uno, uno-a-multi, NAT uno a uno.

<sup>48</sup> Texto agregado en virtud a la consulta y/u observación N° 56, 302 y 448 respectivamente.

<sup>49</sup> Texto agregado en virtud a la consulta y/u observación N° 312 y 430 respectivamente.

<sup>50</sup> Texto suprimido en virtud a la consulta y/u observación N° 313 y 431 respectivamente.

<sup>51</sup> Texto suprimido y agregado en virtud a la consulta y/u observación N° 53

<sup>52</sup> Texto agregado en virtud a la consulta y/u observación N° 314 y 432 respectivamente.



- (opcionalmente)<sup>53</sup> la solución propuesta debe ser compatible con NAT444 (CGNAT) y con la exportación de la tabla de asignación estática NAT444 como un archivo.
- La solución propuesta debe ser compatible con la detección de reenvío bidireccional (BFD), la interacción BFD con la ruta estática, OSPF o BGP.
- (opcionalmente)<sup>54</sup> la solución propuesta debe admitir la expansión del grupo NAT para que una dirección IPv4 pública admita más de 64K direcciones IP privadas.
- La solución propuesta debe ser compatible con NAT46, NAT64, y opcionalmente<sup>55</sup> DNS64.
- La solución propuesta debe ser compatible con Full Cone NAT(opcional)<sup>56</sup>, STUN (opcional).<sup>57</sup>
- La solución propuesta debe ser compatible con la función NetFlow, el dispositivo puede recopilar el tráfico de ingreso del usuario y enviarlo al servidor con la herramienta de análisis de datos NetFlow, para detectar, monitorear y cobrar el tráfico.
- Soporte para ver información de estado de enlaces de múltiples interfaces al mismo tiempo para análisis comparativo.
- Soporte para identificar el comportamiento de acceso compartido en la red.
- Admite la función de habilitar la detección de un nombre de dominio específico, que se puede especificar como un modo de indagación o iniciar un modo de solicitud de DNS.
- El modo de traducción de puerto dinámico SNAT es compatible con Round-robin, es decir, la sesión generada por cada IP de origen se sondeará para asignar la dirección IP.

#### Firewall

- La solución propuesta debe admitir objetos de políticas predefinidos y personalizados. Debe soportar la agrupación de objetos.
- La solución propuesta debe ser compatible con la política de seguridad basada en aplicación, el rol del usuario y la ubicación geográfica.
- La solución propuesta debe admitir ALG para al menos los siguientes protocolos: MSRPC, PPTP, RAS, RSH, RTSP, SIP, SQLNetV2, SUNRPC, FTP, TFTP, HTTP, DCERPC, DNS-TCP, DNS-UDP, H. 245, H.323, Q.931, XDMCP
- La solución propuesta debe ser compatible con NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT(opcional)<sup>58</sup>, STUN (opcional)<sup>59</sup>
- La solución propuesta debe ser compatible con VoIP: SIP, H.323, SCCP, NAT transversal, y (opcionalmente)<sup>60</sup> RTP pin holing
- La solución propuesta debe permitir la creación de una sola política para el control de aplicaciones, control basado en el usuario, prevención de amenazas, antivirus, filtrado de archivos, dentro de una sola política.
- La solución propuesta debe soportar la verificación de redundancia de las políticas de seguridad.
- La solución propuesta debe admitir el recuento de visitas de políticas en WebUI (hit counts).
- La solución propuesta debe ser compatible con la búsqueda de políticas en WebUI.
- La solución propuesta debe ser compatible con la política programada, una sola vez o recurrente.
- La solución propuesta debe ser compatible para configurar el grupo de políticas a través de WebUI
- La solución propuesta debe admitir el límite de sesión en función de la IP de origen, la IP de destino, la programación, el protocolo de la aplicación (mysql, ms-sql, sqlnet, descarga de P2P, video, juego, etc.) y limitar las nuevas conexiones, sesiones simultáneas.
- La solución propuesta debe soportar defensa contra protocolos anormales.
- La solución propuesta debe soportar defensa contra ataques ARP.
- La solución propuesta debe ser compatible con la protección DDoS, contra inundaciones de consultas DNS, inundaciones SYN, inundaciones UDP, inundaciones ICMP, ping de la

<sup>53</sup> Texto agregado en virtud a la consulta y/u observación N° 315 y 433 respectivamente.

<sup>54</sup> Texto suprimido y agregado en virtud a la consulta y/u observación N° 63, 316 y 434 respectivamente

<sup>55</sup> Texto agregado en virtud a la consulta y/u observación N° 317 y 435 respectivamente.

<sup>56</sup> Texto agregado en virtud a la consulta y/u observación N° 318 y 436 respectivamente.

<sup>57</sup> Texto agregado en virtud a la consulta y/u observación N° 318 y 436 respectivamente.

<sup>58</sup> Texto agregado en virtud a la consulta y/u observación N° 64, 320 y 427 respectivamente

<sup>59</sup> Texto agregado en virtud a la consulta y/u observación N° 64, 320 y 427 respectivamente

<sup>60</sup> Texto adicionado en virtud a la Consulta N° 321 y 409 respectivamente



muerte, pitufo, WinNuke, TCP Split Handshake; la acción soportada incluye registro y reinicio.

- La solución propuesta deberá soportar diferentes configuraciones para las diferentes zonas de seguridad.

#### **Antivirus**

- La solución debe admitir al menos 2 millones de firmas de antivirus, con actualizaciones de firma manual o automática.
- La solución debe ser compatible con Antivirus basado en flujo de red: los protocolos incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP.
- La solución debe admitir la detección de virus para archivos comprimidos como RAR, ZIP, GZIP, BZIP2, TAR; admite la detección de archivos comprimidos de múltiples capas para no menos de 5 capas de descompresión y personaliza la acción para cuando supera los comportamientos
- La solución debe admitir acciones personalizadas para archivos comprimidos cifrados.
- (opcionalmente)<sup>61</sup> La solución debe admitir al menos 3 acciones: fill magic, reset a la conexión o solo registrar el log cuando se detecte un virus o un sitio web malicioso
- La solución debe admitir la advertencia de virus y sitios web maliciosos, alertar al usuario de que el sitio web es un sitio web malicioso o que se detectó un virus.

#### **Filtro URL**

- La solución debe ser compatible con el filtrado web dinámico con una base de datos de categorización en tiempo real basada en la nube: más de 140 millones de URL con no menos de 64 categorías (no menos de 8 de las cuales están relacionadas con la seguridad)
- La solución debe ser compatible con la inspección de filtrado web basada en flujo.
- La solución debe admitir el filtrado web definido manualmente en función de la URL, el contenido web y el encabezado MIME
- La solución debe ser compatible con las siguientes funciones de filtrado web adicionales:
  - Filtro de Java Applet, ActiveX y / o cookie.
  - Bloquear HTTP Post
  - Registrar palabras clave de búsqueda
  - Excepción de escaneo de conexiones cifradas en ciertas categorías para privacidad
- La solución debe admitir la anulación del perfil de filtrado de URL, para que el administrador pueda asignar temporalmente diferentes perfiles a usuario/grupo/IP
- La solución debe permitir personalizar la página de advertencia para el filtrado de URL.
- La solución debe ser compatible para configurar el filtrado de URL según la zona de seguridad.

#### **Sandbox**

- La solución debe ser compatible con la carga de archivos maliciosos a la nube para su análisis
- La solución debe admitir la carga de archivos maliciosos desde protocolos que incluyen HTTP/HTTPS, POP3, IMAP, SMTP y FTP.
- La solución debe admitir tipos de archivos que incluyen PE, ZIP, RAR, Office, PDF, APK, JAR y (opcional)<sup>62</sup> SWF.
- La solución debe admitir la dirección de transferencia de archivos y el control del tamaño del archivo.
- La solución debe proporcionar un informe completo de análisis de comportamiento para archivos maliciosos
- La solución debe admitir el bloqueo de resultados de detección para bloquear una amenaza desconocida rápidamente.
- La solución debe ser compatible con el intercambio global de inteligencia de amenazas y bloqueo de amenazas en tiempo real.

#### **Botnet**

<sup>61</sup> Texto adicionado en virtud a la Consulta Nro. 67

<sup>62</sup> Texto adicionado en virtud a la Consulta Nro. 325 y 405 respectivamente.



- La solución debe descubrir de forma efectiva los bots de la intranet y evitar nuevos ataques de amenazas avanzadas mediante la comparación de la información obtenida con la base de datos de direcciones de C&C.
- La solución debe ser compatible con las actualizaciones regulares de la dirección del servidor Botnet.
- La solución debe admitir dos tipos de base de datos de direcciones C&C: la base de datos de direcciones IP y la base de datos del dominio.
- La solución debe admitir la detección de los protocolos TCP, HTTP y DNS.
- La solución debe permitir la creación de una lista blanca C&C (IPs y dominio)

#### IP Reputation

- Soporte para filtrar el tráfico de IPs con baja reputación, incluidos Botnet, Spam, nodos comprometidos, fuerza bruta, etc.<sup>63</sup>
- Soporte para registrar, eliminar o bloquear paquetes si el tráfico malicioso llega a la lista de reputación de IP.
- Soporte para actualizar la base de datos de reputación de IP instalando una licencia para este fin.
- Soporte para filtrar la dirección IP de los bots y del servidor botnet.

#### SSL Decryption

- La solución debe admitir la identificación de la aplicación para el tráfico cifrado SSL
- La solución debe soportar IPS para tráfico cifrado SSL
- La solución debe soportar AV para tráfico cifrado SSL
- La solución debe admitir el filtrado de URL para el tráfico cifrado SSL
- La solución debe ser compatible con el modo de descarga de proxy SSL.
- El proxy SSL se configura según la política y no en la configuración global (después de vincular el perfil del proxy SSL a una regla de política, el sistema procesará el tráfico que coincide con la regla de acuerdo con la configuración del perfil)
- El Proxy SSL podría ejecutarse en Require mode (el dispositivo realiza la función de proxy SSL en la comunicación cifrada por el certificado del sitio web especificado) o el modo exento (el dispositivo no realiza la función de proxy SSL en la comunicación cifrada por el certificado del sitio web especificado)
- La solución debe soportar lista de recursos.

#### Identificación y control

- La solución debe admitir la identificación de al menos 10 sistemas operativos en el end point: como Windows, IOS, Android, etc.<sup>64</sup>
- La solución debe admitir consultas basadas en IP y cantidad de puntos finales.
- La solución debe admitir más de 3,000 aplicaciones, debe admitir el filtro de aplicaciones por nombre, categoría, subcategoría, tecnología y riesgo.
- La solución debe admitir la visualización de la descripción, los factores de riesgo, las dependencias, los puertos típicos utilizados y las URL para obtener referencias adicionales, y la información para cada aplicación en WebUI.
- La solución debe admitir el bloqueo, reinicio, el monitoreo y la configuración del tráfico para las aplicaciones.
- La solución debe ser capaz de identificar y controlar las aplicaciones en la nube, debe proporcionar monitoreo y estadísticas multidimensionales para las aplicaciones en la nube, incluyendo la categoría de riesgo y las características.
- La solución debe admitir el control de transferencia de archivos en función del nombre, tipo y tamaño del archivo.
- La solución debe soportar el control de transferencia de archivos en los siguientes protocolos: HTTP, HTTPS, FTP, SMTP, POP3
- La solución debe admitir la firma de archivos y la identificación de sufijos para más de 100 tipos de archivos

<sup>63</sup> Texto suprimido en virtud a la consulta y/u observación N° 326 y 404 respectivamente.

<sup>64</sup> Texto suprimido en virtud a la consulta y/u observación N° 327 y 403 respectivamente.



- La solución debe admitir el filtrado de contenido para los protocolos HTTP-GET, HTTP-POST, FTP y SMTP.
- La solución debe ser compatible con la identificación de IM y la auditoría de comportamiento de la red.
- La solución debe soportar la base de datos de usuarios local.
- La solución debe admitir la autenticación de usuarios con TACACS +, LDAP, Radius, Active Directory
- La solución debe admitir la interacción con el sistema de autenticación de terceros a través de la API abierta.
- La solución debe ser compatible con la autenticación de 2 factores, ya sea con soporte de terceros, servidor de token integrado y SMS
- La solución debe admitir la sincronización de grupos de usuarios basada en AD y LDAP.
- La solución debe ser compatible con 802.1X, SSO Proxy
- La solución debe ser compatible con la página de autenticación web personalizada.
- La solución debe ser compatible con la autenticación activa basada en la interfaz.
- La solución debe ser compatible con el inicio de sesión único: Windows AD, función SSO de AD sin agente (AD Polling)
- La solución debe admitir el protocolo SSO-monitor para la sincronización de usuarios autorizados.
- La solución debe ser compatible con WebAuth basada en MAC.

#### QoS

- La solución debe ser compatible con el control de ancho de banda máximo o garantizado, en una dirección IP o usuario.
- La solución debe admitir la asignación de túneles en función del dominio de seguridad, la interfaz, la dirección, usuarios o grupo de usuarios, servidores o grupo de servidores, aplicaciones o grupo de aplicaciones, los TOS, las VLAN.
- La solución debe admitir el ancho de banda asignado por tiempo, prioridad o el mismo ancho de banda compartido.
- La solución debe ser compatible con TOS y DiffServ.
- La solución debe soportar políticas de QoS programada.
- La solución debe admitir la asignación flexible y priorizada del ancho de banda restante no utilizado
- La solución debe admitir dos niveles de configuración de tráfico que permitan la configuración del tráfico en diferentes dimensiones, como usuarios y aplicaciones. La solución debe admitir al menos cuatro túneles por nivel, lo que proporciona una jerarquía de control de tráfico.
- La solución debe admitir la asignación de ancho de banda según la categoría de URL
- La solución debe admitir direcciones IPv6 en la función QoS.
- El monitor debe permitir el monitoreo del tráfico de acuerdo a las políticas de QoS definidas

#### VPN

- La solución debe ser compatible con las siguientes funciones de VPN IPsec:
  - Modo IPSEC Fase 1: modo de protección agresivo y principal
  - Compatible con IKEv1 e IKEv2 (RFC 4306)
  - Método de autenticación: certificado y clave precompartida.
  - Soporte de configuración del modo IKE (como servidor o cliente)
  - DHCP sobre IPSEC
  - Cifrado de Fase 1 / Fase 2: DES, 3DES, AES128, AES192, AES256
  - Autenticación Fase 1 / Fase 2: MD5, SHA1, SHA256, SHA384, SHA512
  - Soporte Fase 1 / Fase 2 Diffie-Hellman: 1,2,5
  - XAuth como modo servidor y para usuarios de acceso telefónico.
  - Replay detection.
  - Autokey keep-alive para Phase 2 SA
- La solución debe ser compatible con VPN IPsec basada en rutas y políticas.
- La solución debe ser compatible con los siguientes modos de implementación VPN IPSEC: puerta de enlace a puerta de enlace, malla completa, hub y spoke, túnel redundante, terminación de VPN en modo transparente.



- La solución debe ser compatible mínimamente<sup>65</sup> con SSLVPN para Linux, iOS<sup>66</sup>, Android y Windows XP/Vista/<sup>67</sup> Windows 10, incluye<sup>68</sup> sistemas operativos Windows de 64 bits.
- La solución debe ser compatible con SSLVPN con un inicio de sesión único que evita inicios de sesión simultáneos con el mismo nombre de usuario
- La solución debe soportar el portal SSL limitando a los usuarios
- La solución debe ser compatible con SSL. El módulo de reenvío de puerto VPN cifra los datos del cliente y los envía al servidor de aplicaciones.
- La solución debe admitir la comprobación de la integridad del host y la comprobación del sistema operativo antes de la conexión del túnel SSL.
- La solución debe ser compatible con la verificación de MAC por portal.
- La solución debe admitir la opción de limpieza de la memoria caché antes de finalizar la sesión SSL VPN
- La solución debe permitir múltiples inicios de sesión SSL VPN personalizados asociados con grupos de usuarios (rutas de URL, diseño)
- La solución debe admitir la autenticación SSL con una llave USB
- La solución debe ser compatible con el modo de servidor y cliente L2TP, L2TP sobre IPSEC y GRE sobre IPSEC
- La solución debe ser compatible con PnPVPN para el despliegue rápido de múltiples sucursales VPN de sitio a sitio.

#### IPV6

- La solución debe ser compatible con la administración de dispositivos a través de IPv6, el registro de IPv6 y HA en IPV6.
- La solución debe ser compatible con túneles IPv6, DNS64 / NAT64, etc.
- La solución debe ser compatible con los protocolos de enrutamiento IPv6 de enrutamiento estático, enrutamiento de políticas, ISIS, RIPng, OSPFv3 y BGP4 +
- La solución debe ser compatible con IPsec VPN para IPv6.
- La solución debe ser compatible con IPv6 IPS, identificación de la aplicación, filtrado de URL, antivirus, control de acceso, defensa de ataque ND
- La solución debe ser compatible con el conjunto estadístico, registro y monitoreo para IPv6.
- La solución debe ser compatible para configurar y bloquear direcciones IPv6.

#### Alta Disponibilidad (HA)

- La solución debe ser compatible con los modos Activo/Activo y Activo/Pasivo
- La solución debe admitir interfaces redundantes heartbeats para HA
- La solución debe admitir la sincronización de sesiones standalone.
- La solución debe ser compatible con la conmutación por error de alta disponibilidad basada en la interfaz, HTTP, ICMP, ARP, DNS y seguimiento de objetos basados en TCP.
- La solución debe admitir las siguientes opciones de implementación de HA:
  - HA con agregación de enlaces
  - HA de malla completa
  - HA geográficamente disperso
- La solución debe ser compatible con HA en peer-mode, para evitar problemas de enrutamiento asimétrico en la implementación del modo Activo-Activo.

#### Logs y Reportes

- La solución debe admitir el rollback del sistema operativo, debe admitir al menos dos copias de firmware en la memoria flash del sistema.
- La solución debe guardar diez versiones del archivo de configuración.
- La solución debe admitir la exportación de configuraciones actuales y de respaldo a destinos externos, incluidos el servidor FTP, el servidor TFTP y a una flash USB.
- La solución debe soportar SNMP

<sup>65</sup> Texto agregado en virtud a la consulta y/u observación N° 204.

<sup>66</sup> Texto suprimido en virtud a la consulta y/u observación N° 204.

<sup>67</sup> Texto suprimido en virtud a la consulta y/u observación N° 204.

<sup>68</sup> Texto suprimido en virtud a la consulta y/u observación N° 204.



- La solución debe ser accesible mediante la interfaz de usuario web integrada (WebUI) y la interfaz de línea de comandos (CLI)
- La solución debe admitir el acceso de administración desde HTTP (opcional)<sup>69</sup> /HTTPS, SSH, telnet (opcional)<sup>70</sup>, consola
- La solución debe admitir al menos 3 roles de administrador, incluidos administrador, operador y auditor (se aceptará roles con diferentes nombres siempre que cumpla con la función de administrador, operador y auditor)<sup>71</sup>
- La solución debe poder proteger el sistema de ataques de fuerza bruta en el nombre de usuario y la contraseña
- La solución debe admitir la política de seguridad de contraseña para las cuentas de administrador.
- La solución debe ser compatible con la implementación rápida mediante la instalación automática de USB, la ejecución local y remota de scripts.
- (Opcionalmente)<sup>72</sup> la solución debe ser compatible con SYSLOG estándar y registro de formato binario; el almacenamiento distribuido de registro binario a múltiples servidores de registro, el algoritmo distribuido es compatible con Round robin, Src IP HASH.
- (opcionalmente)<sup>73</sup> la solución debe admitir el registro en la memoria local o en los servidores de syslog.
- La solución debe admitir el registro para el cambio de la política de seguridad.
- La solución debe ser compatible con el registro confiable utilizando la opción TCP (RFC 3195)
- La solución debe soportar el envío de log en formato binario o de texto.
- La solución debe admitir la transferencia de registros a través del protocolo UDP, TCP, Secure-TCP
- La solución debe admitir al menos tres informes predefinidos: seguridad, flujo e informes de red.
- La solución debe admitir informes definidos por el usuario. El informe se puede exportar en PDF a través de correo electrónico o FTP También se aceptará que la solución pueda admitir o integrarse con una herramienta que permita la personalización de reportes y que el informe pueda exportarse en PDF a través de correo electrónico o FTP<sup>74</sup>.
- La solución debe ser compatible con RESTAPI para la libreta de direcciones IP, AV, IPS, regla de políticas, NAT, interfaz, zona de seguridad, enrutamiento, administración de actualizaciones

#### Monitoreo

- Soporta las estadísticas de tráfico de aplicaciones por usuario
- La solución debe ser compatible con el monitoreo de estadísticas multidimensionales para aplicaciones basadas en riesgo, categoría, características y tecnología.
- La solución debe admitir estadísticas para la visita de URLs y categoría de URLs.
- Soporta estadísticas y análisis de tráfico en tiempo real
- Estadísticas de eventos de seguridad
- Soporte de monitoreo definido por el usuario
- Soporte para monitorear el estado del dispositivo, como CPU, memoria, temperatura, etc.
- Los reportes podrán ser exportados en formatos PDF, Word o HTML.
- La solución deberá contar con un monitoreo centralizado para múltiples dispositivos, incluyendo CPU, memoria (opcional)<sup>75</sup>, tráfico, sesiones, aplicaciones, usuarios, amenazas, etc.<sup>76</sup> a través de una aplicación móvil, de los últimos 90 días.
- La aplicación de monitoreo deberá soportar acceso web y acceso a través de aplicaciones en dispositivos móviles
- La aplicación de monitoreo proporcionará informes personalizados y programados.

<sup>69</sup> Texto agregado en virtud a la consulta y/u observación N° 339; 391 respectivamente.

<sup>70</sup> Texto agregado en virtud a la consulta y/u observación N° 339; 391 respectivamente.

<sup>71</sup> Texto agregado en virtud a la consulta y/u observación N° 38

<sup>72</sup> Texto agregado en virtud a la consulta y/u observación N° 54, 340 y 390 respectivamente.

<sup>73</sup> Texto agregado en virtud a la consulta y/u observación N° 341 y 389 respectivamente.

<sup>74</sup> Texto agregado en virtud a la consulta y/u observación N° 85.

<sup>75</sup> Texto agregado en virtud a la consulta y/u observación N° 344 y 386 respectivamente.

<sup>76</sup> Texto suprimido en virtud a la consulta y/u observación N° 344 y 386 respectivamente.



**1.6.1.7. Anti DDOS Local (opcional)<sup>77</sup>**

Deberá considerarse una solución en sitio (aparte de la solución en la nube solicitada), la cual deberá soportar el ancho de banda solicitado. El contratista adjudicado deberá realizar las configuraciones y conexiones necesarias a fin de que la solución Anti DDOS (en sitio); solicitada sincronice automáticamente vía un protocolo de señalización con la solución en nube del contratista para la protección de ataques DDoS del tipo volumétrico, el appliance dedicado deberá ser nuevo y de tecnología vigente el cual deberá ser respaldado por carta del fabricante a presentarse como parte de la oferta y cubrir los siguientes requisitos mínimos:

- El servicio de protección contra ataques de DDoS debe implementarse con dispositivos de propósito específico dedicado a proteger la disponibilidad del servicio; por lo que no se aceptarán dispositivos que mantengan el estado de la conexión como cortafuegos, sistemas de prevención y sus variantes o combinaciones como UTM, NGFW, NGIPS, ADC, Proxis y WAF ya que al conservar el estado de la conexión son susceptibles a ataques de DDoS.
- La solución debe de contar con un mecanismo de bypass (se requiere el bypass sea con los puertos de fibra ya que se requieren interfaces 10GE SFP+), en caso de no contar con bypass en fibra se aceptará el equipo en Alta disponibilidad), en cada interface para garantizar la disponibilidad y continuidad de los servicios, el cual debe de activarse en los siguientes casos:
  - ✓ Corte de energía
  - ✓ Falla en el hardware
  - ✓ Falla Software
- La solución implementada debe proporcionar al menos 4 interfaces de 10 Gbps de cobre para proteger dos segmentos de red.
- La solución debe tener una capacidad de inspección de al menos 5 Gbps considerando la sumatoria de tráfico de subida más bajada y debe ser posible ampliar esta capacidad por medio de una licencia de actualización utilizando el mismo dispositivo.
- La solución instalada en sitio deberá soportar un crecimiento de hasta 20Gbps sin necesidad de hacer cambio de hardware. Se requiere de al menos 20Gbps de throughput, es decir 10Gbps de subida y 10Gbps de bajada que es la capacidad de las interfaces 10GE SFP+.
- El sistema no debe de realizar ningún seguimiento a las conexiones, por lo que no deberá de tener un número máximo de conexiones simultáneas.
- Al posicionarse en línea, el sistema deberá de ser completamente transparente. El tráfico debe fluir a través de él y deberá de analizar, detectar y mitigar los ataques antes de que lleguen a su destino.
- El sistema debe ser capaz de soportar un modo inactivo cuando se configura en línea, que permita el ajuste de la configuración de protección sin bloquear el tráfico y proporcione reportes de todo el tráfico que bloquearía si se define como "activo".
- El sistema debe soportar la implementación en modo monitor, en el que no introduce ningún punto adicional de falla a la red por medio de un puerto espejo habilitado en un enrutador ("router"), conmutador ("switch") o un tap de red.
- El sistema debe incluir fuentes de alimentación de energía AC redundantes y debe admitir intercambio caliente ("hot swap") de una fuente de alimentación degradada durante el funcionamiento normal del sistema.
- El sistema debe de soportar interfaces de administración redundantes.
- El sistema debe de permitir el acceso CLI a través de un puerto serial RJ-45.
- El sistema debe soportar el funcionamiento como terminador de túneles GRE (Encapsulación de Enrutamiento Genérico).
- El sistema debe de proporcionar una Interface de Programación de Aplicaciones (API) para poder acceder y ampliar sus funcionalidades.
- El sistema deberá de contar con actualizaciones sobre inteligencia de amenazas, para detectar y detener amenazas emergentes dirigidas hacia la infraestructura y servicios del centro de datos, las cuales deberán de actualizarse de manera automática sin necesidad de actualizar el software.

<sup>77</sup> Texto agregado en virtud a la consulta y/u observación N° 205, 346 y 428 respectivamente.



- El sistema debe de proporcionar un filtro de amenazas salientes para evitar que el tráfico malicioso abandone la red, utilizando la inteligencia de amenazas y sus categorías.
- El sistema debe proporcionar una actualización constante sobre inteligencia de amenazas para las siguientes categorías: Firmas de botnets, comando y control, reputación de DDoS, correo electrónico, por ubicación IP, basadas en su ubicación, de malware, móvil y ataques dirigidos.
- El sistema deberá de poder inspeccionar tráfico SSL a través de un módulo de seguridad basado en hardware embebido dentro del mismo dispositivo
- El sistema debe de realizar una inspección SSL pasiva, por lo que no deberá terminar las sesiones SSL o actuar como proxy.
- La inspección de tráfico SSL deberá de soportar suites de cifrado ECDH (Curvas Elípticas de Diffie Hellman) y uno de los cifrados siguientes: RSA o AES.
- El Hardware ofertado debe ser el de última generación disponible y no debe contar con EoS en el plazo de contrato.

#### 1.6.1.7.1. Administración

- El sistema debe proporcionar documentación en línea en la Interfaz de Usuario (UI) para ayudar a comprender las funciones de cada pantalla.
- La Interfaz de Usuario (UI) del sistema debe permitir múltiples niveles de acceso, como son: de administración completa, de administración limitada para la configuración de mitigaciones y de lectura.
- La interfaz de Usuario (UI) debe incluir un registro de cambios sobre los eventos que ocurren en el sistema, cambios en la configuración, descarga de archivos y para solucionar problemas.
- El sistema debe proporcionar la capacidad para crear y exportar paquetes de diagnóstico que contienen información del estado y configuración a utilizarse para resolver problemas.
- El sistema debe proporcionar la capacidad para administrar sus archivos a través de la Interfaz del Usuario (UI), incluida la carga, descarga y eliminación. Se aceptará opcionalmente la descarga de informes en PDF o CSV.
- El sistema debe proporcionar una interfaz CLI para instalar y actualizar el software, realizar la configuración inicial además de otras funciones avanzadas
- El sistema debe proporcionar notificaciones a través de SYSLOG, SNMP o SMTP.
- El sistema debe admitir su monitoreo a través de SNMP v2 o v3 para obtener el estado del sistema, la configuración o las estadísticas de las interfaces.
- El sistema debe ser capaz de generar los siguientes tipos de alertas: de sistema, de protección, de implementación, de dispositivos bloqueados, ancho de banda y registro de cambios.
- El sistema debe permitir la creación, eliminación y administración de cuentas de usuario a través de la Interfaz de Usuario (UI).
- El sistema deberá permitir el acceso remoto mediante SSH.
- El acceso a la Interfaz de Usuario deberá de ser a través de un protocolo seguro como es HTTPS, con la posibilidad de cambiar el certificado digital por uno propietario.
- Los administradores del sistema deben de poder bloquear una cuenta manualmente y especificar el número de intentos de inicio de sesión que puede hacer un usuario antes de que la cuenta quede bloqueada automáticamente.
- A los usuarios sin privilegios administrativos se le permitirá administrar la configuración de sus propias cuentas y contraseñas, pero no podrá cambiar cuentas de otros usuarios.
- El sistema debe poder realizar una autenticación de contraseña estática por medio de la integración de RADIUS o TACACS +

#### 1.6.1.7.2. Funcionalidades de la Interfaces de usuario

- El sistema debe proporcionar un panel de estado de dispositivo que incluya información sobre las alertas activas, total del tráfico permitido y bloqueado a través de las interfaces, estado de la CPU y memoria de sistema.



- El sistema debe proporcionar estadísticas detalladas para cada protección, mostrando su impacto en el tráfico durante los últimos 5 minutos, 1 hora, 24 horas, 7 días o un rango de tiempo.
- El sistema debe mostrar estadísticas de protección sobre tráfico permitido y bloqueado en bits por segundo (bps) y paquetes por segundo (pps).
- Las estadísticas detalladas y gráficos para cada grupo de protección para servidores genéricos deben incluir información sobre el tráfico total, tráfico por URL, tráfico por dominio, información de ubicación IP, distribución de protocolos, distribución de servicios y estadísticas principales de hosts bloqueados.
- El sistema debe admitir la generación de informes PDF que contiene las estadísticas detalladas y gráficos para cada grupo de protección.
- El sistema debe admitir la generación de reportes por correo electrónico con las estadísticas detalladas y gráficos para cada grupo de protección.

#### 1.6.1.7.3. Funcionalidades de prevención y mitigación

- El sistema debe ser capaz de bloquear paquetes TCP / IP inválidos
- El sistema deberá permitir la configuración de listas de filtros de cabecera L2/L3/L4.
- El sistema debe ser capaz de detectar fuentes que envíen cantidades excesivas de tráfico bajo umbrales configurables, para después colocar esas fuentes en listas de hosts bloqueados temporalmente (bloqueo basado en la tasa de tráfico).
- El sistema debe de ser capaz de descartar paquetes según puertos TCP específicos y payloads que coincidan o no con expresiones regulares configurables se aceptara que la solución permita creación de firmas<sup>78</sup>
- El sistema debe de ser capaz de descartar paquetes según puertos UDP específicos y payloads que coincidan o no con expresiones regulares configurables se aceptara que la solución permita creación de firmas<sup>79</sup>
- El sistema debe de soportar prevención de inundación suplantada (spoofing) de SYN's TCP que autentifiquen conexiones TCP desde los hosts origen.
- La prevención de inundación suplantada de SYN's TCP debe de ser capaz de especificar los puertos TCP origen a ser ignorados.
- La prevención de inundación suplantada de SYN's TCP deberá de proporcionar mecanismos de autenticación donde el sistema responda con un ACK imitando una conexión existente y semi abierta para las aplicaciones basadas en TCP que son sensitivas a envío de TCP RST.
- La prevención de inundación suplantada de SYN's TCP debe de ser capaz de establecer un umbral para la automatización de este proceso, indicando a cuantos paquetes SYN enviados a cualquier host protegido deberá de realizar la autenticación de TCP.
- El sistema deberá de poder limitar el número de conexiones concurrentes de TCP que provenientes de un solo origen.
- El sistema debe de soportar la supresión de sesiones TCP inactivas si el cliente no envía una cantidad de datos configurable por el usuario dentro de un periodo de tiempo determinado por el usuario.
- El sistema deberá de ser capaz de autenticar solicitudes DNS obligando al origen a que envíen solicitudes a través de TCP y suprimir aquellas que no puedan ser autenticadas dentro de un tiempo específico.
- El sistema debe de soportar el bloqueo de solicitudes DNS malformadas en el puerto 53 que no cumplan con el estándar RFC.
- El sistema debe ser capaz de limitar el número de consultas DNS por segundo a una velocidad configurable por el usuario.
- El sistema debe ser capaz de bloquear el tráfico desde cualquier host que genere más solicitudes DNS fallidas consecutivas del límite configurado y poner al host origen en una lista negra.

<sup>78</sup> Texto agregado en virtud a la consulta y/u observación N° 88

<sup>79</sup> Texto agregado en virtud a la consulta y/u observación N° 89



- El sistema debe proporcionar la posibilidad de configurar expresiones REGEX para suprimir el tráfico DNS específico con los encabezados que coincidan con las expresiones.
- El sistema deberá de prevenir el bloqueo global de CDN o proxys.
- El sistema debe ser capaz de detectar y eliminar paquetes con formatos incorrectos de HTTP que no se ajusten a los RFC's para los encabezados de solicitud y poner al host origen en una lista negra.
- El sistema debe permitir al usuario configurar el número máximo de solicitudes por segundo y el número máximo de objetos HTTP solicitados por cada host hacia un servicio Web y si la tasa definida es excedida el host deberá de ser bloqueado.
- El sistema debe ser capaz de suprimir paquetes HTTP específicos según los encabezados HTTP coincidentes con expresiones REGEX configurables.
- El sistema debe de proporcionar un mecanismo de protección contra ataques SSL o TLS forzando el uso correcto del protocolo bloqueando solicitudes malformadas.
- El sistema debe de soportar el bloqueo de solicitudes SIP malformadas que no cumplan con el estándar RFC.
- El sistema debe limitar el número de solicitudes SIP que puede enviar un host en un segundo para evitar ataques que podrían irrumpir este servicio.
- El sistema debe de proporcionar la capacidad de limitar la velocidad de reenvío de tráfico que coincide con una expresión específica.
- El sistema debe proporcionar la capacidad para detectar y bloquear las inundaciones de SYN's TCP por encima de la tasa configurada.
- El sistema debe proporcionar la capacidad para detectar y bloquear las inundaciones ICMP por encima de la tasa configurada.
- El sistema debe proporcionar la capacidad para detectar y bloquear las inundaciones UDP por encima de la tasa configurada.
- El sistema debe proporcionar la capacidad de bloquear el tráfico originado por bots según las firmas proporcionadas por el sistema.
- La solución deberá de mitigar ataques de fragmentación.
- El sistema deberá de poder bloquear tráfico Multicast.
- El sistema deberá de poder bloquear tráfico de direcciones privadas.
- El sistema debe proporcionar la capacidad de bloquear el tráfico procedente de fuentes que interrumpen reiteradamente solicitudes HTTP.
- El sistema debe proporcionar la posibilidad de actualizar automáticamente sus firmas de protección de ataques periódicamente a intervalos configurables.
- El sistema deberá de identificar web crawlers y monitorear su uso.
- El sistema debe permitir la configuración de protecciones predefinidas asociadas con servicios específicos, como Web, DNS, VoIP o un servidor genérico.
- El sistema debe de soportar la capacidad de cambiar el Nivel de Protección que se aplica al tráfico, cambiando efectivamente la configuración en uso por el sistema para todas las prevenciones, contando al menos con los niveles de protección: Baja, Media y Alta
- El sistema debe sugerir ciertas configuraciones de protección basadas en el aprendizaje del comportamiento típico de la red.
- El sistema debe de permitir que los parámetros de protección sean cambiados mientras la protección está corriendo.
- El sistema debe de poder bloquear por país de origen.
- El sistema debe poder evitar que el tráfico malicioso salga de la red utilizando un mecanismo de detección y contención a través de categorías de amenazas.
- El sistema debe tener la capacidad de cambiar el nivel de protección a alto de manera automática cuando el tráfico total exceda los umbrales definidos
- El sistema debe soportar la importación de IOCs (Indicadores de compromiso) de fuentes externas en formato STIX and TAXII.
- Los IOC soportados debe incluir, direcciones IP, dominios y Urls.
- El sistema debe soportar hasta 3 Millones de IOC.

#### 1.6.1.8. Solución de Protección de Suplantación de Identidad



El CONTRATISTA deberá incluir, como parte del servicio, un sistema que permita autenticar el dominio de la entidad para el envío legítimo de correos a las instituciones y evitar la suplantación de identidad basado fortaleciendo el protocolo DMARC, SPF y DKIM y considerando que la entidad cuenta con 5000 casillas de correo y deberá cumplir con las siguientes características mínimas:

- El sistema de autenticación de dominio debe contar con un dashboard que permita mostrar el volumen de correos autenticado y no autenticado.
- El sistema de autenticación de dominio debe permitir observar e identificar si el correo de la institución está en cumplimiento con los protocolos de seguridad SPF y DKIM.
- El sistema de autenticación de dominio debe permitir visualizar picos de volumen de email.
- El sistema de autenticación de dominio debe contar con un informe que detalle las IPs de envío.
- El sistema de autenticación de dominio debe mostrar la lista de servidores que envían y/o retransmiten correos en nombre del dominio de la institución.
- El sistema de autenticación de dominio debe permitir identificar la fuente del correo electrónico mal intencionado para tomar una decisión.
- El sistema de autenticación de dominio debe permitir identificar los países en donde se encuentran los servidores que utilizan el dominio de la institución.
- El sistema de autenticación de dominio debe procesar tanto reportes agregados como reportes forenses.
- El sistema de autenticación de dominio debe permitir configurar de manera ordenada los protocolos de seguridad SPF, DMARC y DKIM.
- El sistema de autenticación de dominio debe permitir configurar BIML.
- El sistema de autenticación de dominio debe permitir delegar los protocolos SPF, DMARC y DKIM para ser gestionado desde el propio sistema.
- El sistema de autenticación de dominio debe permitir activar políticas restrictivas asegurando sus fuentes de correos mediante la aplicación de protocolo de DMARC.
- El sistema de autenticación de dominio debe permitir la compresión del SPF a fin de evitar el exceso de lookups.
- El sistema de autenticación de dominio debe permitir gestionar tantos dominios como sean necesarios. Ya sean activos como inactivos.
- El sistema de autenticación de dominio debe permitir aplicar políticas para que los correos provenientes de fuentes no autorizadas sean identificados y puestos en cuarentena o rechazados según corresponda.
- El sistema de autenticación de dominio debe proveer reportes periódicos y automáticos sobre el nivel de exposición de la infraestructura de envío.
- El sistema de autenticación de dominio debe permitir detectar quién envía correos a nombre del dominio que no sea parte del servidor de correos.
- El sistema de autenticación de dominio debe permitir autorizar el envío de correos sólo a remitentes que pertenezca a la institución o sean autorizados por ella.
- El sistema de autenticación de dominio debe estar alojado en una red privada y que no sea accesible fuera del ecosistema.
- El sistema de autenticación de dominio debe contar con el tráfico VLAN privada y encriptado usando SSL y TLS.
- El sistema de autenticación de dominio debe contar con un firewall que regula la carga de conectividad a la plataforma web.
- El sistema de autenticación de dominio debe contar con un sistema de prevención contra intrusos e inspección de todo tipo de tráfico.
- El sistema de autenticación de dominio debe contar con una protección anti DDoS de manera nativa.
- El sistema de autenticación de dominio debe contar con una gestión de reputación para el dominio protegido.
- El sistema de autenticación de dominio debe contar doble factor de autenticación para los usuarios.





- El sistema de autenticación de dominio debe contar gestión de permisos de administrador de cuenta, usuario de cuenta y usuario de solo lectura.
- El sistema de autenticación de dominio debe contar con integración API
- El sistema de autenticación de dominio debe permitir SSO.
- El proveedor debe entregar un acceso a la plataforma de autenticación de dominio.
- La plataforma o el servicio debe estar registrado a nombre de la institución y debe ser entregado de manera virtual.
- El sistema de autenticación de dominio debe permitir autorizar el envío de correos a fuentes o remitentes que pertenezcan a la institución o sean autorizados por ella<sup>80</sup>.
- El sistema de autenticación de dominio debe contar con una funcionalidad para conocer el estado de reputación de las fuentes que envían usando el dominio protegido.<sup>81</sup>

#### 1.6.1.9. Servicio de Detección y Respuesta de Red para brechas de amenazas

El contratista deberá incluir como parte del servicio una solución de tipo appliance de propósito dedicado para el cumplimiento del servicio requerido, en formato Rackeable; para ello debe ofrecer equipos nuevos y de tecnología vigente, se deberá adjuntar carta del fabricante indicando el cumplimiento a lo solicitado y deberá cumplir con los siguientes requisitos mínimos:

- No se aceptarán soluciones basadas en software, en la nube o virtualizadas.
- El appliance deberá cumplir mínimamente las siguientes especificaciones:
  - Throughput de Detección: 5 Gbps
  - Sesiones concurrentes (HTTP): 3M
  - Nuevas sesiones / segundo (HTTP): 200,000
  - Storage: 1 TB (SSD)
  - Interfaces: 4 x 10GE SFP+
  - Factor de Forma: 1U (opcional)<sup>82</sup>
- La solución propuesta debe soportar el modo de operación de tapping, sin ser intrusiva para la red del cliente.
- Debe incluir Análisis de Correlación de amenazas.
- Debe incluir Detección avanzada de amenazas basadas en comportamiento.
- Detección, de al menos 2,000 familias de programas maliciosos, conocidos y desconocidos, incluyendo virus, desbordamiento, gusanos, troyanos, etc.
- La solución debe ser compatible con descubrir de forma efectiva los bots de la intranet y evitar nuevos ataques de amenazas avanzadas mediante la comparación de la información obtenida con la base de datos de direcciones de C&C.
- La solución debe admitir la actualización automática de la biblioteca de firmas de defensa de Botnet/C&C.
- Más de 30.000 firmas, detección de anomalías de protocolo y detección basada en la tasa
- Firmas personalizadas, actualización de firmas push or pull automático o manual, enciclopedia integrada de amenazas
- Soportar más de 20 tipos de protocolos de detección de anomalías, incluyendo HTTP, SMTP, IMAP, POP3, VoIP, NetBIOS, VxLAN, MPLS, etc. La solución debe soportar al menos 8,000 firmas<sup>83</sup>.
- Debe admitir firmas personalizadas, manual, actualizaciones automáticas de inserción o extracción de firmas y una enciclopedia de amenazas integrada.
- Correlación entre las amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales
- Soporte para desbordamiento de búfer y detección de ataques por scripting de Cross-site.

<sup>80</sup> Texto agregado en virtud a la consulta y/u observación N° 207.

<sup>81</sup> Texto agregado en virtud a la consulta y/u observación N° 208.

<sup>82</sup> Texto agregado en virtud a la consulta y/u observación N° 353 y 380 respectivamente.

<sup>83</sup> Se suprime texto en virtud a la consulta y/u observación N° 94 y 212.



- Debe admitir detección de contraseña débil para protocolos FTP / HTTP / SMTP / POP3 / IMAP / TELNET.
- La solución debe soportar al menos 4 millones de firmas de antivirus, con actualizaciones de firma manual o automática.
- Permitir la detección de ataques de protocolos anormales, detección de ataques ARP, inundaciones de consultas DNS, inundaciones de tráfico SYN.
- La solución debe admitir informes definidos por el usuario. El informe se puede exportar al menos en formato PDF y/o ser enviada a una dirección de correo electrónico o FTP.
- La solución debe admitir configurar alarmas para la utilización del CPU, utilización de la memoria, utilización del espacio en disco, nuevas conexiones, o similares.
- La plataforma deberá contar con un sistema de monitoreo que permita tener una visión general de riesgos del estado interno de la red y zona de servidores, incluyendo activos críticos, riesgo en el anfitrión, la gravedad y el tipo de amenaza, ataque externo a geolocalizaciones, etc.
- La plataforma deberá permitir la visualización detallada del estado de amenaza para los activos críticos y otros hosts arriesgados, incluyendo el nivel de riesgo, la certeza de riesgo, ataques por geolocalización, mapeo Kill Chain y otra información estadística.
- En relación a los informes obtenidos, deberá manejar informe de Seguridad, Flujos e informes.
- Este servicio debe tener la capacidad de integrarse con el equipo de Firewall de Siguierte Generación para la detección y mitigación de las brechas de seguridad detectadas.

**1.6.1.10. Servicio de Switches Core**

- El CONTRATISTA, deberá entregar como parte del servicio una solución Switch CORE, compuesto por 02 switches de 48 puertos de fibra óptica y 01 Switch de 48 puertos de 1G Base-T; nuevos y de primer uso, que luego de terminado el servicio pasarán a ser propiedad de la entidad, y deberá contar<sup>84</sup> con las capacidades y funcionalidades técnicas mínimas requeridas siguientes:

**1.6.1.10.1. CAPACIDADES:**

**A. DOS (02) SWITCHES CORE - 48 PUERTOS FIBRA OPTICA**

- Unidades de Rack: 1 RU
- Cantidad de Puertos de Acceso: 48 x 1G (SFP)/10G(SFP+)/25G (SFP28)
- Cantidad de Puertos de Uplink: 8 x 40G/100G QSFP28 (Soporte de 100G)
- Funcionalidad de Interfaz Cruzada Dependiente del Medio (MDIX).
- Dos (02) puertos físicos para Administración, Gestión y configuración del equipo (Conexión Serial RJ45 y Conexión 100 Mbps Base-T RJ45) y un (01) puerto mediante conexión USB, destinado para función de Backup.
- Memoria DRAM: 16 GB
- Memoria SSD: 50 GB
- Indicadores LED Por puerto: Actividad, full dúplex.
- Fuente de Alimentación: 220 VAC 60 Hz.
- Soportar ahorro de energía cuando el switch no está en uso.
- Soporte para fuente de poder redundante.
- Soporte de interfaces ópticas de tipo SFP/SFP+ monomodo y multimodo
- Soporte de funcionalidad Stacking, Virtual Chassis o equivalente. Al menos 2 miembros.
- Se debe incluir el cable DAC del fabricante de los equipos, de al menos 3 metros, para el apilamiento de ambos switches.
- Fuentes de poder y ventilación hot-swappable.
- MAC addresses: 288K

**RENDIMIENTO**

- Capacidad de Conmutación Total: 4 Tbps (Full Duplex)

<sup>84</sup> Texto agregado en virtud a la consulta y/u observación N° 137, 139 y 491 respectivamente.



- Throughput: 2 Bpps
- Operación de Puertos a Line-rate en todos los puertos de acceso de manera simultanea
- VLAN IDs disponibles: por lo menos 4000
- Soporte para Jumbo Frame: 9216 bytes.

**B. 01 SWITCH 48 PUERTOS 1G BASE-T**

- Unidades de Rack: 1 RU
- Cantidad de Puertos de Acceso: 48 x 100M/1G Base-T
- Cantidad de Puertos de Uplink: 4 x 10G/25G de tipo SFP28
- Funcionalidad de Interfaz Cruzada Dependiente del Medio (MDIX).
- Dos (02) puertos físicos para Administración, Gestión y configuración del equipo (Conexión Serial RJ45 y Conexión 100 Mbps Base-T RJ45) y un (01) puerto mediante conexión USB, destinado para función de Backup.
- Memoria DRAM: 4 GB
- Storage Flash/SSD: 20 GB
- Indicadores LED Por puerto: Actividad, full dúplex.
- Fuente de Alimentación: 220 VAC 60 Hz.
- Soportar ahorro de energía cuando el switch no está en uso. (802.3az)
- Soporte para fuente de poder redundante.
- Stacking, Virtual Chassis o equivalente de por lo menos nueve (09) equipos
- Capacidad del fabric de VC = 400G (Full Duplex)
- Soporte de interfaces ópticas de tipo SFP/SFP+ monomodo y multimodo

**RENDIMIENTO**

- Capacidad de Conmutación Total: 648 Gbps
- Throughput: 515 Mpps
- Operación de Puertos a Line-rate en todos los puertos de acceso de manera simultanea
- VLAN IDs disponibles: por lo menos 4000
- Soporte para Jumbo Frame: 9216 bytes.
- Fuentes de poder y ventilación hot-swappable.
- MAC addresses: 112K

**1.6.1.10.2. SOFTWARE**

- Contar con la última versión estable del sistema operativo recomendado por el fabricante.
- Deberá tener un sistema operativo dedicado y desarrollado por el fabricante para tal equipamiento.
- Sistema operativo modular (no monolítico) con separación del plano de control del plano de datos.
- Deberá permitir crear y almacenar hasta 49 copias locales de configuraciones anteriores a la configuración de operación actual, por requerimientos de auditoría.
- A través de su sistema operativo debe permitir la comparación de la configuración activa de trabajo con las configuraciones históricas almacenadas. Esto es requerido para facilitar el pronóstico de resolución de inconvenientes.
- Se aceptarán equipos que tengan capacidad de comparar las configuraciones anteriores sobre la actual a través de una herramienta externa del mismo fabricante
- Deberá permitir realizar copia de su configuración y exportarlo mediante FTP, TFTP y USB.
- Debe proveer la funcionalidad ISSU.

**1.6.1.10.3. FUNCIONALIDADES DE RED**

- Capaz de operar en capa 2 y capa 3.
- Soporte de IPv4 e IPv6 para todas las funcionalidades de red (conmutación de nivel 2, enrutamiento y funcionalidades avanzadas de nivel 3).
- Soporte Listas de Control de Acceso en Capa 2 y Capa 3.





- Soporte para enrutamiento basado en políticas.
- Soportar protocolo Spanning-Tree.
- Los puertos deben tener la capacidad de configurar VLAN de voz y datos.
- Soporte de Protocolos:
  - IEEE 802.3 10BASE-T
  - IEEE 802.3u 100BASE-TX
  - IEEE 802.3ab 1000BASE-T, Gigabit sobre cobre.
  - IEEE 802.3z 1000BASE-X, Gigabit sobre fibra.
  - IEEE 802.3ae 10Gigabit Ethernet IEEE 802.1d, Spanning Tree Protocol
  - IEEE 802.1p, CoS Priorización de tráfico IEEE 802.1q, trunking
  - IEEE 802.1s, MSTP IEEE 802.1w, RSTP IEEE 802.1ab LLDP IEEE 802.3ad, LACP
  - IEEE 802.3x, Control de flujo
  - SNMP v1, v2c o v2 y v3.
- Soporte de 802.3af/at/bt en todos los puertos de acceso
- Soporte de calidad de servicio 802.1p y DSCP.
- Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad. Se deberá asegurar que se pueda realizar la agregación en al menos dos puertos ubicados en switches distintos.
- Soportar protocolos DHCP server y DHCP relay.
- Soporte de protocolos NTP y DNS.
- Soporte de protocolos EVPN, VxLAN para overlay en el Data Center

#### 1.6.1.10.4. GESTIÓN Y MONITOREO

- Gestión por consola y puerto independiente para gestión fuera de banda en cada switch de red.
- Permitir la administración como mínimo utilizando protocolos como SSHv2, telnet, HTTPS y SNMP. La administración HTTPS podrá ser también a través de una herramienta externa del mismo fabricante.
- Permitir múltiples sesiones simultáneas de administración.
- Incluir el soporte de SNMP v2c o v2 y v3.
- Soporte para Netflow o Sflow.
- Registro de eventos vía Syslog y Syslog Remoto.
- Soporte de protocolos de transferencia de archivos TFTP, FTP y/o SFTP.
- Soporte para permitir procesos de debug para el análisis detallado de fallas y tráfico de datos. (Opcional, siempre y cuando se ofrezca esta funcionalidad a través de algún otro mecanismo como una consola del mismo fabricante).
- Soporte para contar con herramientas que permitan recolectar datos para el análisis de tráfico en tiempo real: Debug de paquetes, Consulta a Tabla ARP, etc. Dichas herramientas podrán ser internas (mediante el switch de red) y/o externas (mediante la consola de gestión).
- Soporte de IPFlow (Sflow o Netflow) para el análisis de tráfico de red en tiempo real, para lo cual deberá exportar información según: Interfaz de Vlan o Interfaz física (en capa 3) de cada puerto del switch de red o interfaz LACP en Capa 3, etc.
- Brindar la funcionalidad de "puerto espejo" por puerto físico o grupo de puertos y también por VLAN.
- Permitir configurar sesiones de "puerto espejo" así como "puerto espejo remoto".
- Deberá poder integrarse a una consola de gestión y monitoreo de mismo fabricante a fin de ser administrado centralizadamente.

#### 1.6.1.10.5. CALIDAD DE SERVICIO (QoS)

- Debe ser capaz de implementar Clasificación, Marcado y Remarcado basado en CoS (Clase de Servicio – Nivel 2) y DSCP (Punto de Código de Servicios Diferenciados – nivel 3).
- Deberá poder implementar al menos 8 colas de prioridad de hardware por puerto.
- Debe permitir la clasificación y priorización de paquetes con base en información de capa 2, 3 y 4 del modelo OSI, para al menos: dirección MAC, dirección IP, número de puerto TCP o UDP, valor del campo COS (802.1p) y valor del campo TOS (con precedencia IP y DSCP).
- Debe tener una cola de prioridad QoS (strict priority).





1.6.1.10.6. MECANISMOS DE SEGURIDAD

- Seguridad por puerto, en base a la dirección MAC.
- Supresión y limitación de tormentas de broadcast, multicast y unicast.
- Control de acceso centralizado mediante RADIUS. Se precisa que lo solicitado es la integración con un servicio RADIUS y no que se tenga incorporada la funcionalidad de Radius Server en los equipos.
- Permitir personalizar cómo mínimo 3 niveles de privilegios de acceso para administración y monitoreo por consola, Telnet, SSH y RADIUS, según los siguientes perfiles: Administrador, Operador (Control de interfaces, protocolos, consultas ARP, consultas tabla MAC, Debug de paquetes, etc.) y usuario simple (lectura).
- La finalidad de este requerimiento es personalizar los comandos que se puedan asignar a cada rol o perfil de acceso al Switch de red.
- Permitir la restricción del acceso (listas de control de acceso) a nivel de administración desde múltiples IP.
- Debe soportar: DHCP Snooping, Port Security, IP source guard, Dynamic ARP Inspection o equivalentes.
- Soporte de Vlan nativa y que permita aplicar tagging en las interfaces trunk.
- Soporte para Vlan privada.
- El equipo deberá soportar 802.1ae, con la finalidad de cifrar las comunicaciones en la LAN.
- La versión del sistema operativo no debe poseer vulnerabilidades DoS conocidas a la fecha de publicación de las bases.

1.6.1.10.7. ACCESORIOS

- Se deberán incluir por cada equipo de Core, 15 Transceivers monomodo de 10G, 17 Transceivers multimodo de 10G y 5 Transceivers de SFP+ a RJ45.

1.6.1.10.8. SOPORTE DE FABRICANTE

- Se deberá incluir el soporte de fabricante en modalidad NBD durante 3 años

1.6.1.11. Servicio de CyberDefensa y SIEM

El CONTRATISTA, deberá entregar un servicio de ciberdefensa y SIEM propio o de un tercero, este servicio debe ser operado por su CyberSOC certificado ISO27001 en gestión de incidentes, gestión de cambios y ciberseguridad. Este servicio deberá permitir mediante el análisis de logs de la solución de seguridad propuesta, permita realizar investigaciones y escalar incidentes con las siguientes características:

- Deberá incluir el servicio de SIEM para los equipos de seguridad parte de la presente propuesta y para 50 servidores Windows y 1 Directorio Activo.
- Incluir capas adicionales como analítica de comportamiento de usuarios y entidades (UEBA) o analítica de comportamiento de usuarios (UBA)<sup>85</sup>, orquestación, automatización y respuesta de seguridad (SOAR), para procesar múltiples eventos de seguridad y mecanismos de detección propietarios basados en Inteligencia artificial totalmente integrados al servicio.
- Con el objetivo de validar y dar seguimiento a las investigaciones de ciberseguridad, el CONTRATISTA deberá entregar un Portal web seguro con doble factor de autenticación para revisar las investigaciones.
- El portal debe actuar como una interfaz gráfica de usuario (GUI) que muestre investigaciones que fueron realizadas por los componentes (SIEM, UEBA o UBA<sup>86</sup>, SOAR, I.A.), es decir que la herramienta cuenta con la auditoria de usuarios que realizaron cambios en la misma.

<sup>85</sup> Texto agregado en Virtud a la consulta y/u observación N° 97

<sup>86</sup> Texto agregado en Virtud a la consulta y/u observación N° 98 y 101 respectivamente



- Capas adicionales al SIEM como analítica de comportamiento de usuarios (UEBA), orquestación, automatización y respuesta de seguridad (SOAR), para procesar múltiples eventos de seguridad y mecanismos de detección propietarios basados en Inteligencia artificial totalmente integrados al servicio.
- Monitoreo 24x7 identificando amenazas cibernéticas que puedan afectar la operación.
- Inteligencia de amenazas mediante actualizaciones de indicadores de compromiso (IOC) de múltiples fuentes que incluyen indicadores internos extraídos de eventos, comunidades de código abierto, redes sociales, inteligencia técnica y/o inteligencia procedente de la Deep and Dark Web. Las fuentes de inteligencia de amenazas deberán ser enviadas al gestor de eventos de la seguridad de la información para correlacionar y generar detecciones.
- Caza de amenazas sobre el gestor de eventos de seguridad, identificando, evaluando y mejorando la capacidad de detección mediante búsqueda exhaustiva de ciber-amenazas y actividades maliciosas.
- Respuesta y mitigación de incidentes en tiempo real ante ciber- amenazas.
- Optimización de procesos consistentes de desarrollo y aprendizaje que incluyan optimización de reglas, actualizaciones y sugerencias de implementación de nuevas tecnologías de detección de amenazas cibernéticas.
- opcionalmente <sup>87</sup> la Inteligencia de amenazas debe comprobar todas las comunicaciones salientes; alertar sobre la comunicación con la IP, dominios y URL maliciosos; y finalizar la conexión inmediatamente, todo esto sucede en tiempo real.
- Investigación forense de procesos en curso de presuntas actividades maliciosas y amenazas cibernéticas incluyendo el análisis post mortem de incidentes verificados, identificando el origen del ataque, la causa raíz y proporcionar información sobre quién inició el ataque. Mínimo de 4 horas mensuales de ser requerido.
- El servicio deberá tener la capacidad de integrarse a cualquier solución de seguridad, fuente de registro y Endpoint.
- Configuración personalizable de notificaciones vía email (notificaciones, recomendaciones, acciones pendientes, nuevas investigaciones, escalamiento de una investigación en curso, modificación del estado de una investigación en curso)
- Este servicio debe tener la capacidad de ser retroalimentado por un emisor externo de incidentes para que de esta manera no sea juez ni parte en la emisión de investigaciones, a fin de asegurar la imparcialidad y permitir que la entidad pueda dar seguimiento de los tiempos de resolución y atención del postor.

1.6.1.12.

**SERVICIO DE RESPALDO EN NUBE**

- Plataforma tecnológica la cual debe contar por lo menos con una certificación de continuidad de negocio en los procesos de conectividad.
- Modalidad Software como Servicio (SaaS Software as a Service), la cual debe encontrarse en un centro de datos. La disponibilidad del almacenamiento en este centro de datos debe ser de mínimo de 99.9% para garantizar la alta disponibilidad de este.
- La interacción del servicio de almacenamiento con la infraestructura local la UNIVERSIDAD NACIONAL DE TRUJILLO se podrá realizar a través del ancho de banda solicitado en el presente requerimiento entre la UNIVERSIDAD NACIONAL DE TRUJILLO y la nube como contingencia. Por lo indicado, se podrá enviar información (servidores virtuales, estaciones de trabajo, medios de almacenamiento, carpetas, bases de datos y archivos de cualquier tipo) hacia el servicio de almacenamiento con fines de trasladar la información sensible de la entidad hacia un sitio externo.
- Tamaño de almacenamiento mínimo: 20 TB.
- El almacenamiento de la nube deberá ser presentado a los servidores vía protocolos estándar HTTP y/o NFS.

<sup>87</sup> Se agrega Texto en Virtud a la Consulta y/u Observación N° 99



- La plataforma debe contar con cifrado militar y protección con contraseña.
- La solución de respaldo en la nube es por un periodo de 24 meses contados a partir del día siguiente de entregadas las credenciales de acceso al correo dsc@unitru.edu.pe
- El proveedor brindará soporte técnico, a partir del día siguiente de entregadas las credenciales de acceso al correo dsc@unitru.edu.pe de acuerdo a las siguientes características:
  - ✓ Soporte remoto: 7 días por 24 horas debe incluir feriados, sábados y domingos.
  - ✓ Registrar incidentes por sistema de tickets reportados por correo electrónico, el proveedor deberá indicar la dirección de correo electrónico al cual se reportarán, dicho correo deberá ser comunicado a la Oficina de Tecnologías de la Información.

#### 1.6.1.12. SOPORTE TÉCNICO

##### • GESTIÓN DEL SERVICIO

- El contratista deberá garantizar un eficiente sistema de gestión de sus redes de comunicación. El centro de gestión deberá estar en capacidad de realizar acciones de controles preventivos, correctivos y pruebas técnicas. Se requiere un (01) mantenimiento preventivo anual para toda la solución.
- El contratista deberá garantizar el profesionalismo, responsabilidad y conocimientos técnicos de su personal en los centros de llamadas de reportes de fallas, centros de gestión, y personal de reparación de averías.
- La Universidad Nacional de Trujillo se reserva la potestad de constatar la información presentada por el contratista en cualquier momento.
- Durante el periodo de prestación del servicio, se evaluarán los tiempos de respuesta y la calidad del servicio, a fin de que el Universidad Nacional de Trujillo determine las correcciones necesarias si fuera el caso.
- Para la atención del servicio es indispensable que el contratista cuente con local propio o alquilado<sup>88</sup> en la ciudad de Trujillo. Así mismo deberá contar con personal técnico capacitado a fin de dar una mejor solución al problema.

##### • ATENCIÓN DE AVERÍAS O FALLAS

- Se entenderá por avería a una interrupción total del servicio, cabe precisar que no se considerará para el cálculo de penalidades por indisponibilidad del servicio las averías parciales y/o degradaciones del servicio, no obstante, el contratista tiene que brindar los recursos necesarios a tiempo completo durante el horario normal de trabajo para restaurar el servicio a niveles satisfactorios y teniendo como plazo máximo de tiempo de reparación total de las degradaciones del servicio 24 horas.
- Toda actividad o provisión de bienes que tenga que ejecutar el contratista para subsanar la avería serán sin costo alguno para la Universidad Nacional de Trujillo, salvo el caso en que la avería sea imputable a la Universidad Nacional de Trujillo.
- Se entenderá por Tiempo de Atención, al tiempo transcurrido desde que se detecta la avería hasta que la Universidad Nacional de Trujillo comunique la avería al contratista del servicio y se le brinde un ticket por parte del centro de gestión del contratista. Este tiempo no deberá exceder de dos (02) horas.
- Se entenderá por Tiempo de Subsanación, al tiempo transcurrido entre la comunicación al contratista de la existencia de una avería, por parte de la Universidad Nacional de Trujillo (llamada de servicio) o por el Centro de Gestión de Redes del contratista, y la subsanación de la misma a su satisfacción. Este tiempo empezará a correr después de generado el ticket por el centro de gestión del contratista. Este tiempo no deberá exceder de cuatro (04) horas para la ciudad Universitaria (Sede principal), Facultad de Medicina, Sede Local Central, Sede dirección de planificación (zepita), Consultorio jurídico gratuito; de ocho (08) horas para clínica estomatológica de Moche; y de doce (12) horas para ciudad universitaria Guadalupe, campus universitario Santiago de chuco, campus universitario Huamachuco. Estos tiempos aplican para el servicio de internet y transmisión de datos.

<sup>88</sup> Texto agregado en virtud a la consulta y/u observación N° 519



- Para las soluciones de Protección contra Intrusos dedicado en el perímetro, Solución de seguridad perimetral en alta disponibilidad, AntiDDoS Local, Detección y Respuesta de Red para brechas de amenazas y Servicio de Switches Core, se aceptará un tiempo de reposición de equipos en caso de fallas de máximo setenta y dos (72) horas.
- De presentarse problemas de Planta Externa ajenas al contratista, el tiempo de subsanación de la avería podría tomar un tiempo adicional de hasta 08 horas adicionales para la solución.
- El tiempo de subsanación de averías no aplica solo en los siguientes casos:
  - Cualquier demora por no poder contactar con el representante técnico de la Universidad Nacional de Trujillo en el sitio de incidencia o si este no puede brindar acceso al sitio o lugar de incidencia.
  - Cualquier error en la información proporcionada por la Universidad Nacional de Trujillo que pueda afectar el rápido despliegue del recurso humano o material del contratista.
  - Cualquier demora por no contar con condiciones climatológicas favorables para realizar trabajos en altura, en horario nocturno, entre otros que impliquen riesgos al realizar trabajos en altura.
  - Razones de fuerza mayor (ej. Inaccesibilidad del sitio o localidad debido a desastres, bloqueo de carreteras, permisos de autoridades de Gobierno, otros.)
- Se aplicará parada de reloj en el caso que no se tengan accesos a las instalaciones de la Universidad Nacional de Trujillo por horario fuera de oficina, factores externos entre otros.
- La Universidad Nacional de Trujillo solamente reportará a un único número telefónico el cual será una ventanilla única que atenderá todas las averías del servicio contratado, permitiendo un adecuado control, gestión y seguimiento de la misma, debiendo indicar número telefónico. El contratista del servicio deberá contar con un número gratuito para la atención de las llamadas. Para la suscripción el contrato, deberá detallar el número completo y las opciones de atención.
- La Universidad Nacional de Trujillo podrá efectuar llamadas de servicio de lunes a domingo incluyendo feriados desde las 00:00 hasta las 24:00 horas. El contratista deberá contar con un centro de atención de llamadas de reparación o asistencia técnica instalado de tal manera que le asegure a la Universidad Nacional de Trujillo que se encuentra en condiciones de cumplir con lo estipulado en las bases.
- El postor deberá sustentar experiencia en respuesta frente a incidentes de seguridad.
- El contratista deberá contar con un centro de operaciones de seguridad (SOC – Security Operation Center), propio o tercerizado y con certificación ISO 27001 de al menos 03 años de antigüedad; este centro de operaciones debe estar disponible para brindar asistencia las 24 horas del día los 365 días del año, además deberá cumplir con las siguientes funciones: correlación de eventos de seguridad, monitoreo estratégico, Threat Intelligence, respuesta a incidentes e investigación forense.

#### 1.6.1.13. CAPACITACIÓN Y/O ENTRENAMIENTO

- El postor deberá brindar capacitación oficial en seguridad de sistemas de información para dos<sup>89</sup> tres (03) participantes e incluir el voucher de examen, que permita al personal de la Oficina de Tecnologías de la Información validar y acreditar conocimientos técnicos y administrativos para diseñar, instalar & operar los sistemas de seguridad core así como la gestión de la información de los cada vez más complejos ataques cibernéticos. La capacitación será impartida en idioma español y podrá ser entregada de manera presencial en el Centro de Entrenamiento que el Postor determine o podrá ser de manera virtual a través de una plataforma educativa provista por el Centro de Entrenamiento. El centro de Entrenamiento deberá acreditar representación oficial y vigente de la institución a la que pertenezca la certificación oficial.
- El postor deberá brindar capacitación oficial en ciberseguridad para 01 (un) participante, deberá cubrir los siguientes temas: criptografía, seguridad web, seguridad OSINT, vulnerabilidades, seguridad en redes corporativas, seguridad en arquitecturas

<sup>89</sup> Texto suprimido en virtud a la consulta y/u observación N° 101, 229, 247 y 510 respectivamente.



basadas en Linux, malware y códigos maliciosos, desarrollo seguro y gestión de identidad. La capacitación será impartida en idioma español y podrá ser entregada de manera presencial en el Centro de Entrenamiento que el Postor determine o podrá ser de manera virtual a través de una plataforma educativa provista por el Centro de Entrenamiento. El centro de Entrenamiento deberá acreditar representación oficial y vigente de la institución a la que pertenezca la certificación oficial.

- Las capacitaciones podrán brindarse luego de iniciar el servicio y hasta en un plazo de 180 días calendarios<sup>90</sup>.

## 1.6.2. CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE LOS SERVICIOS

### 1.6.2.1. DISPONIBILIDAD DEL SERVICIO

- La Disponibilidad del Servicio contempla una medición mensual y se calculará mediante la siguiente fórmula:

$$DS = \frac{(TM - TAM) * 100}{TM}$$

DS=Disponibilidad del servicio

TM= Tiempo mensual expresado en Minutos

TAM= Tiempo de Avería Mensual expresado en Minutos

Ejemplo: Si un enlace tuviera 5 caídas en 1 mes de 1 hora de duración cada caída por causas atribuibles al contratista, la disponibilidad será:

TM= 60x24x30 (en 1 mes con 30 días calendario) = 43200 minutos

TAM= 5 horas = 300 minutos.

$$DS = \frac{(43200 - 300) * 100}{43200} = 99.3\%$$

- En caso la indisponibilidad del Servicio sea atribuible a terceros, esta no será considerada en el cálculo de penalidades, siempre que esta sea debidamente sustentada.
- El servicio de internet y demás servicios deberán ser brindados las 24 horas del día, los siete (07) días de la semana, los trescientos sesenta y cinco (365) días del año con una disponibilidad de:
  - Servicio de internet mensual debe ser de mínimo 99.90%
  - Servicio de transmisión de datos mensual en las sedes remotas deberá ser de mínimo 96.66%.
- En relación al servicio de seguridad perimetral en alta disponibilidad, el nivel de disponibilidad no se verá afectado, ni se aplicará penalidades ante la avería de uno (01) de los equipos, siempre y cuando se siga brindando el servicio con todas las funcionalidades requeridas. El cambio del equipo dependerá de los plazos de ejecución del RMA del fabricante.

### 1.6.2.2. CONDICIONES DEL SERVICIO

- El contratista para el periodo de instalación y post instalación deberá asignar a un Jefe de proyecto.
- El personal técnico deberá poseer experiencia en implementaciones de última milla para la realización del mismo tipo de servicios.
- El contratista deberá garantizar, para cada uno de los enlaces, los parámetros de disponibilidad mensual, ancho de banda y calidad del servicio especificado en los requerimientos mínimos para el servicio de Internet y transmisión de datos.
- La implementación del servicio debe incluir todos los componentes. Por lo tanto, la Universidad Nacional de Trujillo (UNT) proveerá lo siguiente:
  - Tomacorrientes.
  - Energía estabilizada 220 VAC, UPS.

<sup>90</sup> Texto agregado en virtud a la consulta y/u observación N° 133 y 143 respectivamente.



- Tendido de cableado eléctrico
  - Sistema de pozo a tierra menor o igual a 5 Ohm.
  - Cableado estructurado correspondiente a la red LAN de la Entidad.
  - Temperatura y humedad adecuados para el funcionamiento de equipos de red.
- El contratista deberá realizar los cambios de configuración solicitados por la Universidad Nacional de Trujillo (UNT) durante la vigencia del contrato sin que esto implique costo alguno para la Universidad Nacional de Trujillo (UNT). La atención a estos no deberá exceder las 04 horas luego de solicitado el requerimiento.
  - Los cambios en las configuraciones, se encuentran referidos a cambios dentro de las políticas ya definidas durante el proceso de implementación, mas no aplicaría en cambios de configuraciones derivados de solicitudes en cambio de topología/ arquitectura de la red, puesto que esto demandaría mayor tiempo de ejecución. En caso de requerimientos que ameriten trabajos en ventana de mantenimiento o que necesiten de una configuración especial, se podrá tener un mayor tiempo de atención previa coordinación con la Entidad, sin que se aplique penalidades de algún tipo

#### 1.6.2.3. INSPECCIÓN Y PRUEBAS

- El contratista y el personal correspondiente de Universidad Nacional de Trujillo, una vez terminada la instalación, realizarán en forma conjunta la inspección y pruebas sobre los equipos instalados, de tal forma que le permita a Universidad Nacional de Trujillo establecer que los servicios serán brindados de conformidad con lo requerido en las bases y en la propuesta técnica del contratista.
- Las pruebas se realizarán en los lugares de instalación. Los costos que demanden las mismas, no implicarán en ningún caso reconocimiento de gastos por parte de Universidad Nacional de Trujillo y deberán ser provistos por el contratista.
- El proveedor deberá realizar pruebas de saturación con un equipo generador de tráfico, para lo cual la Universidad otorgará las facilidades respectivas para la ejecución de estas pruebas.
- La omisión en la oferta de algún producto que al momento de las pruebas resulte necesario para la provisión de los servicios, o para el cumplimiento de las especificaciones funcionales y/o técnicas ofrecidas, obligará al contratista a brindarlo sin cargo alguno.
- Cualquier defecto notificado por la Universidad Nacional de Trujillo (UNT) al contratista durante la realización de las pruebas de aceptación, será rectificado por este sin cargo alguno, teniendo como plazo máximo 5 (cinco) días hábiles a partir de su notificación.
- Una vez realizados los procedimientos de inspección y pruebas a conformidad de la Universidad Nacional de Trujillo, está levantará y entregará al contratista el Acta de Conformidad e Inicio de Servicios mediante un documento formal.

#### 1.6.3. ACTIVIDADES

- Activación del servicio de internet de 2. 6 Gbps
- Activación de un enlace de contingencia de la misma capacidad de ancho de banda contratado (Activo/Pasivo) el cual incluye Router y enlace de Fibra Óptica.
- Activación del servicio de transmisión de datos para la interconexión de las sedes remotas con la Ciudad Universitaria – Trujillo
- Activación de Solución de Seguridad para protección de ataques DDoS
- Activación de la solución de seguridad Firewall HA
- Testeo de servicios contratados, entrega de informe, conformidad e inicio de contratación.
- Capacitación al personal de la Oficina de Tecnologías de la Información
- Activación del servicio de IPS Perimetral
- Activación del servicio de Análisis y Detección de Brechas de Amenazas en la zona de servidores.
- Activación del servicio de monitoreo y correlación de eventos.
- Activación del servicio de monitoreo de red (plataforma)

#### 1.6.4. PLAN DE TRABAJO

- El contratista ganador de la buena pro deberá presentar un plan de trabajo del servicio a brindar durante los quince (15) primeros días calendarios después de haber suscrito el contrato, con la finalidad de que la entidad tome las medidas correspondientes del caso.





**1.6.5. REQUISITOS SEGÚN LEYES, REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS, REGLAMENTOS Y DEMÁS NORMAS**

- El contratista contará con la acreditación correspondiente para brindar los servicios requeridos.
- El contratista contará con los permisos y autorizaciones para la prestación del servicio refrendado por las entidades competentes (MTC).
- De ser el caso el contratista deberá contar o tramitar los permisos municipales para brindar el servicio sin que esto afecte al plazo de implementación del servicio.

**1.6.6. SEGUROS**

- El personal a realizar las labores de implementación, mantenimiento y soporte técnico en las instalaciones de la UNT deberá contar con Seguro Complementario de Trabajo de Riesgo como medida preventiva obligatoria.

**1.6.7. LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO**

**1.6.7.1. LUGAR**

- La prestación del servicio se realizará en las sedes indicadas en la Tabla N° 01. SEDES UNT.

**1.6.7.2. PLAZO**

- Plazo de implementación del servicio: El tiempo de implementación de todo lo solicitado se realizará como máximo en noventa (90) días calendarios contados a partir del día siguiente de la firma de contrato.
- Plazo de duración del servicio: es de 730 días calendarios ~~o 02 años~~<sup>91</sup>, contados a partir del día siguiente del acta de activación de servicio.

**1.6.8. RESULTADOS ESPERADOS**

- Obtener un servicio de internet de 2.6 Gbps
- Realizar la interconexión de todas las sedes de la UNT.
- Mejorar las condiciones actuales de gestión y servicios a través del servicio de internet, datos y seguridad.

**REQUISITOS Y RECURSOS DEL CONTRATISTA**

**1.7.1. REQUISITOS DEL CONTRATISTA**

- Ser una empresa prestadora de servicios de telecomunicaciones con experiencia en el servicio materia de objeto de la presente contratación o similares con experiencia brindando servicio de internet en el Perú.
- Contar con la acreditación correspondiente para brindar los servicios requeridos, permisos que deben estar refrendados por las entidades competentes (MTC).
- El contratista deberá ser miembro del NAP Perú, con conexión igual o superior a los 10 Gbps y con infraestructura propia no arrendada a terceros.

**1.7.2. RECURSOS A SER PROVISTOS POR EL CONTRATISTA**

**1.7.2.1. EQUIPAMIENTO**

- El servicio deberá incluir los equipos de acceso (CPE)
- Los equipos de comunicación a instalarse y/o requeridos para los servicios de internet y transmisión de datos deben estar vigentes tecnológicamente durante el plazo de contrato.

**1.7.2.2. PERSONAL**

**A. PERSONAL CLAVE**

- **Jefe de proyecto (1)**
  - Profesional titulado en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o carreras afines, con experiencia mínima de dos (02) años desempeñándose como jefe de proyectos en servicios de comunicaciones.
- ~~Especialista en ciberseguridad (1)~~

<sup>91</sup> Texto suprimido en virtud a la consulta y/u observación N° 05; 150, 151, 235 y 260 respectivamente.



~~Profesional técnico o bachiller o titulado en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o computación e informática o Redes de computadoras y comunicación de datos o carreras afines, con experiencia mínima de un (01) año implementando soluciones firewalls y herramientas SIEM.~~

• **Especialista de seguridad de firewalls (1)**

~~Profesional técnico o bachiller o titulado en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o Computación e informática o Redes de computadoras y comunicación de datos o carreras afines, con experiencia mínima de un (01) año implementando firewalls de los que oferte el contratista.~~

• **Especialista en sistemas de gestión y monitoreo (1)**

~~Profesional técnico o titulado o bachiller en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o Computación e informática o Redes de computadoras y comunicación de datos o carreras afines, con experiencia mínima de un (01) año implementando herramientas de gestión y monitoreo de los que oferte el contratista.<sup>92</sup>~~

**B. OTRO PERSONAL**

• **Especialista en ciberseguridad (1)**

Profesional técnico o bachiller o titulado en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o computación e informática o Redes de computadoras y comunicación de datos o carreras afines, con experiencia mínima de un (01) año implementando soluciones firewalls y herramientas SIEM.

• **Especialista de seguridad de firewalls (1)**

Profesional técnico o bachiller o titulado en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o Computación e informática o Redes de computadoras y comunicación de datos o carreras afines, con experiencia mínima de un (01) año implementando firewalls de los que oferte el contratista.

• **Especialista en sistemas de gestión y monitoreo (1)**

Profesional técnico o titulado o bachiller en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o Computación e informática o Redes de computadoras y comunicación de datos o carreras afines, con experiencia mínima de un (01) año implementando herramientas de gestión y monitoreo de los que oferte el contratista.<sup>93</sup>

• **Técnicos instaladores**

- Profesional técnico, o Bachiller, o Titulado en Sistemas, o Computación e informática o Redes de computadoras y comunicación de datos o telecomunicaciones o electrónica o carreras afines, con experiencia mínima de un (1) año en la supervisión y/o conducción en implementaciones de última milla para la realización de servicios materia de objeto de la presente contratación o similares.

**1.8. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN**

**1.8.1. OTRAS OBLIGACIONES**

**1.8.1.1. OTRAS OBLIGACIONES DEL CONTRATISTA**

- El contratista deberá tomar en cuenta todas las configuraciones de red con las que cuenta actualmente la Universidad Nacional de Trujillo a fin de que contemplen las mismas para su implementación y evitar afectaciones en los servicios.
- El contratista será responsable de la configuración en los equipos de comunicación que entregará como parte de sus servicios de comunicación (incluyendo las soluciones de seguridad gestionada y los equipos de transmisión)
- Cualquier rotura o deterioro que se produzca como consecuencia de la realización de los trabajos que son objeto de la presente contratación, será de exclusiva responsabilidad del contratista, el mismo que deberá reponer o reparar a todo costo y a entera satisfacción de la Universidad Nacional de Trujillo.

<sup>92</sup> Texto suprimido en virtud a la consulta y/u observación N° 413.

<sup>93</sup> Texto agregado en virtud a la consulta y/u observación N° 413



- El contratista deberá realizar los trabajos dentro y fuera del local incluyendo trámites de permisos Municipales y otros sin que esto implique costo adicional a la UNT.
- Si para la instalación de los servicios es necesario realizar obras civiles los costos serán asumidos por el proveedor.

#### 1.8.1.2. OTRAS OBLIGACIONES DE LA ENTIDAD

- El personal de la Universidad nacional de Trujillo brindará las facilidades de acceso a las instalaciones para la implementación, soporte y mantenimiento del servicio de manera oportuna.
- De requerirse el contratista podrá solicitar una visita técnica guiada, en coordinación con la DSC de la UNT.

#### 1.8.2. ADELANTOS

- No aplica

#### 1.8.3. SUBCONTRATACIÓN

- El proveedor es el único responsable de la ejecución total de las prestaciones frente a la entidad, las obligaciones y responsabilidades derivadas de la subcontratación son ajenas a la entidad.
- El subcontratista debe estar inscrito en el Registro Nacional de Proveedores y no debe estar suspendido o inhabilitado para contratar con el Estado. El subcontrato no puede exceder 40% del monto total del contrato.

#### 1.8.4. CONFIDENCIALIDAD

- El contratista y su personal se obliga a mantener y guardar estricta reserva y absoluta confidencialidad sobre todos los documentos e informaciones de la Universidad Nacional de Trujillo (UNT) a los que tenga acceso en ejecución del presente contrato. En tal sentido, El contratista y su personal deberán abstenerse de divulgar tales documentos e informaciones, sea en forma directa o indirecta, a personas naturales o jurídicas, salvo autorización expresa y por escrito de la Universidad Nacional de Trujillo (UNT). Asimismo, El contratista y su personal conviene en que toda la información suministrada en virtud de este contrato es confidencial y de propiedad de la Universidad Nacional de Trujillo (UNT), no pudiendo El contratista y su personal usar dicha información para uso propio o para dar cumplimiento a otras obligaciones ajenas a las del presente contrato.
- Los datos de carácter personal entregados por la Universidad Nacional de Trujillo (UNT) a El contratista y su personal, y obtenidos por estos durante la ejecución del servicio, única y exclusivamente podrán ser aplicados o utilizados para el cumplimiento de los fines del presente documento contractual. El contratista se compromete a cumplir con lo indicado en la Ley N° 29733, Ley de protección de datos personales
- El contratista deberá adoptar las medidas de índole técnica y organizativa necesarias para que sus trabajadores, directores, accionistas, contratistas y en general, cualquier persona que tenga relación con El contratista no divulgue a ningún tercero los documentos e informaciones a los que tenga acceso, sin autorización expresa y por escrito de la Universidad Nacional de Trujillo (UNT), garantizando la seguridad de los datos de carácter personal y evitar su alteración. Asimismo, El contratista y su personal se hacen responsables por la divulgación que se pueda producir, y asumen el pago de la indemnización por daños y perjuicios que la autoridad competente determine.
- La obligación de confidencialidad establecida en la presente cláusula seguirá vigente incluso luego de la culminación del presente contrato, hasta por tres (03) años.
- El incumplimiento de lo establecido en la presente cláusula, por parte del contratista y su personal, constituye causal de resolución del presente contrato.
- Resulte accesible al público por causa distinta del incumplimiento de la obligación de confidencialidad por la parte receptora.
- Haya sido publicada con anterioridad a la fecha de la firma de contrato.
- Se encuentre en poder de la Parte receptora y no esté sujeta a cualquier otro impedimento o restricción puesto de manifiesto a la otra Parte en el momento de la revelación o luego de ella.





- Sea recibida a través de terceros sin restricciones y sin que implique incumplimiento del Contrato.
- Sea independientemente desarrollada por la Parte receptora, siempre que no se hubiese utilizado para ello la información confidencial proporcionada por la otra Parte.
- Deba ser revelada para dar cumplimiento de una orden de naturaleza judicial o administrativa, en cuyo caso la Parte receptora deberá informar a la otra Parte en forma inmediata a la sola recepción de la citada orden<sup>94</sup>.

#### 1.8.5. MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

- El contratista en el plazo de ejecución será supervisado por personal asignado de la Oficina de tecnologías de la información de la UNT, para la realización de sus labores dentro de las instalaciones de la Universidad.

#### 1.8.6. CONFORMIDAD DE LA PRESTACIÓN

- El director de la Oficina de tecnologías de la información de la UNT, brindará la conformidad de la instalación y de la prestación mensual del servicio previa revisión de los informes solicitados.

#### 1.8.7. FORMA DE PAGO

- El pago se realizará mensualmente en 24 armadas iguales, luego de la conformidad del servicio por parte de la Oficina de tecnologías de la información de la UNT.

#### 1.8.8. PENALIDADES

- **PENALIDAD POR MORA EN LA IMPLEMENTACIÓN DEL SERVICIO (Hasta el 10% por incumplimiento de la facturación total)**

En caso de retraso injustificado del contratista en la implementación del servicio (75 días calendario), la Entidad aplica automáticamente una penalidad por mora por cada día de atraso, de conformidad con el artículo 162 del Reglamento, y de acuerdo a la siguiente fórmula

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{monto vigente}}{0.25 \times \text{plazo vigente en días}}$$

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.

Cuando se llegue a cubrir el monto máximo de la penalidad por mora, LA ENTIDAD puede resolver el contrato por incumplimiento.

#### 1.8.9. OTRAS PENALIDADES APLICABLES

N°	INCUMPLIMIENTO	PENALIDAD
1	Disponibilidad del <b>servicio de Internet</b> menor al 99.90% mensual	Hasta el 5% por incumplimiento de la facturación mensual.
2	Disponibilidad del <b>servicio de transmisión de datos</b> menor al 96.66% mensual	Hasta el 5% por incumplimiento de la facturación mensual.

Cálculo del costo por Hora:

<sup>94</sup> Texto agregado en Virtud a la consulta y/o observación N° 127



Donde:

$$C = \frac{FM}{M * H}$$

FM: Facturación mensual del servicio de internet o transmisión de datos

M: Días del mes (30 días)

H: Horas del día (24 Horas)

- Dado que cualquiera de los servicios también podría depender de una mala manipulación del usuario final se entenderá como penalidad a los problemas de interrupción total del servicio detectados a nivel de conexión directa al Router principal.
- El procedimiento mediante el cual se verificarán los supuestos a penalizar será mediante un informe de la Oficina de Tecnologías de la Información.

#### 1.8.10. RESPONSABILIDAD POR VICIOS OCULTOS.

- El plazo será de dos (02) años uno (01) año<sup>95</sup> de responsabilidad del contratista por vicios ocultos

## II. REQUISITOS DE CALIFICACIÓN

### 2.1. CAPACIDAD LEGAL

#### 2.1.1. Habilitación

- **Requisitos:**
  - El contratista debe estar debidamente registrado y habilitado ante las entidades y en conformidad con lo establecido por la Ley general de telecomunicaciones, como empresa proveedora de telecomunicaciones.
  - El contratista debe pertenecer al NAP (Network Access Point) – Perú activo y operativo.
- **Acreditación:**
  - Copia simple de la Resolución del ministerio de transportes y comunicaciones; o copia del certificado de registro de empresas prestadoras de servicios de valor añadido expedido por Dirección general de concesiones en comunicaciones del MTC; o impresión simple del registro de empresas prestadoras de servicios de valor añadido publicadas en la página web MTC; o impresión simple del registro de empresas prestadoras de servicios de valor añadido publicadas en la página web MTC
  - Constancia expedida por el mismo NAP PERÚ o la captura de pantalla de la página web del NAP PERÚ, donde se indique que el contratista es asociado de la referida institución.

### 2.2. CAPACIDAD TÉCNICA Y PROFESIONAL (Tercerizado y/o propio)

#### 2.2.1. Calificaciones del personal clave

##### 2.2.1.1. Formación académica

- **Jefe de proyecto:** Profesional titulado en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o carreras afines.
- ~~**Especialista en ciberseguridad:** Profesional técnico o Bachiller o titulado en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o Computación e informática o Redes de computadoras y comunicación de datos o carreras afines.~~
- ~~**Especialista de seguridad de firewalls:** Profesional técnico o bachiller o titulado en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o Computación e informática o Redes de computadoras y comunicación de datos o carreras afines.~~
- ~~**Especialista en sistemas de gestión y monitoreo:** Profesional técnico o Titulado o bachiller en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o Computación e informática o Redes de computadoras y comunicación de datos o carreras afines.<sup>96</sup>~~

**Acreditación:** El título profesional o grado requerido será verificado por el comité de

<sup>95</sup> Texto suprimido y agregado en virtud a la consulta y/u observación N° 146, 148, 252 y 256 respectivamente.

<sup>96</sup> Texto suprimido en virtud a la consulta y/u observación N° 413



selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <https://enlinea.sunedu.gob.pe/> o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: <http://www.titulosinstitutos.pe/>, según corresponda.  
En caso El título profesional requerido no se encuentre inscrito en el referido registro, el contratista debe presentar la copia del diploma.

#### 2.2.1.2. Capacitación

- **Jefe de proyecto:** 120 horas lectivas en gestión de telecomunicaciones y/o gestión de proyectos y/o certificado PMP.
- ~~**Especialista en ciberseguridad:** certificado a nivel especialista otorgado por una institución internacional de ciberseguridad.~~
- ~~**Especialista de seguridad de firewalls:** certificado técnico vigente a nivel asociado o profesional en el manejo de la solución firewall ofertado por el contratista.~~
- ~~**Especialista en sistema de gestión y monitoreo:** certificado técnico vigente a nivel asociado o profesional en el manejo del sistema de gestión y monitoreo ofertado por el contratista.<sup>97</sup>~~

**Acreditación:** Se acreditará con copias simples de los certificados o diplomas u otros.

#### 2.2.2. Experiencias del personal clave

- **Jefe de proyecto:** experiencia mínima de DOS (02) años, desempeñándose como Jefe de Proyectos en servicios de comunicaciones.
- ~~**Especialista en ciberseguridad:** experiencia mínima de UN (01) año, en implementación de soluciones firewall, y herramientas SIEM~~
- ~~**Especialista de seguridad de firewalls:** experiencia mínima de UN (01) año, en implementación de la solución firewall ofertado por el contratista.~~
- ~~**Especialista en sistema de gestión y monitoreo:** experiencia mínima de Un (01) año, implementando herramienta de gestión y monitoreo ofertado por el contratista.<sup>98</sup>~~

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

### 2.3. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

#### 2.3.1. Facturación:

- El contratista deberá acreditar un monto facturado acumulado equivalente ~~a no mayor a tres (3) veces el valor estimado de la contratación S/ 12,613,333.38 (Doce millones seiscientos trece mil trescientos treinta y tres con 38/100 soles)<sup>99</sup>~~, por la venta de servicios iguales o similares al objeto de la convocatoria, durante un periodo no mayor de ocho (08) años anteriores a la fecha de la presentación de propuestas.

Se consideran servicios similares a los siguientes: servicio de internet con gestión de seguridad, servicios de datos con gestión de seguridad, servicio de internet gestionado, servicio de RPV, servicio de datos gestionados, internet en general, acceso a internet, servicio de trasmisión de datos, red de transmisión de datos, servicio de transmisión de datos por fibra óptica, interconexión, enlace de datos, servicio de ancho de banda, interconexión de datos, internet y transmisión de datos, acceso dedicado a internet, enlace dedicado a internet, transmisión de voz y datos, servicio de telecomunicaciones, servicio de internet<sup>100</sup>.

#### **Acreditación:**

- La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de

<sup>97</sup> Texto suprimido en virtud a la consulta y/u observación N° 413

<sup>98</sup> Texto suprimido en virtud a la consulta y/u observación N° 413

<sup>99</sup> Texto aclarativo en virtud a la consulta y/u observación N° 253.

<sup>100</sup> Texto agregado en Virtud a la consulta y/u observación N° 170, 254, 255 y 518 respectivamente.



cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones

### 3.2. REQUISITOS DE CALIFICACIÓN

<b>A</b>	<b>CAPACIDAD LEGAL</b>
	<b>HABILITACIÓN</b>
	<u>Requisitos:</u>
	<ul style="list-style-type: none"> <li>- El contratista debe estar debidamente registrado y habilitado ante las entidades y en conformidad con lo establecido por la Ley general de telecomunicaciones, como empresa proveedora de telecomunicaciones.</li> <li>- El contratista debe pertenecer al NAP (Network Access Point) – Perú activo y operativo.</li> </ul>
	<b>Importante</b>
	<p><i>De conformidad con la Opinión N° 186-2016/DTN, la habilitación de un postor, está relacionada con cierta atribución con la cual debe contar el proveedor para poder llevar a cabo la actividad materia de contratación, este es el caso de las actividades reguladas por normas en las cuales se establecen determinados requisitos que las empresas deben cumplir a efectos de estar habilitadas para la ejecución de determinado servicio o estar autorizadas para la comercialización de ciertos bienes en el mercado.</i></p>
	<u>Acreditación:</u>
	<ul style="list-style-type: none"> <li>- Copia simple de la Resolución del ministerio de transportes y comunicaciones; o copia del certificado de registro de empresas prestadoras de servicios de valor añadido expedido por Dirección general de concesiones en comunicaciones del MTC; o impresión simple del registro de empresas prestadoras de servicios de valor añadido publicadas en la página web MTC; o impresión simple del registro de empresas prestadoras de servicios de valor añadido publicadas en la página web MTC u oficio emitido por el MTC donde se señale las concesiones y/o autorizaciones vigentes que mantiene la empresa de telecomunicaciones, así como el cuadro de servicio de Empresas Prestadoras de Valor Añadido<sup>101</sup></li> <li>- Constancia expedida por el mismo NAP PERÚ o la captura de pantalla de la página web del NAP PERÚ, donde se indique que el contratista es asociado de la referida institución.</li> </ul>
	<b>Importante</b>
	<p><i>En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito.</i></p>
<b>B</b>	<b>CAPACIDAD TÉCNICA Y PROFESIONAL</b>
<b>B.3</b>	<b>CALIFICACIONES DEL PERSONAL CLAVE</b>
<b>B.3.1</b>	<b>FORMACIÓN ACADÉMICA</b>
	<u>Requisitos:</u>
	<ul style="list-style-type: none"> <li>- <b>Jefe de proyecto:</b> Profesional titulado en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o carreras afines.</li> <li>- <del>Especialista en ciberseguridad:</del> Profesional técnico o Bachiller o titulado en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o Computación e informática o Redes de computadoras y comunicación de datos o carreras afines.</li> <li>- <del>Especialista de seguridad de firewalls:</del> Profesional técnico o bachiller o titulado en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o Computación e informática o Redes de computadoras y comunicación de datos o carreras afines.</li> <li>- <del>Especialista en sistemas de gestión y monitoreo:</del> Profesional técnico o Titulado o bachiller</li> </ul>

<sup>101</sup> Texto agregado en virtud a la consulta y/u observación N° 167.



	<p><del>en ingeniería de telecomunicaciones o ingeniería electrónica o ingeniería de sistemas o Computación o informática o Redes de computadoras y comunicación de datos o carreras afines.</del><sup>102</sup></p> <p><b>Acreditación:</b></p> <p>El título profesional o grado requerido será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <a href="https://enlinea.sunedu.gob.pe/">https://enlinea.sunedu.gob.pe/</a> o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: <a href="http://www.titulosinstitutos.pe/">http://www.titulosinstitutos.pe/</a>, según corresponda.</p> <p>En caso EL GRADO O TITULO PROFESIONAL REQUERIDO no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
B.3.2	<p><b>CAPACITACIÓN</b></p> <p><b>Requisitos:</b></p> <ul style="list-style-type: none"> <li>- <b>Jefe de proyecto:</b> 120 horas lectivas en gestión de telecomunicaciones y/o gestión de proyectos y/o certificado PMP.</li> <li>- <del>Especialista en ciberseguridad:</del> certificado a nivel especialista otorgado por una institución internacional de ciberseguridad.</li> <li>- <del>Especialista de seguridad de firewalls:</del> certificado técnico vigente a nivel asociado o profesional en el manejo de la solución firewall ofertado por el contratista.</li> <li>- <del>Especialista en sistema de gestión y monitoreo:</del> certificado técnico vigente a nivel asociado o profesional en el manejo del sistema de gestión y monitoreo ofertado por el contratista.<sup>103</sup></li> </ul> <p><b>Acreditación:</b></p> <p>Se acreditará con copia simple de los certificados o diplomas u otros.</p> <p><b>Importante</b></p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p>
B.4	<p><b>EXPERIENCIA DEL PERSONAL CLAVE</b></p> <p><b>Requisitos:</b></p> <ul style="list-style-type: none"> <li>- <b>Jefe de proyecto:</b> experiencia mínima de DOS (02) años, desempeñándose como Jefe de Proyectos en servicios de comunicaciones.</li> <li>- <del>Especialista en ciberseguridad:</del> experiencia mínima de UN (01) año, en implementación de soluciones firewall, y herramientas SIEM</li> <li>- <del>Especialista de seguridad de firewalls:</del> experiencia mínima de UN (01) año, en implementación de la solución firewall ofertado por el contratista.</li> <li>- <del>Especialista en sistema de gestión y monitoreo:</del> experiencia mínima de UN (01) año, implementando herramienta de gestión y monitoreo ofertado por el contratista.<sup>104</sup></li> </ul> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><b>Acreditación:</b></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <p>Se podrá acreditar o sustentar la experiencia del Personal Clave en el cumplimiento de funciones</p>

<sup>102</sup> Texto suprimido en virtud a la consulta y/u observación N° 413

<sup>103</sup> Texto suprimido en virtud a la consulta y/u observación N° 413

<sup>104</sup> Texto suprimido en virtud a la consulta y/u observación N° 413.



	<p>iguales o similares a las que se realizarán, con independencia de la denominación del cargo que ocupe el Personal Clave<sup>105</sup></p> <p><b>Importante</b></p> <ul style="list-style-type: none"> <li>Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.</li> <li>En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.</li> <li>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</li> <li>Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.</li> </ul>
<b>C</b>	<p><b>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</b></p> <p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 12, 613,333.38 (Doce millones seiscientos trece mil trescientos treinta y tres con 38/100 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: SERVICIO DE INTERNET CON GESTIÓN DE SEGURIDAD, SERVICIOS DE DATOS CON GESTIÓN DE SEGURIDAD, SERVICIO DE INTERNET GESTIONADO, SERVICIO DE RPV, SERVICIO DE DATOS GESTIONADOS, SERVICIO DE INTERNET DEDICADO, SERVICIO DE TRANSMISIÓN DE DATOS, SERVICIO DE INTERNET, SERVICIO DE TELECOMUNICACIONES, INTERNET EN GENERAL, ACCESO A INTERNET, SERVICIO DE TRASMISION DE DATOS, RED DE TRASMISIÓN DE DATOS, SERVICIO DE TRANSMISIÓN DE DATOS POR FIBRA ÓPTICA, INTERCONEXIÓN, ENLACE DE DATOS, SERVICIO DE ANCHO DE BANDA, INTERCONEXIÓN DE DATOS, INTERNET Y TRASMISIÓN DE DATOS, ACCESO DEDICADO A INTERNET, ENLACE DEDICADO A INTERNET, TRANSMISIÓN DE VOZ Y DATOS, SERVICIO DE TELECOMUNICACIONES, SERVICIO DE INTERNET<sup>106</sup>.</p> <p><u>Acreditación:</u></p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago<sup>107</sup>, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia</p>

<sup>105</sup> Texto agregado en virtud a la consulta y/u observación N° 169.

<sup>106</sup> Texto agregado en Virtud a la consulta y/u observación N° 170, 254, 255 y 518 respectivamente.

<sup>107</sup> 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".



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".

#### Importante

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



**CAPÍTULO IV  
FACTORES DE EVALUACIÓN**

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

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

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
<b>A. PRECIO</b>	
<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  <b>90 puntos</b>

<b>OTROS FACTORES DE EVALUACIÓN</b>	<b>10 puntos</b>
<b>H. MEJORAS A LOS TÉRMINOS DE REFERENCIA</b>	



OTROS FACTORES DE EVALUACIÓN	10 puntos (Máximo 10 puntos)
<p><u>Evaluación:</u></p> <p>500 Mbps simétricos con overbooking 1:1 adicionales de SERVICIO DE INTERNET</p> <p><u>Acreditación:</u></p> <p>Se acreditará únicamente mediante la presentación de Declaración Jurada.</p> <p><b>Importante</b></p> <ul style="list-style-type: none"> <li>De conformidad con la Opinión N° 144-2016-OSCE/DTN, constituye una mejora, todo aquello que agregue un valor adicional al parámetro mínimo establecido en las especificaciones técnicas o términos de referencia, según corresponda, mejorando su calidad o las condiciones de su entrega o prestación, sin generar un costo adicional a la Entidad.</li> <li>En este factor se pueden incluir aspectos referidos a la sostenibilidad ambiental o social, tales como el compromiso de que durante la ejecución del contrato se verifiquen condiciones de igualdad de género o de inclusión laboral de personas con discapacidad; el uso de equipos energéticamente eficientes o con bajo nivel de ruido, radiaciones, vibraciones, emisiones, etcétera; la implementación de medidas de ecoeficiencia; el uso de insumos que tengan sustancias con menor impacto ambiental; la utilización de productos forestales de fuentes certificadas, orgánicos o reciclados, el manejo adecuado de residuos sólidos, entre otros.</li> </ul>	<p>Mejora 1 : 10 puntos</p>
<b>PUNTAJE TOTAL</b>	<b>100 puntos<sup>108</sup></b>

**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.

<sup>108</sup> Es la suma de los puntajes de todos los factores de evaluación.



## CAPÍTULO V PROFORMA DEL CONTRATO

### Importante

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

Conste por el presente documento, la contratación del servicio de [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 PAGO<sup>109</sup>

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en [INDICAR MONEDA], en [INDICAR SI SE TRATA DE PAGO ÚNICO, PAGOS PARCIALES O PAGOS PERIÓDICOS], luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

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

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

<sup>109</sup> En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.



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

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

#### **CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN**

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

##### **Importante para la Entidad**

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

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

*Incorporar a las bases o eliminar, según corresponda.*

##### **Importante para la Entidad**

*En el caso de contratación de prestaciones accesorias, se puede incluir la siguiente cláusula:*

#### **CLÁUSULA ...: PRESTACIONES ACCESORIAS<sup>110</sup>**

*"Las prestaciones accesorias tienen por objeto [CONSIGNAR EL OBJETO DE LAS PRESTACIONES ACCESORIAS]."*

*El monto de las prestaciones accesorias asciende a [CONSIGNAR MONEDA Y MONTO], que incluye todos los impuestos de Ley.*

*El plazo de ejecución de las prestaciones accesorias es de [.....], el mismo que se computa desde [CONSIGNAR SI ES DEL DÍA SIGUIENTE DEL CUMPLIMIENTO DE LAS PRESTACIONES PRINCIPALES, 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 DE LAS PRESTACIONES ACCESORIAS, DEBIENDO INDICAR LAS MISMAS EN ESTE ÚLTIMO CASO]."*

*[DE SER EL CASO, INCLUIR OTROS ASPECTOS RELACIONADOS A LA EJECUCIÓN DE LAS PRESTACIONES ACCESORIAS]."*

*Incorporar a las bases o eliminar, según corresponda*

#### **CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO**

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

#### **CLÁUSULA SÉTIMA: GARANTÍAS**

EL CONTRATISTA entregó al perfeccionamiento del contrato la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de LA

<sup>110</sup> De conformidad con la Directiva sobre prestaciones accesorias, los contratos relativos al cumplimiento de la(s) prestación(es) principal(es) y de la(s) prestación(es) accesorias, pueden estar contenidos en uno o dos documentos. En el supuesto que ambas prestaciones estén contenidas en un mismo documento, estas deben estar claramente diferenciadas, debiendo indicarse entre otros aspectos, el precio y plazo de cada prestación.



ENTIDAD, por los conceptos, montos y vigencias siguientes:

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

**Importante**

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

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

En el caso que corresponda, consignar lo siguiente:

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

**Importante**

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

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

**Importante**

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

**CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN**

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

**Importante para la Entidad**

*Sólo en el caso que la Entidad hubiese previsto otorgar adelanto, se debe incluir la siguiente cláusula:*

**CLÁUSULA NOVENA: ADELANTO DIRECTO**

*"LA ENTIDAD otorgará [CONSIGNAR NÚMERO DE ADELANTOS A OTORGARSE] adelantos directos por el [CONSIGNAR PORCENTAJE QUE NO DEBE EXCEDER DEL 30% DEL MONTO DEL CONTRATO ORIGINAL] del monto del contrato original.*

*EL CONTRATISTA debe solicitar los adelantos dentro de [CONSIGNAR EL PLAZO Y OPORTUNIDAD PARA LA SOLICITUD], adjuntando a su solicitud la garantía por adelantos mediante carta fianza o*



póliza de caución acompañada del comprobante de pago correspondiente. Vencido dicho plazo no procederá la solicitud.

LA ENTIDAD debe entregar el monto solicitado dentro de [CONSIGNAR EL PLAZO] siguientes a la presentación de la solicitud del contratista."

Incorporar a las bases o eliminar, según corresponda.

#### **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 CONTROVERSIAS<sup>111</sup>**

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

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

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

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

**CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA**

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

**CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL**

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

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

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

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

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

\_\_\_\_\_  
"LA ENTIDAD"

\_\_\_\_\_  
"EL CONTRATISTA"

**Importante**

*Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales<sup>112</sup>.*

<sup>111</sup> 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).

<sup>112</sup> 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 <sup>113</sup>	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.  
Respuesta a la solicitud de acceso al expediente de contratación.  
Notificación de la orden de servicios<sup>114</sup>

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.*

<sup>113</sup> 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.

<sup>114</sup> 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 <sup>115</sup>		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE <sup>116</sup>		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE <sup>117</sup>		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:

- Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
- Solicitud de reducción de la oferta económica.
- Solicitud de subsanación de los requisitos para perfeccionar el contrato.

<sup>115</sup> 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.

<sup>116</sup> Ibidem.

<sup>117</sup> Ibidem.



4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios<sup>118</sup>

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.*

<sup>118</sup> 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] [ % ]  
119

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [ % ]  
120

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%<sup>121</sup>

<sup>119</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>120</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>121</sup> 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 precios unitarios 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	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
<b>TOTAL</b>			

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**

- *En caso que el postor reduzca su oferta, según lo previsto en el artículo 68 del Reglamento, debe presentar nuevamente este Anexo.*
- *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*



**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
<b>TOTAL</b>	

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*

**Importante para la Entidad**

En caso de la prestación de servicios bajo el esquema mixto de suma alzada y precios unitarios 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:

OFERTA A PRECIOS UNITARIOS DE LOS COMPONENTES SIGUIENTES:

CONCEPTO	CANTIDAD	PRECIO UNITARIO	COSTO
Monto del componente a precios unitarios			

OFERTA A SUMA ALZADA DE LOS COMPONENTES SIGUIENTES:

CONCEPTO	PRECIO TOTAL
Monto del componente a suma alzada	
Monto total de la oferta	

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 en su oferta los precios unitarios de los componentes previstos para este sistema en el presente anexo y por un monto fijo integral de los componentes previstos a suma alzada.



- 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 las disposiciones, según corresponda. Una vez culminada la elaboración de las bases, las notas que no se incorporen deben ser eliminadas*



**Importante para la Entidad**

*En caso de la prestación de servicios bajo el sistema en base a porcentajes 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	OFERTA
Porcentaje ofertado <sup>122</sup>	%
<b>Monto Total Ofertado</b>	

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 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 las disposiciones, según corresponda. Una vez culminada la elaboración de las bases, las notas que no se incorporen deben ser eliminadas.*

<sup>122</sup> De conformidad con la Opinión N° 202-2016/DTN, corresponde al porcentaje del monto total a cobrar o recuperar.



**Importante para la Entidad**

*En caso de la prestación de servicios bajo el sistema en base a honorario fijo y comisión de éxito 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	MONTO
(A) Honorario Fijo	
(B) Comisión de éxito <sup>123</sup>	
<b>Precio de la Oferta (A) + (B)</b>	

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 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 las disposiciones, según corresponda. Una vez culminada la elaboración de las bases, las notas que no se incorporen deben ser eliminadas*

<sup>123</sup> De conformidad con la Opinión N° 011-2017/DTN: "El postor formula su oferta contemplando un monto fijo y un monto adicional como incentivo que debe pagársele en caso consiga el resultado esperado".

**Importante para la Entidad**

*Si durante la fase de actos preparatorios, las Entidades advierten que es posible la participación de proveedores que gozan del beneficio de la exoneración del IGV prevista en la Ley N° 27037, Ley de Promoción de la Inversión en la Amazonía, incluir el siguiente anexo:*

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

**ANEXO N° 7**

**DECLARACIÓN JURADA DE CUMPLIMIENTO DE CONDICIONES PARA LA APLICACIÓN DE LA EXONERACIÓN DEL IGV**

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 que gozo del beneficio de la exoneración del IGV previsto en la Ley N° 27037, Ley de Promoción de la Inversión en la Amazonía, dado que cumplo con las condiciones siguientes:

- 1.- Que el domicilio fiscal de la empresa<sup>124</sup> se encuentra ubicada en la Amazonía y coincide con el lugar establecido como sede central (donde tiene su administración y lleva su contabilidad);
- 2.- Que la empresa se encuentra inscrita en las Oficinas Registrales de la Amazonía (exigible en caso de personas jurídicas);
- 3.- Que, al menos el setenta por ciento (70%) de los activos fijos de la empresa se encuentran en la Amazonía; y
- 4.- Que la empresa no presta servicios fuera de la Amazonía.

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

*Quando se trate de consorcios, esta declaración jurada será presentada por cada uno de los integrantes del consorcio, salvo que se trate de consorcios con contabilidad independiente, en cuyo caso debe ser suscrita por el representante común, debiendo indicar su condición de consorcio con contabilidad independiente y el número de RUC del consorcio.*

<sup>124</sup> En el artículo 1 del "Reglamento de las Disposiciones Tributarias contenidas en la Ley de Promoción de la Inversión en la Amazonía" se define como "empresa" a las "Personas naturales, sociedades conyugales, sucesiones indivisas y personas consideradas jurídicas por la Ley del Impuesto a la Renta, generadoras de rentas de tercera categoría, ubicadas en la Amazonía. Las sociedades conyugales son aquellas que ejerzan la opción prevista en el Artículo 16 de la Ley del Impuesto a la Renta."



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 <sup>125</sup>	FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>126</sup>	EXPERIENCIA PROVENIENTE <sup>127</sup> DE:	MONEDA	IMPORTE <sup>128</sup>	TIPO DE CAMBIO VENTA <sup>129</sup>	MONTO FACTURADO ACUMULADO <sup>130</sup>
1										
2										
3										
4										

<sup>125</sup> 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.

<sup>126</sup> Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho periodo.

<sup>127</sup> 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".

<sup>128</sup> Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

<sup>129</sup> 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.

<sup>130</sup> Consignar en la moneda establecida en las bases.



UNIVERSIDAD NACIONAL DE TRUJILLO  
CONCURSO PÚBLICO N° 02-2013-UNT/CS – PRIMERA CONVOCATORIA

BASES INTEGRADAS

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP <sup>125</sup>	FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>126</sup>	EXPERIENCIA PROVENIENTE <sup>127</sup> DE:	MONEDA	IMPORTE <sup>128</sup>	TIPO DE CAMBIO VENTA <sup>129</sup>	MONTO FACTURADO ACUMULADO <sup>130</sup>
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.

**Importante para la Entidad**

*En el caso de procedimientos por relación de ítems cuando la contratación del servicio va a ser prestado fuera de la provincia de Lima y Callao y el monto del valor estimado de algún ítem no supere los doscientos mil Soles (S/ 200,000.00) debe considerarse el siguiente anexo:*

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

**ANEXO N° 10**

**SOLICITUD DE BONIFICACIÓN DEL DIEZ POR CIENTO (10%) POR SERVICIOS PRESTADOS FUERA DE LA PROVINCIA DE LIMA Y CALLAO**  
**(DE SER EL CASO, SOLO PRESENTAR ESTA SOLICITUD EN EL ÍTEM [CONSIGNAR EL N° DEL ÍTEM O ÍTEMS CUYO VALOR ESTIMADO NO SUPERA LOS DOSCIENTOS MIL SOLES (S/ 200,000.00)])**

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], solicito la asignación de la bonificación del diez por ciento (10%) sobre el puntaje total en [CONSIGNAR EL ÍTEM O ÍTEMS, SEGÚN CORRESPONDA, EN LOS QUE SE SOLICITA LA BONIFICACIÓN] debido a que el domicilio de mi representada se encuentra ubicado en la provincia o provincia colindante donde se ejecuta la prestación.

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

- Para asignar la bonificación, el comité de selección, verifica el domicilio consignado por el postor en el Registro Nacional de Proveedores (RNP).
- Para que el postor pueda acceder a la bonificación, debe cumplir con las condiciones establecidas en el literal f) del artículo 50 del Reglamento.



**Importante**

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

**ANEXO N° 10**

**SOLICITUD DE BONIFICACIÓN DEL DIEZ POR CIENTO (10%) POR SERVICIOS PRESTADOS FUERA DE LA PROVINCIA DE LIMA Y CALLAO**  
**(DE SER EL CASO, SOLO PRESENTAR ESTA SOLICITUD EN EL ÍTEM [CONSIGNAR EL N° DEL ÍTEM O ÍTEMS CUYO VALOR ESTIMADO NO SUPERA LOS DOSCIENTOS MIL SOLES (S/ 200,000.00)]**

Señores

**COMITÉ DE SELECCIÓN**

**CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]**

Presente.-

Mediante el presente el que se suscribe, [.....], representante común del consorcio [CONSIGNAR EL NOMBRE DEL CONSORCIO], solicito la asignación de la bonificación del diez por ciento (10%) sobre el puntaje total en [CONSIGNAR EL ÍTEM O ÍTEMS, SEGÚN CORRESPONDA, EN LOS QUE SE SOLICITA LA BONIFICACIÓN] debido a que los domicilios de todos los integrantes del consorcio se encuentran ubicados en la provincia o provincias colindantes donde se ejecuta la prestación.

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

- Para asignar la bonificación, el comité de selección, verifica el domicilio consignado de los integrantes del consorcio, en el Registro Nacional de Proveedores (RNP).
- Para que un consorcio pueda acceder a la bonificación, cada uno de sus integrantes debe cumplir con las condiciones establecidas en el literal f) del artículo 50 del Reglamento.

**Nota para la Entidad**

*En el caso de procedimientos por relación de ítems cuando el monto del valor estimado de algún ítem corresponda a una Adjudicación Simplificada, se incluye el siguiente anexo:*

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

**ANEXO N° 11**

**SOLICITUD DE BONIFICACIÓN DEL CINCO POR CIENTO (5%) POR TENER LA CONDICIÓN DE MICRO Y PEQUEÑA EMPRESA**  
**ITEM [CONSIGNAR EL N° DEL ÍTEM O ÍTEM CUYO VALOR ESTIMADO CORRESPONDE A UNA AS])**

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], solicito la asignación de la bonificación del cinco por ciento (5%) sobre el puntaje total obtenido, debido a que mi representada cuenta con la condición de micro y pequeña empresa.

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

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



ANEXO N° 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.*

