

# ***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> <div>Importante</div> <ul style="list-style-type: none"> <li>• Abc</li> </ul> </div>	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	<div> <div>Advertencia</div> <ul style="list-style-type: none"> <li>• Abc</li> </ul> </div>	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	<div> <div>Importante para la Entidad</div> <ul style="list-style-type: none"> <li>• Xyz</li> </ul> </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 sombrear.
- La nota **IMPORTANTE** no puede ser modificada ni eliminada en la Sección General. En el caso de la Sección Específica debe seguirse la instrucción que se indica en dicha nota.

Elaboradas en enero de 2019

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



UNIVERSIDAD  
NACIONAL DE SAN CRISTÓBAL  
DE HUAMANGA

*Real, Pontificia y Nacional*  
1677

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

### **CONCURSO PÚBLICO N° 2-2024-UNSCH-CS-1**

#### **CONTRATACIÓN DE SERVICIO DE**

INTERNET Y SEGURIDAD PARA EL CENTRO HISTORICO Y CAMPUS DE LA  
UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA



## 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 accesorio, la misma que debe ser renovada periódicamente hasta el cumplimiento total de las obligaciones garantizadas.

#### Importante

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

#### 3.2.3. GARANTÍA POR ADELANTO

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



### 3.3. REQUISITOS DE LAS GARANTÍAS

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

#### Importante

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

#### Advertencia

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

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

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

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

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

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

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

RUC N° : 20143660754

Domicilio legal : PQ. PORTAL INDEPENDENCIA NRO. 57 U.V. PARQUE SUCRE AYACUCHO - HUAMANGA - AYACUCHO

Teléfono: : -

Correo electrónico: : abastecimiento@unsch.edu.pe

### 1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la CONTRATACIÓN DE SERVICIO DE INTERNET Y SEGURIDAD PARA EL CONTRO HISTORICO Y CAMPUS DE LA UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA.

### 1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado FORMATO N° 02 - OSCE el 08/05/2024.

### 1.4. FUENTE DE FINANCIAMIENTO

RECURSOS ORDINARIOS

#### Importante

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

### 1.5. SISTEMA DE CONTRATACIÓN

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

### 1.6. DISTRIBUCIÓN DE LA BUENA PRO

NO CORRESPONDE

### 1.7. ALCANCES DEL REQUERIMIENTO

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

### 1.8. PLAZO DE PRESTACIÓN DEL SERVICIO



Los servicios materia de la presente convocatoria se prestarán en el plazo de 12 MESES 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 UNIDAD DE ABASTECIMIENTO, SITO JR. AREQUIPA 175, TERCER PISO.

#### 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° 31954 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2024.
- Ley N° 30225 y su modificación efectuada mediante Decreto Legislativo N° 1444.
- Reglamento de la Ley N° 30225, aprobada mediante Decreto Supremo N° 344-2018-EF modificado mediante Decreto Supremo N° 377-2019-EF, Decreto supremo N° 168-2020-EF y Decreto Supremo N° 250-2020-EF y 162-2021-EF.

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



## CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

### 2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

#### Importante

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

### 2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos<sup>2</sup>, la siguiente documentación:

#### 2.2.1. Documentación de presentación obligatoria

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

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

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

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

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

#### Advertencia

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

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

<sup>2</sup> La omisión del índice no determina la no admisión de la oferta.

<sup>3</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) *Licencia de funcionamiento y un certificado emitido por una empresa consultora externa (certificadora en servicios TI y/o infraestructura), que acredite la operación e infraestructura propia del NOC & SOC*
- f) *Certificaciones de ANSI/TIA y/o EPIS de Diseño o Construcción y Operación.*
- g) *Diagrama de la salida internacional detallando los dos nombres de los proveedores TIER I.*

- a) Declaración jurada de plazo de prestación del servicio. **(Anexo N° 4)**<sup>4</sup>
- b) 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)**
- c) El precio de la oferta en SOLES. Adjuntar obligatoriamente el **Anexo N° 6**.  
  
El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales. Los precios unitarios pueden ser expresados con más de dos (2) decimales.

#### Importante

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

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

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

#### 2.2.2. Documentación de presentación facultativa:

#### Advertencia

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

### 2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

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

<sup>4</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.



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>5</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).*

- f) Domicilio para efectos de la notificación durante la ejecución del contrato.
- g) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación <sup>6</sup> (**Anexo N° 12**).
- h) Detalle de los precios unitarios del precio ofertado<sup>7</sup>.
- i) Estructura de costos<sup>8</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.*

- j) Constancia emitida por el NAP PERÚ

#### Importante

<sup>5</sup> 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>6</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>7</sup> Incluir solo en caso de la contratación bajo el sistema a suma alzada.

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



- *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>9</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 MESA DE PARTES VIRTUAL O DE FORMA FISICA EN MESA DE PARTES DE LA DIRECCION GENERAL DE ADMINISTRACION DE LA UNSCH .

### Importante

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

## 2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en PAGOS PERIÓDICOS (MENSUAL)

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 TECNOLOGIAS DE LA INFORMACION emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

Dicha documentación se debe presentar en [CONSIGNAR MESA DE PARTES O LA DEPENDENCIA ESPECÍFICA DE LA ENTIDAD DONDE SE DEBE PRESENTAR LA DOCUMENTACIÓN], sito en [CONSIGNAR LA DIRECCIÓN EXACTA].

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





### CAPÍTULO III REQUERIMIENTO

#### Importante

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

#### 3.1. TERMINOS DE REFERENCIA



UNSCH

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

### 3.1. TERMINOS DE REFERENCIA

#### CONTRATACION DE SERVICIO DE INTERNET Y SEGURIDAD PARA EL CENTRO HISTÓRICO Y CAMPUS UNIVERSITARIO DE LA UNIVERSIDAD NACIONAL SAN CRISTÓBAL DE HUAMANGA.

**1. ÁREA USUARIA O SOLICITANTE:**

UNIVERSIDAD NACIONAL SAN CRISTÓBAL DE HUAMANGA.

**2. FINALIDAD PÚBLICA**

El presente proceso de selección busca contar con un servicio de Internet síncrono de ancho de banda dedicado de **1500 Mbps** para las sedes de la **UNIVERSIDAD NACIONAL SAN CRISTÓBAL DE HUAMANGA** - UNSCH, necesaria para brindar acceso al Internet a las diferentes áreas administrativas que también se conectarán a la red y servidores de la UNSCH, los cuales permitirán asegurar la continuidad de los servicios optimizando los recursos tecnológicos críticos y contribuir al fortalecimiento de la UNSCH mediante la adecuada gestión de tecnologías de información y de los recursos informáticos.

**3. DENOMINACION DE LA CONTRATACIÓN**

CONTRATACION DE SERVICIO DE INTERNET Y SEGURIDAD PARA EL CENTRO HISTÓRICO Y CAMPUS UNIVERSITARIO DE LA UNIVERSIDAD NACIONAL SAN CRISTÓBAL DE HUAMANGA.

**4. ANTECEDENTES**

La **UNIVERSIDAD NACIONAL SAN CRISTÓBAL DE HUAMANGA**, encargada de planificar y administrar eficientemente sus funciones, contribuyendo al logro de los objetivos institucionales, mediante una infraestructura tecnológica que soporte los sistemas de información, no cuenta con un servicio de Internet dedicado tipo síncrono en sus sedes del centro histórico y campus universitario.

LA ENTIDAD es un organismo público, que se encuentra a disposición de la ciudadanía siendo necesario la ejecución del servicio de internet, para cumplimiento de los objetivos de la entidad y sus correspondientes acciones estratégicas institucionales.

**5. GENERALIDADES**

- a) LA ENTIDAD requiere el servicio en modalidad de suma alzada, por lo que el postor deberá comprometerse a realizar la instalación, configuración y pruebas hasta dejar operativos los servicios y equipos ofrecidos de acuerdo a las condiciones y disposiciones contenidas en las bases.
- b) LA ENTIDAD requiere que los equipos sean proporcionados por el proveedor en la última milla, los mismos que serán entregados en calidad de comodato y estos serán devueltos a la empresa proveedora al término del contrato.
- c) El postor debe estar registrado en el MTC para brindar servicios de valor añadido emitido.
- d) El postor debe contar con un Centro de Operaciones de Red (NOC - Network Operations Center) y un Centro de Operaciones de Seguridad (SOC - Security Operations Center) propio, los cuales asegurarán (sin la intervención de empresas externas) la comunicación directa con el proveedor ganador del servicio, teniendo como objetivo validar la calidad del servicio, realizar el seguimiento de las solicitudes de atención y/o supervisar los plazos establecidos en la presente bases; para ello, el postor deberá presentar su licencia de funcionamiento y un certificado emitido por una empresa consultora externa (certificadora en servicios TI y/o infraestructura), que acredite la operación e infraestructura propia del NOC & SOC, siendo presentado para la etapa de presentación de oferta.

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA  
Ing. Huéner Jarampa Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
CIPM 122145



**UNSCH**

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- e) El postor debe ofrecer el servicio de DNS (Sistema de Nombres de Dominio) de manera auto gestionable, teniendo la entidad el acceso a un entorno web (con usuario y clave) que permitirá la capacidad de crear, actualizar registrar, modificar y eliminar las configuraciones de sus registros DNS, sin la necesidad de asistencia técnica del equipo de soporte. (No se requerirá la instalación de equipos adicionales.
- f) El DNS deberá ser propio del postor y tendrá que estar alojado por seguridad en el (los) servidor(es) de su Data Center del postor, para ello el centro de datos deberá contar como mínimo con las certificaciones de ANSI/TIA y/o EPIS de Diseño o Construcción y operación, siendo presentado para la etapa de presentación de oferta.
- g) El postor debe ser miembro de la Asociación NAP Perú en calidad de Operador ISP, con capacidad de 2 enlaces x 100 Gbps, para ello deberá presentar una constancia emitida por el NAP PERÚ en la etapa de firma del contrato.
- h) El postor debe contar como mínimo, con dos proveedores TIER I de mínimo 100 Gbps para las salidas internacionales, 100% en fibra óptica tanto para la salida principal como contingencia, para ello el postor deberá presentar un diagrama de la salida internacional detallando los nombres de los proveedores TIER I, en la etapa de presentación de oferta.
- i) El backbone de la red local del postor deberá ser redundante y se deberá contar ruta (enlace de contingencia en la salida internacional, demostrando 2 salidas diferentes, sea la red propia o subcontratando a terceros).
- j) El postor deberá contar con servidores DNS redundados y en centro de datos distintos.
- k) El medio de acceso deberá ser de fibra óptica al 100% desde el nodo de atención hasta el data center donde se alojarán los equipos en el local de la Entidad.
- l) No se aceptarán enlaces o conexiones con medio de transmisiones inalámbricas, microondas o satelitales.
- m) El postor debe contar con un sistema de monitoreo vía web que permita visualizar el tráfico del enlace que se contrate, este sistema de monitoreo debe ser accesible para LA ENTIDAD sin que esto represente costo adicional para el mismo. LA ENTIDAD podrá observar la disponibilidad del servicio contratado, monitorear la performance del equipo, observar cuales son los periodos de mayor tráfico y obtener reportes.
- n) El proveedor debe contar con una línea exclusiva para el servicio de atención al cliente y soporte técnico 24x7. La línea es exclusiva para clientes corporativos y el horario es de lunes a domingo las 24 horas del día.
- o) El Proveedor debe contar con un centro de soporte y servicio de Postventa propio y especializado para el segmento corporativo.
- p) El proveedor debe implementar lo solicitado en el presente proceso, en coordinación con la entidad.
- q) El proveedor tiene la obligación de ejecutar los servicios de acuerdo a lo establecido en los términos de referencia, teniendo responsabilidad total sobre la instalación, implementación, pruebas y puesta en marcha de los servicios contratados.
- r) El proveedor asumirá todos los gastos de transporte del contratista hacia la Entidad necesarios para instalación de los equipos, así como de los materiales y demás componentes necesarios para la instalación, implementación, pruebas y puesta en marcha de los servicios

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Humberto J. Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
DPM/12245



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- s) El postor deberá contar con los lineamientos de certificación internacional para asegurar la gestión de la calidad, seguridad de la información y la continuidad de Servicios.
- t) La red de transporte del postor deberá ser de tecnología IP/MPLS, no se aceptará tecnología MetroEthernet, lo cual permite eficiencia en el enrutamiento y escalabilidad del servicio.

## 6. ALCANCES Y DESCRIPCIÓN DE LOS SERVICIOS A CONTRATAR

### 6.1. ALCANCE GENERAL

- a) El medio de acceso en última milla deberá ser necesariamente vía fibra óptica al 100%.
- b) La provisión y el dimensionamiento (teniendo como base las características técnicas indicadas en los Términos de Referencia) de los equipos, licencias de softwares y hardware, parches y firmwares, así como materiales, accesorios e insumos necesarios para el correcto funcionamiento de los servicios requeridos, serán de responsabilidad del Proveedor, así como su instalación, implementación, pruebas y puesta en marcha de los servicios en el local de prestación. No deberán generar un costo adicional a la Entidad.
- c) Poseer servidores DNS redundantes y distribuidos en nodos y/o datacenters del postor
- d) Los enlaces deberán contar con un Router o dispositivo de enrutamiento IP que permita soportar el ancho de banda contratado. Este equipo deberá ser nuevo, de primer uso y contar con vigencia tecnológica.

### 6.2. DESCRIPCIÓN DEL SERVICIO DE INTERNET DEDICADO

- a) Servicio de Acceso a Internet con conexión dedicada, simétrico y con overbooking 1:1.
- b) La disponibilidad del servicio de internet para el campus universitario debe ser como mínimo de 99.95% y el centro histórico será como mínimo de 99.00%.
- c) El enlace de internet para el campus universitario deberá estar en activo-pasivo, donde la ruta del enlace contingencia será con una ruta distinta a la del enlace principal.
- d) El proveedor deberá proporcionar para la sede campus universitario un pool de 16 IP's públicas IPv4 y para el centro histórico un pool de 4 IP's, dentro de las cuales se considera la IP de red, la IP de broadcast y la IP para el Gateway.
- e) El medio de acceso deberá ser de fibra óptica al 100% desde el nodo de atención hasta el Datacenter donde se alojarán los equipos en el local de la entidad.
- f) No se aceptará como salidas internacionales redundantes, rutas con un mismo proveedor internacional.
- g) LA ENTIDAD requiere contratar el servicio de Internet, con un enlace de última milla en fibra óptica por un periodo de 12 meses, el cual deberá ser provisionado mediante un circuito dedicado con overbooking 1:1.
- h) El caso de caída de la sede centro histórico, el postor deberá tener la capacidad enrutar el tráfico de Internet saliente por el enlace de la sede campus universitario.
- i) Habilitar enlace de fibra de 300m del centro de datos a los laboratorios de Ingeniería de Sistemas que debe incluir los transceiver SFP+ 10G a ambos extremos.

El servicio de internet será brindado como se muestra en el siguiente cuadro:

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
2024  
Ing. Humberto Jaramba Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
0904122145





UNSCH

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

N°	Nombre de la Sede	Departamento	Provincia	Distrito	Servicio (Principal y/o Contingencia)	Ancho de banda mínimo
1	Campus universitario	Ayacucho	Huamanga	Ayacucho	principal	1Gbps
2	Campus universitario	Ayacucho	Huamanga	Ayacucho	Contingencia	150Mbps
3	Centro histórico	Ayacucho	Huamanga	Ayacucho	principal	500Mbps
4	Centro histórico	Ayacucho	Huamanga	Ayacucho	Contingencia	100Mbps

#### 6.3. DESCRIPCIÓN DEL SERVICIO DE MITIGACIÓN DE ATAQUES DE DDOS

- El postor deberá ofrecer un servicio de mitigación de ataques DDOS ubicado en la infraestructura del proveedor.
- La mitigación en la nube se realizará cuando el enlace de conexión a Internet sea saturado por un ataque DDOS volumétrico.
- El postor debe proteger el enlace de Internet del campus universitario con un servicio de detección y mitigación de ataques de Denegación de Servicio Volumétricos dirigidos a las IPs públicas de la Entidad.
- Deberá ser una solución con capacidad de mitigación de al menos 100 Gbps dentro de la infraestructura del proveedor.
- El servicio de mitigación ofertado debe basarse en tecnologías que analicen el patrón de tráfico hacia el cliente y solo al detectar un inminente ataque hagan un desvío del tráfico hacia un centro de limpieza.
- El sistema desplegado en la red del postor debe ser un appliance diseñado específicamente (Stateless) para proporcionar disponibilidad de servicios IP y debe estar dedicado a esta función, por lo que no se aceptarán dispositivos que mantengan estado de las conexiones como cortafuegos, sistemas de prevención y detección, y las variantes o combinaciones como UTM, NGFW, NGIPS; ya que al conservar el estado de la conexión se vuelven ellos mismos susceptibles a ataques DDOS.
- El sistema debe ser capaz de informar la cantidad de tráfico malicioso bloqueado en bps y durante una mitigación activa.
- Se deberá brindar un usuario de lectura para la solución de Mitigación de ataques de DDOS.

#### 6.4. DESCRIPCIÓN DEL SERVICIO DE SEGURIDAD PERIMETRAL

- Para la sede campus universitario se requiere un (01) appliance físico nuevo y de primer uso, de propósito específico de NGFW, licenciados por el periodo del servicio. Dicho equipo debe incluir las siguientes capacidades:

##### 1. Características de rendimiento

- Soportar al menos 11,4 Gbps de throughput de NGFW, medido en Enterprise Mix.
- Soportar al menos 14 Gbps de throughput de IPS, medido en Enterprise Mix.
- Soportar al menos 10,4 Gbps de throughput de Threat Protection, medido en Enterprise Mix.
- Soporte a por lo menos 8M conexiones simultáneas TCP
- Soporte a por lo menos 550K nuevas conexiones por segundo TCP
- Throughput de al menos 55 Gbps de VPN IPSec, medido con paquetes de 512 bytes
- Estar licenciado para, o soportar sin necesidad de licencia, 1,9K túneles de VPN IPSec site-to-site simultáneos
- Estar licenciado para, o soportar sin necesidad de licencia, 50K túneles de clientes VPN IPSec simultáneos
- Throughput de al menos 4,3 Gbps de VPN SSL
- Soportar al menos 10000 clientes de VPN SSL simultáneos
- Soportar al menos 9 Gbps de throughput de Inspección SSL, medido con conexiones HTTPS

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Humberto J. Pantoja Pantoja  
JEFE DE TECNOLOGÍAS DE LA INFORMACIÓN  
DIPLOMA 1322145



UNSCH

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- 1.12. Soportar al menos 32 Gbps de throughput de Application Control, medido en HTTP 64 KB
- 1.13. Tener al menos 16 interfaces 1 Gbps RJ45, las cuales serán utilizadas exclusivamente para tráfico de red
- 1.14. Tener al menos 8 slots de 1Gbps SFP, las cuales serán utilizadas exclusivamente para tráfico de red
- 1.15. Tener al menos 4 slots de 10Gbps SFP+, las cuales serán utilizadas exclusivamente para tráfico de red
- 1.16. Tener al menos 4 slots de 25Gbps SFP28 / 10Gbps SFP+, las cuales serán utilizadas exclusivamente para tráfico de red
- 1.17. Tener al menos 1 interfaz dedicada para gestión
- 1.18. Tener al menos 1 interfaz dedicada para HA
- 1.19. Tener al menos 2 fuentes de poder internas.
- 1.20. Tener al menos 1 puerto de consola
- 1.21. Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance.

## 2. Características Generales

- 2.1. La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.;
- 2.2. El sistema operativo debe contar con certificación USGv6 en la suite de Basic Interoperability.
- 2.3. Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- 2.4. Las funcionalidades de protección de red que conforman la plataforma de seguridad, pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;
- 2.5. La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;
- 2.6. Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19", incluyendo un rail kit (si sea necesario) y los cables de alimentación;
- 2.7. La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;
- 2.8. Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
- 2.9. Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
- 2.10. Los dispositivos de protección de red deben soportar Policy based routing o policy based forwarding;
- 2.11. Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
- 2.12. Los dispositivos de protección de red deben soportar DHCP Relay y DHCP Server
- 2.13. Los dispositivos de protección de red deben soportar sFlow;
- 2.14. Los dispositivos de protección de red deben soportar Jumbo Frames;
- 2.15. Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
- 2.16. Debe ser compatible con NAT dinámica (varios-a-1);
- 2.17. Debe ser compatible con NAT dinámica (muchos-a-muchos);
- 2.18. Debe soportar NAT estática (1-a-1);
- 2.19. Debe admitir NAT estática (muchos-a-muchos);
- 2.20. Debe ser compatible con NAT estático bidireccional 1-a-1;
- 2.21. Debe ser compatible con la traducción de puertos (PAT);
- 2.22. Debe ser compatible con NAT Origen;

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Huéner Jarampa Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
CUPN 121142



UNSCH

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- 2.23. Debe ser compatible con NAT de destino;
- 2.24. Debe soportar NAT de origen y NAT de destino de forma simultánea;
- 2.25. Debe soportar NAT de origen y NAT de destino en la misma política
- 2.26. Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
- 2.27. Debe ser compatible con NAT64 y NAT46;
- 2.28. Debe implementar el protocolo ECMP;
- 2.29. La solución debe incluir capacidades de SD-WAN durante la vigencia del contrato.
- 2.30. Las capacidades de SD-WAN de la solución deben permitir monitorear el tráfico de aplicaciones desde un servicio en nube del fabricante.
- 2.31. Debe soportar el balanceo de enlace por hash de IP de origen y destino;
- 2.32. Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;
- 2.33. Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;
- 2.34. Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;
- 2.35. Enviar logs a sistemas de gestión externos simultáneamente;
- 2.36. Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
- 2.37. Debe soportar protección contra la suplantación de identidad (anti-spoofing);
- 2.38. Implementar la optimización del tráfico entre dos dispositivos;
- 2.39. Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
- 2.40. Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
- 2.41. Soportar OSPF graceful restart;
- 2.42. Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
- 2.43. Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
- 2.44. Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
- 2.45. Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
- 2.46. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
- 2.47. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
- 2.48. Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
- 2.49. La configuración de alta disponibilidad debe sincronizar: Sesiones, asociaciones de seguridad VPN y ablas FIB;
- 2.50. La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
- 2.51. En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
- 2.52. Debe soportar la creación de sistemas virtuales en el mismo equipo;
- 2.53. Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA  
Ing. Huéner Jankupa Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
0974 22245





UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- 2.54. Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;
  - 2.55. La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;
  - 2.56. Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);
  - 2.57. La consola de administración debe soportar como mínimo, inglés, español y Portugués.
  - 2.58. La solución debe incluir la capacidad de detectar al menos los siguientes valores dentro del tráfico analizado: nombre del host y sistema operativo.
  - 2.59. La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.
- 3. Control por Política de Firewall**
- 3.1. Debe soportar controles de zona de seguridad;
  - 3.2. Debe contar con políticas de control por puerto y protocolo;
  - 3.3. Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
  - 3.4. Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
  - 3.5. Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
  - 3.6. Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
  - 3.7. Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
  - 3.8. Debe soportar el protocolo estándar de la industria VXLAN;
  - 3.9. La solución debe permitir la implementación sin asistencia de SD-WAN
  - 3.10. En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
  - 3.11. La solución debe soportar la integración nativa con una solución de sandboxing.
- 4. Control de Aplicación**
- 4.1. Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
  - 4.2. Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, video, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
  - 4.3. Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Humberto Pineda Párraga  
JEFE DE TECNOLOGÍAS DE LA INFORMACIÓN  
01001422145





UNSCH

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- 4.4. Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;
  - 4.5. Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;
  - 4.6. Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
  - 4.7. Actualización de la base de firmas de la aplicación de forma automática;
  - 4.8. Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;
  - 4.9. Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
  - 4.10. Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;
  - 4.11. El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
  - 4.12. Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
  - 4.13. Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
  - 4.14. Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video;
  - 4.15. Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freerate, etc.) permitiendo granularidad de control/reglas para el mismo;
  - 4.16. Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones, nivel de riesgo de la aplicación y categoría de aplicación.
  - 4.17. Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente
- 5. Prevención de Amenazas**
- 5.1. Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
  - 5.2. Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
  - 5.3. Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
  - 5.4. Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
  - 5.5. Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;
  - 5.6. Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
  - 5.7. Debe incluir la protección contra ataques de denegación de servicio;
  - 5.8. Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, análisis para detectar anomalías de protocolo, desfragmentación IP, reensamblado de paquetes TCP y bloqueo de paquetes con formato incorrecto (malformed packets);
  - 5.9. Debe ser capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.;

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA  
Ing. Humberto J. Antuña Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
01/04/2024



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- 5.10. Detectar y bloquear los escaneos de puertos de origen;
- 5.11. Bloquear ataques realizados por gusanos (worms) conocidos;
- 5.12. Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- 5.13. Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
- 5.14. Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- 5.15. Identificar y bloquear la comunicación con redes de bots;
- 5.16. Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;
- 5.17. Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- 5.18. Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
- 5.19. La capacidad de filtro de DNS debe ser alimentada por un servicio de inteligencia de amenazas de la propia marca.
- 5.20. Debe permitir la translación en el firewall de una consulta de DNS, a fin de redirigir la resolución hacia otro destino diferente del original.
- 5.21. Los eventos deben identificar el país que origino la amenaza;
- 5.22. Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- 5.23. Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- 5.24. Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
- 5.25. Debe incluir la protección contra ataques de día cero a través de una estrecha integración con análisis Sandbox en nube;
- 6. Filtrado de URL**
  - 6.1. Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);
  - 6.2. Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;
  - 6.3. Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
  - 6.4. Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;
  - 6.5. Tener por lo menos 75 categorías de URL;
  - 6.6. Debe tener la funcionalidad de exclusión de URLs por categoría;
  - 6.7. Permitir página de bloqueo personalizada;
  - 6.8. Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
- 7. Identificación de Usuarios**
  - 7.1. Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
- 7.2. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios;
  - 7.3. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;
  - 7.4. Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios;
  - 7.5. Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios;
  - 7.6. Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autenticación residente en el equipo de seguridad (portal cautivo);
  - 7.7. Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
  - 7.8. Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
  - 7.9. Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
  - 7.10. Debe incluir al menos dos tokens dentro del servicio, permitiendo la autenticación de dos factores para los usuarios administradores del firewall;
- 8. QoS Traffic Shaping**
- 8.1. Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;
  - 8.2. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen, dirección de destino, por usuario y grupo.
  - 8.3. Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
  - 8.4. Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
  - 8.5. En QoS debe permitir la definición de tráfico con ancho de banda garantizado, con máximo ancho de banda y colas de prioridad.
  - 8.6. Soportar marcación de paquetes DiffServ, incluso por aplicación;
  - 8.7. Soportar la modificación de los valores de DSCP para Diffserv;
  - 8.8. Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
  - 8.9. Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;
- 9. Filtro de Datos**
- 9.1. Permite la creación de filtros para archivos y datos predefinidos;

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Huéner Jankupa Patulla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
DIPN° 122145





UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- 9.2. Los archivos deben ser identificados por tamaño y tipo;
  - 9.3. Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;
  - 9.4. Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
  - 9.5. Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
  - 9.6. Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;
- 10. Geo Localización**
- 10.1. Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
  - 10.2. Debe permitir la visualización de los países de origen y destino en los registros de acceso;
  - 10.3. Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;
- 11. VPN**
- 11.1. Soporte VPN de sitio-a-sitio y cliente-a-sitio;
  - 11.2. Soportar VPN IPsec;
  - 11.3. Soportar VPN SSL;
  - 11.4. La VPN IPsec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
  - 11.5. La VPN IPsec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
  - 11.6. La VPN IPsec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
  - 11.7. La VPN IPsec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
  - 11.8. Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
  - 11.9. Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPsec;
  - 11.10. Debe permitir activar y desactivar túneles IPsec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;
  - 11.11. Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;
  - 11.12. Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;
  - 11.13. Soportar autenticación vía AD/LDAP, con token, certificado y base de usuarios local;
  - 11.14. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
  - 11.15. Deberá mantener una conexión segura con el portal durante la sesión;
  - 11.16. El agente de VPN SSL o IPSEC cliente-a-sitio debe permitir ser instalado al menos en Windows, Mac OS, Linux, Android y IOS. De ser requerido, se debe incluir el licenciamiento necesario para permitir esta capacidad.
  - 11.17. La plataforma debe tener la capacidad de soportar al menos 100 conexiones VPN SSL concurrentes desde dispositivos endpoint y móviles, usando agente y sin agente.
  - 11.18. El agente de VPN client-to-site debe validar la configuración del dispositivo cliente antes de otorgar el acceso a la red. Debe soportar como mínimo los siguientes criterios de evaluación antes de brindar el acceso a la red:



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

protección activa del antivirus, firewall de host y versión de sistema operativo, así como una combinación de estos criterios.

- b) Para la sede centro histórico se requiere un (01) appliance físico nuevo y de primer uso, de propósito específico de NGFW, licenciados por el periodo del servicio. Dicho equipo debe incluir las siguientes capacidades:

#### 12. Características de rendimiento

- 12.1. Soportar al menos 10 Gbps de throughput de NGFW, medido en Enterprise Mix.
- 12.2. Soportar al menos 12 Gbps de throughput de IPS, medido en Enterprise Mix.
- 12.3. Soportar al menos 9 Gbps de throughput de Threat Protection, medido en Enterprise Mix.
- 12.4. Soporte a por lo menos 7,7M conexiones simultáneas TCP
- 12.5. Soporte a por lo menos 500K nuevas conexiones por segundo TCP
- 12.6. Throughput de al menos 55 Gbps de VPN IPSec, medido con paquetes de 512 bytes
- 12.7. Estar licenciado para, o soportar sin necesidad de licencia, 1,9K túneles de VPN IPSec site-to-site simultáneos
- 12.8. Estar licenciado para, o soportar sin necesidad de licencia, 50K túneles de clientes VPN IPSec simultáneos
- 12.9. Throughput de al menos 3,5 Gbps de VPN SSL
- 12.10. Soportar al menos 5000 clientes de VPN SSL simultáneos
- 12.11. Soportar al menos 8 Gbps de throughput de Inspección SSL, medido con conexiones HTTPS
- 12.12. Soportar al menos 28 Gbps de throughput de Application Control, medido en HTTP 64 KB
- 12.13. Tener al menos 16 interfaces 1 Gbps RJ45, las cuales serán utilizadas exclusivamente para tráfico de red
- 12.14. Tener al menos 8 slots de 1Gbps SFP, las cuales serán utilizadas exclusivamente para tráfico de red
- 12.15. Tener al menos 8 slots de 10Gbps SFP+, las cuales serán utilizadas exclusivamente para tráfico de red
- 12.16. Tener al menos 1 interfaz dedicada para gestión
- 12.17. Tener al menos 1 interfaz dedicada para HA
- 12.18. Tener al menos 2 fuentes de poder internas.
- 12.19. Tener al menos 1 puerto de consola
- 12.20. Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance.

#### 13. Características Generales

- 13.1. La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.
- 13.2. El sistema operativo debe contar con certificación USGv6 en la suite de Basic Interoperability.
- 13.3. Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- 13.4. Las funcionalidades de protección de red que conforman la plataforma de seguridad, pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;
- 13.5. La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;
- 13.6. Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19", incluyendo un rail kit (si sea necesario) y los cables de alimentación;

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Hubert J. Jarama Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
DPM 122145



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- 13.7. La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;
- 13.8. Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
- 13.9. Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
- 13.10. Los dispositivos de protección de red deben soportar Policy based routing o policy based forwarding;
- 13.11. Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
- 13.12. Los dispositivos de protección de red deben soportar DHCP Relay y DHCP Server;
- 13.13. Los dispositivos de protección de red deben soportar sFlow;
- 13.14. Los dispositivos de protección de red deben soportar Jumbo Frames;
- 13.15. Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
- 13.16. Debe ser compatible con NAT dinámica (varios-a-1);
- 13.17. Debe ser compatible con NAT dinámica (muchos-a-muchos);
- 13.18. Debe soportar NAT estática (1-a-1);
- 13.19. Debe admitir NAT estática (muchos-a-muchos);
- 13.20. Debe ser compatible con NAT estático bidireccional 1-a-1;
- 13.21. Debe ser compatible con la traducción de puertos (PAT);
- 13.22. Debe ser compatible con NAT Origen;
- 13.23. Debe ser compatible con NAT de destino;
- 13.24. Debe soportar NAT de origen y NAT de destino de forma simultánea;
- 13.25. Debe soportar NAT de origen y NAT de destino en la misma política;
- 13.26. Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
- 13.27. Debe ser compatible con NAT64 y NAT46;
- 13.28. Debe implementar el protocolo ECMP;
- 13.29. La solución debe incluir capacidades de SD-WAN durante la vigencia del contrato.
- 13.30. Las capacidades de SD-WAN de la solución deben permitir monitorear el tráfico de aplicaciones desde un servicio en nube del fabricante.
- 13.31. Debe soportar el balanceo de enlace por hash de IP de origen y destino;
- 13.32. Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;
- 13.33. Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;
- 13.34. Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;
- 13.35. Enviar logs a sistemas de gestión externos simultáneamente;
- 13.36. Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
- 13.37. Debe soportar protección contra la suplantación de identidad (anti-spoofing);
- 13.38. Implementar la optimización del tráfico entre dos dispositivos;
- 13.39. Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
- 13.40. Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
- 13.41. Soportar OSPF graceful restart;
- 13.42. Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA  
Ing. Humberto Jaramba Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
0974 122145





UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- 13.43. Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
- 13.44. Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
- 13.45. Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
- 13.46. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
- 13.47. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
- 13.48. Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
- 13.49. La configuración de alta disponibilidad debe sincronizar: Sesiones, asociaciones de seguridad VPN y ablas FIB;
- 13.50. La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
- 13.51. En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
- 13.52. Debe soportar la creación de sistemas virtuales en el mismo equipo;
- 13.53. Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;
- 13.54. Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;
- 13.55. La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;
- 13.56. Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);
- 13.57. La consola de administración debe soportar como mínimo, ingles, español y Portugues.
- 13.58. La solución debe incluir la capacidad de detectar al menos los siguientes valores dentro del tráfico analizado: nombre del host y sistema operativo.
- 13.59. La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.

#### 14. Control por Política de Firewall

- 14.1. Debe soportar controles de zona de seguridad;
- 14.2. Debe contar con políticas de control por puerto y protocolo;
- 14.3. Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
- 14.4. Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
- 14.5. Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
- 14.6. Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Huber J. Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
0907122145



UNSCH

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- 14.7. Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- 14.8. Debe soportar el protocolo estándar de la industria VXLAN;
- 14.9. La solución debe permitir la implementación sin asistencia de SD-WAN
- 14.10. En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
- 14.11. La solución debe soportar la integración nativa con una solución de sandboxing.

#### 15. Control de Aplicación

- 15.1. Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
- 15.2. Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
- 15.3. Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
- 15.4. Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;
- 15.5. Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;
- 15.6. Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
- 15.7. Actualización de la base de firmas de la aplicación de forma automática;
- 15.8. Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;
- 15.9. Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
- 15.10. Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;
- 15.11. El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- 15.12. Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
- 15.13. Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
- 15.14. Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video;
- 15.15. Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
- 15.16. Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones, nivel de riesgo de la aplicación y categoría de aplicación.
- 15.17. Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente.

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Huéner J. J. Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
CIPM 112345





UNSCH

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

#### 16. Prevención de Amenazas

- 16.1. Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
- 16.2. Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
- 16.3. Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
- 16.4. Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
- 16.5. Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;
- 16.6. Deber permitir el bloqueo de vulnerabilidades y exploits conocidos;
- 16.7. Debe incluir la protección contra ataques de denegación de servicio;
- 16.8. Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, análisis para detectar anomalías de protocolo, desfragmentación IP, reensamblado de paquetes TCP y bloqueo de paquetes con formato incorrecto (malformed packets);
- 16.9. Debe ser capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.;
- 16.10. Detectar y bloquear los escaneos de puertos de origen;
- 16.11. Bloquear ataques realizados por gusanos (worms) conocidos;
- 16.12. Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- 16.13. Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
- 16.14. Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- 16.15. Identificar y bloquear la comunicación con redes de bots;
- 16.16. Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;
- 16.17. Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- 16.18. Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
- 16.19. La capacidad de filtro de DNS debe ser alimentada por un servicio de inteligencia de amenazas de la propia marca.
- 16.20. Debe permitir la translación en el firewall de una consulta de DNS, a fin de redirigir la resolución hacia otro destino diferente del original.
- 16.21. Los eventos deben identificar el país que origino la amenaza;
- 16.22. Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- 16.23. Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- 16.24. Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
- 16.25. Debe incluir la protección contra ataques de día cero a través de una estrecha integración con análisis Sandbox en nube;

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Huérfano Esteban Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
0901122245



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

#### 17. Filtrado de URL

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

#### 18. Identificación de Usuarios

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

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Humberto J. Mendoza Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
C/INT 122143



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

#### 19. QoS Traffic Shaping

- 19.1. Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;
- 19.2. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen, dirección de destino, por usuario y grupo.
- 19.3. Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
- 19.4. Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
- 19.5. En QoS debe permitir la definición de tráfico con ancho de banda garantizado, con máximo ancho de banda y colas de prioridad.
- 19.6. Soportar marcación de paquetes DiffServ, incluso por aplicación;
- 19.7. Soportar la modificación de los valores de DSCP para Diffserv;
- 19.8. Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
- 19.9. Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

#### 20. Filtro de Datos

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

#### 21. Geo Localización

- 21.1. Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
- 21.2. Debe permitir la visualización de los países de origen y destino en los registros de acceso;
- 21.3. Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

#### 22. VPN

- 22.1. Soporte VPN de sitio-a-sitio y cliente-a-sitio;
- 22.2. Soportar VPN IPSec;
- 22.3. Soportar VPN SSL;
- 22.4. La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
- 22.5. La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
- 22.6. La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
- 22.7. La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Humberto J. Jarama Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
CIPN 122145





UNSCH

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- 22.8. Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
  - 22.9. Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
  - 22.10. Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;
  - 22.11. Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;
  - 22.12. Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;
  - 22.13. Soportar autenticación vía AD/LDAP, con token, certificado y base de usuarios local;
  - 22.14. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
  - 22.15. Deberá mantener una conexión segura con el portal durante la sesión;
  - 22.16. El agente de VPN SSL o IPSEC cliente-a-sitio debe permitir ser instalado al menos en Windows, Mac OS, Linux, Android y IOS. De ser requerido, se debe incluir el licenciamiento necesario para permitir esta capacidad.
  - 22.17. La plataforma debe tener la capacidad de soportar al menos 100 conexiones VPN SSL concurrentes desde dispositivos endpoint y móviles, usando agente y sin agente.
  - 22.18. El agente de VPN client-to-site debe validar la configuración del dispositivo cliente antes de otorgar el acceso a la red. Debe soportar como mínimo los siguientes criterios de evaluación antes de brindar el acceso a la red: protección activa del antivirus, firewall de host y versión de sistema operativo, así como una combinación de estos criterios.
- c) Se debe incluir un servicio de sandboxing, que podrá ser brindado desde la nube del postor o con un appliance dedicado onpremise, para la detección de amenazas avanzadas desconocidas, el servicio debe estar integrado al firewall de la ciudad universitaria y debe cumplir como mínimo con las siguientes características:
1. La solución debe proporcionar la funcionalidad de inspección del tráfico entrante en busca de malware desconocido (APT: amenazas persistentes avanzadas y amenazas de día cero), ransomware con filtro de amenazas avanzado y análisis de ejecución en tiempo real, e inspección del tráfico saliente de callbacks.
  2. Poseer la capacidad de prevenir amenazas desconocidas
  3. Debido a que el malware es muy dinámico y un Antivirus reactivo común no puede detectarlos con la misma velocidad que se crean sus variaciones, la solución que se ofrece debe tener características para la prevención de malware desconocido incluidas en la propia herramienta (día cero)
  4. La solución debe soportar el análisis de 3000 archivos/día.
  5. La solución debe contar con la nube de inteligencia propia del fabricante que se encarga de actualizar toda la base de seguridad a través de firmas.
  6. Debe ser capaz de monitorear y analizar el tráfico generado por archivos maliciosos y así determinar la naturaleza del tráfico y sus conexiones.
  7. La solución debe poder inspeccionar el tráfico cifrado SSL.
  8. Compatibilidad con el análisis de archivos de paquetes de Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar y class), APK de Android, MacOS y Linux en un entorno sandbox.
  9. Debe soportar los siguientes tipos de archivos: 7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .htm, .html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .potx, .ps1,



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, .rl, .vbs, WEblink, .wsf, .xlam, .xls, .xlsb, .xslm, .xlsx, .xlt, .xltn, .xltx, .xz, .z, .zip
10. Debe ser capaz de diferenciar los archivos analizados en al menos dos categorías: las que se identificaron como virus maliciosos y/o malignos y archivos sospechosos por tener comportamiento no esperado o características indeseables
  11. Debe ser capaz de clasificar los archivos sospechosos de acuerdo con el riesgo que suponen.
  12. Debe ser capaz de exportar los resultados del análisis de archivos maliciosos y sospechosos a PDF desde su propia interfaz de gestión
  13. Debe tener la capacidad de analizar en sandbox enlaces (HTTP y HTTPS) presentes en el cuerpo de los mensajes del correo electrónico SMTP. Debe generarse un informe si la apertura del enlace por el sandbox lo identifica como malicioso.
  14. Debe soportar el monitoreo de archivos transferidos en internet (HTTPS, FTP, HTTP, SMTP)
  15. La solución debe tener un mecanismo para identificar hosts infectados que intentan acceder a direcciones DNS de dominios maliciosos.
  16. Seleccionar mediante política qué tipos de expedientes serán objeto de este análisis y prevención.
  17. Implementar e identificar malware en archivos adjuntos de correo electrónico y URL conocidos.
  18. Implementar detección y bloqueo inmediatos de malware que utilice un mecanismo de explotación en archivos PDF.
  19. El sistema de análisis debe proporcionar información sobre las actividades de los archivos maliciosos y sospechosos en las máquinas virtuales infectadas, información tal como qué procesos se inicializan por el archivo, los archivos creados, los archivos eliminados, los cambios realizados en el registro, el comportamiento de la red, como direcciones URL utilizadas por los programas maliciosos (seguros y no seguros) cambios de registros proporcionando información sobre el usuario infectado (al menos su dirección IP).
  20. Debe permitir la descarga de malware identificados a partir de la interfaz de gestión propia
  21. Se debe tener mecanismo de integración para proporcionar corrección automática. Una vez que se detecta el código malicioso, un paquete de firmas de antivirus basado en amenazas detectadas debe ser desarrollado y enviado a los dispositivos registrados como firewalls, y estaciones de trabajo de usuarios para ayudar en la mitigación.
  22. En caso de un veredicto positivo, debe presentar un desglose del comportamiento de la máquina comprometida, que contenga al menos información para fines de auditoría.:
  23. sobre el Tipo de archivo
  24. IP de origen del malware
  25. IP de destino (cliente que descargó el malware)
  26. virus Link to Reference Total
  27. Resumen del comportamiento del malware
  28. La solución local debe permitir la gestión a través de la interfaz de línea de comandos (CLI).
  29. La solución debe soportar las reglas YARA como estándar para la creación de reglas para la detección de malware
  30. La solución local va a crear cuentas de administrador con al menos dos perfiles distintos: la lectura y escritura y solamente lectura.
  31. La solución local debe permitir la creación de cuentas de administrador con autenticación local o remota a través de servidores RADIUS



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

32. La solución local debe permitir la configuración del servicio de envío de correo electrónico de notificaciones cuando se detectan archivos maliciosos y reportes automáticos frecuentes.
33. La solución local es instalar los paquetes de actualización de los módulos de seguridad tan pronto como estén disponibles.
34. Deben soportar el análisis de los archivos maliciosos en un ambiente controlado con al menos los sistemas operativos Windows 10, Windows 8.1, Windows 7, macOS, Linux, Android, and ICS systems
35. La solución local debe ser compatible con la compra, descarga e instalación de máquinas virtuales adicionales.
36. El sistema de análisis debe trabajar en forma que permita que el firewall envíe archivos para su análisis de forma automática.
37. Permitir a los usuarios introducir una lista de contraseñas predeterminada para los archivos para analizar bajo demanda
38. Permite subir archivos y/o URLs manualmente para su inspección conductual, implica hasta 5 archivos y/o URLs al mes.
39. Deberá permitir la interacción con las máquinas virtuales mientras se realiza el análisis bajo demanda.
40. Todo análisis y bloqueo de malware y/o código malicioso debe ocurrir en tiempo real y el bloqueo debe ser inmediato, no se aceptarán soluciones que solo detecten malware y/o código malicioso

#### 6.5. SERVICIO DE FIREWALL DE APLICACIONES

##### CARACTERÍSTICAS GENERALES

1. La solución podrá ser brindada desde la nube del postor o con un appliance dedicado onpremise.
2. La solución debe de tener un firmware específico destinado a la finalidad de Firewall de Aplicación Web (WAF –Web Application Firewall), así como las licencias necesarias para su funcionamiento y protección de servidores y aplicaciones Web.
3. La solución debe de soportar virtualización en: hypervisor VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Docker Containers, Amazon AWS, Microsoft Azure, Google Cloud, Oracle Cloud.
4. Se debe proteger 2 dominios o subdominios o aplicación
5. La solución debe de soportar el modelo de seguridad positiva definido por OWASP y proteger contra el Top 10 de ataques a aplicaciones definido por OWASP.

##### WAF

6. Debe tener soporte nativo de HTTP/2.
7. Debe soportar traducción de HTTP/2 a HTTP 1.1
8. Deberá soportar interoperabilidad con OpenAPI 3.0
9. Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de virus y reputación IP, la cual se debe actualizar automáticamente y de manera periódica.
10. La solución debe permitir elegir entre utilizar la base de datos completa o solamente la base de datos que contiene los últimos y más peligrosos virus.
11. Deberá tener algoritmos para detección de amenazas avanzadas basados en aprendizaje de máquina con Inteligencia Artificial (AI) para detectar anomalías y aprender si se trata de ataques o no.
12. Deberá minimizar la ocurrencia de Falsos Positivos y falsos negativos utilizando Inteligencia Artificial.
13. Tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs, parámetros de URLs, campos de formularios y lo que se espera de cada campo.
14. El perfil aprendido de forma automática debe de poder ser ajustado.
15. Tener la capacidad de creación de firmas de ataques personalizables

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Humberto Amador Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
01001322143





UNSCH

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

16. Tener la capacidad de protección contra ataques tipo:
  - a. Adobe Flash binary (AMF) protocol
  - b. Botnet
  - c. Browser Exploit Against SSL/TLS (BEAST)
  - d. Acceso por fuerza bruta  
Clickjacking
  - e. Cambios de cookie
  - f. Zero Day Attacks
  - g. Credit Card Theft
  - h. Cross Site Request Forgery (CSRF)
  - i. Cross site scripting (XSS)
  - j. Denial of Service (DoS)
  - k. HTTP header overflow
  - l. Local File inclusion (FLI)
  - m. Man-in-the-middle (MITM)
  - n. Remote File Inclusion (RFI)
  - o. Server Information Leakage
  - p. Low-rate DoS
  - q. Slow POST attack
  - r. Slowloris
  - s. Malformed XML
  - t. SYN flood
  - u. Forms Tampering
  - v. Manipulación de campos ocultos
  - w. Tipo Directory Traversal
  - x. Access Rate Control
17. Protección contra envíos de comandos SQL ocultos en las requisiciones enviadas a la base de datos (SQL Injection).
18. Tener la capacidad de configurar protección del tipo TCP SYN flood-style para prevención de DoS para cualquier política, a través de Syn Cookie y Half Open Threshold.
19. Permitir configurar reglas de bloqueo a métodos HTTP no deseados.
20. Permitir que se configuren reglas de límite de upload por tamaño del archivo.
21. Debe permitir que el administrador bloquee el tráfico de entrada o salida en base a países, sin la necesidad de gestionar manualmente los rangos de dirección IP correspondientes a cada país.
22. Debe soportar crear políticas de geo-localización, permitiendo que el tráfico de determinado país sea bloqueado.
23. Permitir configurar listas negras de bloqueo y listas blancas de confianza, basadas en dirección IP de origen.
24. Permitir la liberación temporal o definitiva (white-list) de direcciones IP bloqueadas por tener originado ataques detectados por la solución.
25. Debe permitir añadir, automáticamente o manualmente, en una lista de bloqueo, las direcciones IP de origen, según la base de IP Reputation.
26. Tener la capacidad de conectarse a una base de datos en Internet para validar que las credenciales que usan los usuarios para acceder a algún sistema no sean credenciales robadas.
27. Tener la capacidad de prevención contra pérdida de información (DLP), bloqueando la pérdida de información del encabezado HTTP.
28. Tener la funcionalidad de proteger el website contra acciones de defacement, con recuperación automática y rápida del website en caso de fallo.
29. Tener la funcionalidad de antivirus integrada para inspección de tráfico y archivos, sin la necesidad de instalación de otro equipo.
30. Tener la capacidad de investigar y analizar todo el tráfico HTTP para validar si cumple con el RFC del protocolo HTTP o si ha sufrido alguna alteración y debe ser bloqueado.
31. Debe de ser capaz de hacer aceleración de tráfico SSL basada en hardware.

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Hubner J. J. Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
CIPM 112145



UNSCH

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

32. La solución debe de ser capaz de funcionar como terminador de sesión SSL para aceleración de tráfico.
33. Para SSL/TLS offload soportar al menos SSL 3.0, TLS 1.0, 1.1, 1.2 y 1.3
34. La solución debe tener la capacidad de almacenar certificados digitales de CA's.
35. La solución debe de ser capaz de generar CSR para ser firmado por una CA.
36. La solución debe de ser capaz de chequear los certificados válidos y que no fueron revocados por una lista CRL.
37. La solución debe contener las firmas de bot conocidos como link checkers, indexadores de web, search engines, spiders y web crawlers que puedan ser añadidos a los perfiles de control de acceso, así como resetear dichas conexiones
38. La solución debe de tener un sistema de bloqueo con base en la reputación de direcciones IP públicas conocidas. La lista de IPs con mala reputación debe de ser actualizado automáticamente.
39. La solución debe de ser capaz de limitar el total de conexiones permitidas hacia cada servidor real de un pool de servidores.
40. La solución debe permitir la customización o reenvío de solicitudes y respuestas HTTP en el HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body y HTTP Location.
41. La solución debe permitir crear reglas definiendo el orden con que las páginas deben de ser accedidas para prevenir ataques como cross-site request forgery (CSRF).
42. La solución debe de tener la capacidad de definir restricción a determinados métodos HTTP.
43. La solución debe tener la capacidad de proteger contra detección de campos ocultos.
44. Permitir que se configuren firmas customizadas de ataques y DLP, a través de expresiones regulares
45. La solución debe permitir la integración con scanners de vulnerabilidades de terceros, tales como Acunetix, IBM AppScan, WhiteHat, etc, para proveer parches virtuales.
46. Debe generar perfil de protección automáticamente a partir de reporte en formato XML generado por scanner de vulnerabilidad de terceros.
47. Debe permitir programar la verificación de vulnerabilidades.
48. La solución debe generar un reporte de análisis de vulnerabilidades en formato HTML.
49. Soportar redirección y reescritura de requisiciones y respuestas HTTP.
50. Permitir redirección de requisiciones HTTP para HTTPS.
51. Permitir reescribir la línea URL del encabezado de una requisición HTTP.
52. Permitir reescribir el campo HOST del encabezado de una requisición HTTP.
53. Permitir reescribir el campo REFERER del encabezado de una requisición HTTP.
54. Permitir redirigir requisiciones para otro website.
55. Permitir enviar respuesta HTTP 403 Forbidden para requisiciones HTTP
56. Permitir reescribir el parámetro LOCATION en el encabezado HTTP de una respuesta de redirección HTTP de un servidor web.
57. Permitir reescribir el cuerpo ("body") de una respuesta HTTP de un servidor web.
58. Permitir añadir el campo X-Forwarded-For para identificación de la dirección IP real del cliente cuando en modo proxy reverso.
59. La solución debe de soportar reglas para definir si las requisiciones HTTP serán aceptadas en función de la URL y origen de la petición y, si necesario, aplicar una tasa específica de velocidad (rate limit).
60. La solución debe de soportar combinación de control de acceso y autenticación utilizando mecanismos como HTML Form, Basic y soporte a SSO, métodos como LDAP y RADIUS para consultas e integración de los usuarios de la aplicación.
61. Tener capacidad de caching para aceleración web.
62. La solución debe de ser capaz de enviar archivos para solución de sandboxing del mismo fabricante, a través de una política de restricción de carga del archivo.
63. Debe permitir al administrador crear nuevas firmas y/o cambiar las firmas pre existentes.

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Humberto Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
01/01/2024



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

#### 7. SOPORTE TÉCNICO

24 (Horas del día) x 7 (días de la Semana) x 12 meses. EL PROVEEDOR deberá contar con una línea de atención de primer nivel para que la entidad pueda reportar las incidencias y problemas. Luego de reportar incidencia el PROVEEDOR emitirá un ticket de atención.

Herramienta Gestión de Red/visualización de tráfico: la cual deberá mostrar el tráfico de datos de manera semanal, quincenal y mensual; con un acceso único de USUARIO Y CONTRASEÑA (se entregará al finalizar la implementación).

Es de responsabilidad del PROVEEDOR brindar el servicio de internet, y cumplir con los tiempos de respuesta y solución ante averías, y garanticen la velocidad, seguridad y disponibilidad mensual del acceso a Internet requerido.

El tiempo de respuesta será máximo de 20 minutos, siendo el tiempo desde que la entidad reporta la incidencia y el proveedor asigne un ticket de atención. El tiempo de solución será máximo de 12 horas. En caso de avería de planta externa (fibra óptica), el tiempo de reparación del servicio será máximo hasta 12 horas adicionales.

En caso de avería de equipo se aceptará el tiempo que tome el fabricante en hacer el cambio.

#### 8. PLAZOS DE EJECUCION DE LA PRESTACION

- El plazo de servicio será por un periodo de **12 meses**, considerados desde el día siguiente de la suscripción del acta de conformidad o acta de inicio de servicio.
- El plazo de implementación para el servicio de Internet y de la seguridad perimetral es de máximo **35 días** calendario, considerado desde la fecha de firma del contrato o de la confirmación de la recepción de la orden de servicio. Si el último día es sábado, domingo o feriado, el último día a considerar será el día útil más próximo.

#### 9. PERSONAL CLAVE

El personal propuesto para la solución del servicio deberá pertenecer a la planilla del postor, teniendo como único objetivo, mantener la comunicación directa y fluida con el contratista.

##### 9.1 JEFE DE PROYECTO (01 Persona)

###### Formación académica:

- Título universitario en ingeniería electrónica y/o ingeniería de telecomunicaciones y/o ingeniería de sistemas y/o Ingeniería electrónica. Colegiatura vigente y habilitado.

###### Capacitación:

- Capacitación de mínimo 20 horas en gestión de proyectos y certificado de PMP vigente (Project Management Profesional)
- Capacitación de mínimo 20 horas en ITIL v4 y certificado ITIL v4

###### Experiencia:

- Experiencia mínima de 05 años en Gestión de proyectos y/o servicios de telecomunicaciones tales como internet y/o transmisión/ comunicación/ enlace/ interconexión de datos y/o telefonía y/o seguridad.

##### 9.2 GESTOR DE PROYECTO (01 Persona)

###### Formación académica:

- Título universitario en ingeniería electrónica y/o ingeniería de telecomunicaciones y/o ingeniería de sistemas y/o Ingeniería electrónica. Colegiatura vigente y habilitado.

###### Capacitación:

- Capacitación de mínimo 20 horas en ITIL v4 y certificado ITIL v4

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Huéner Jaramba Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
CUP 122145





UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- Capacitación de mínimo 20 horas en gestión de proyectos y certificado PMP vigente.

**Experiencia:**

- Experiencia mínima de 05 años en Gestión de proyectos y/o servicios de telecomunicaciones tales como internet y/o transmisión/ comunicación/ enlace/ interconexión de datos y/o telefonía y/o seguridad.

**9.3 ESPECIALISTA DE REDES (01 Persona)**

**Formación académica:**

- Técnico y/o título universitario en electrónica o telecomunicaciones o sistemas o informática o computación o electrónica o Industrial o redes y comunicación.

**Capacitación:**

- Certificado del equipo router ofertado vigente
- Capacitación de mínimo 20 horas en redes
- Certificado ITIL v4

**Experiencia:**

- Experiencia mínima de 03 años en implementación de proyectos de redes.

**9.4 ESPECIALISTA DE SEGURIDAD (01 Persona)**

**Formación académica:**

- Técnico y/o título universitario en electrónica o telecomunicaciones o sistemas o informática o computación o electrónica o Industrial o redes y comunicación.

**Capacitación:**

- Certificado del equipo de seguridad firewall ofertado vigente
- Capacitación de mínimo 20 horas en seguridad.
- Capacitación de mínimo de 20 horas en redes.

**Experiencia:**

- Experiencia mínima de 04 años en implementación de proyectos de seguridad

**10. CAPACITACION Y/O ENTRENAMIENTO**

El proveedor debe otorgar las siguientes capacitaciones:

- 6 cupos para 6 personas en entrenamiento oficial de seguridad en la marca ofertada para el firewall perimetral.
- 6 cupos para 6 personas en entrenamiento en:
  - Fundamentos de ITIL4, en un centro autorizado.
  - Gestión de proyectos PMP, en un centro autorizado.
- Estas capacitaciones podrán ser brindadas de manera virtual o presencial.

**11. 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.

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Huéner J. Jankupa Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
CUPM 112345



UNSCH

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

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.

#### 12. FORMA DE PAGO

- El pago se realizará de forma mensual luego de emitida la conformidad del servicio.
- Comprobante de pago.
- Informe mensual de consumo y uso del servicio

#### 13. CONFIDENCIALIDAD

La empresa contratista se compromete a guardar la más absoluta reserva de la información relacionada a la implementación y prestación del servicio, a fin de garantizar la seguridad e integridad de los procesos, programas, datos e información pertenecientes a LA ENTIDAD. Así como a no violar la confidencialidad, seguridad y propiedad de los archivos, programas y sistemas de aplicación, absteniéndose, a efectuar cualquier tipo de cambio, transacción, modificación y adición de información a los archivos, programas y sistemas de aplicación, no pudiendo facilitar a terceros, bajo ningún concepto, información alguna, sin la respectiva autorización por escrito de LA ENTIDAD.

El Contratista deberá mantener un adecuado resguardo de los datos de carácter personales en tratamiento como producto del presente servicio. Asimismo, deberá dar estricto cumplimiento con lo establecido en la ley N° 29733 – Ley de Protección de Datos Personales, su Reglamento aprobado mediante el Decreto Supremo N° 003-2013-JUS, así como el Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, y modifica la indicada Ley N° 29733; pudiendo adoptarse además buenas prácticas como las contenidas en la Directiva de Seguridad elaborada por la Autoridad Nacional de Protección de Datos Personales.

Asimismo, el Contratista debe considerar que son otras obligaciones contractuales las siguientes:

- La información y documentos proporcionados por LA ENTIDAD para la ejecución del contrato, así como los resultados que se obtengan de éste, son de uso exclusivo para el desarrollo de las actividades inherentes a la contratación e íntegramente propiedad de la entidad.
- Conservar y tratar como reservada toda la información que se declare como información confidencial. Esta no será revelada en ningún caso y bajo ningún motivo sin el consentimiento previo y por escrito de LA ENTIDAD.
- Limitar el acceso a la información confidencial de forma tal que sólo sea accesible a aquellas personas que necesariamente deban involucrarse en las conversaciones, tratativas y/o acuerdos mantenidos con LA ENTIDAD.
- No divulgar ni transferir a terceros la información a la que pudiera tener acceso él o su personal, siendo que, de ser el caso, responderá legalmente por los daños y perjuicios causados.
- Comprometerse a guardar la información confidencial en un archivo especial que posea las condiciones suficientes de seguridad.

Las presentes condiciones de confidencialidad no serán aplicables a información que:

- Resulte accesible al público por causa distinta del incumplimiento de la obligación de confidencialidad por la parte receptora (el contratista).
- Haya sido publicada con anterioridad a la fecha de la firma de contrato.
- Sea independientemente desarrollada por la parte receptora (el contratista), siempre que no se hubiese utilizado para ello ningún tipo de información proporcionada por LA ENTIDAD.

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Humberto Pantoja Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
01041122145



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

- Deba ser revelada para dar cumplimiento de una orden de naturaleza judicial o administrativa, en cuyo caso la parte receptora (el contratista) deberá informar a LA ENTIDAD en forma inmediata a la sola recepción de la citada orden.

**14. DOCUMENTACIÓN OBLIGATORIA PARA LA ADMISIÓN DE LA OFERTA**

- a) Licencia de funcionamiento y un certificado emitido por una empresa consultora externa (certificadora en servicios TI y/o infraestructura), que acredite la operación e infraestructura propia del NOC & SOC
- b) Certificaciones de ANSI/TIA y/o EPIS de Diseño o Construcción y Operación.
- c) Diagrama de la salida internacional detallando los dos nombres de los proveedores TIER I.

**15. DOCUMENTACIÓN ADICIONAL PARA EL PERFECCIONAMIENTO DEL CONTRATO**

- a) Constancia emitida por el NAP PERÚ.

**16. CONFORMIDAD**

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 la OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN en el plazo máximo de SIETE (7) DÍAS, de producida la recepción.

**17. RESPONSABILIDAD POR VICIOS OCULTOS**

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

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

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Huéner Jiménez Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
CIPN° 122145





UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

### 3.2. REQUISITOS DE CALIFICACIÓN

<b>A</b>	<b>CAPACIDAD LEGAL</b>
	<b>HABILITACIÓN</b>
	<p><u>Requisitos:</u></p> <p>El postor deberá estar registrado como empresa prestadora de valor añadido autorizada por el Ministerio de Transportes y Comunicaciones para prestar los servicios de almacenamiento y retransmisión de datos, mensajería interpersonal, mensajería de voz y servicio de conmutación de datos por paquetes (Acceso a internet) a nivel nacional.</p> <p><b>Importante</b></p> <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> <p><u>Acreditación:</u></p> <p>Copia simple del certificado de inscripción en el registro para el servicio de valor añadido emitido por el Ministerio de Transportes y Comunicaciones.</p> <p><b>Importante</b></p> <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.3</b>	<b>CALIFICACIONES DEL PERSONAL CLAVE</b>
<b>B.3.1</b>	<b>FORMACIÓN ACADÉMICA</b>
	<p><u>Requisitos:</u></p> <p><b>JEFE DE PROYECTO (01 Persona)</b> Título universitario en ingeniería electrónica y/o ingeniería de telecomunicaciones y/o ingeniería de sistemas y/o Ingeniería electrónica. Colegiatura vigente y habilitada.</p> <p><b>GESTOR DE PROYECTO (01 Persona)</b> Título universitario en ingeniería electrónica y/o ingeniería de telecomunicaciones y/o ingeniería de sistemas y/o Ingeniería electrónica. Colegiatura vigente y habilitada.</p> <p><b>ESPECIALISTA DE REDES (01 Persona)</b> Técnico y/o título universitario en electrónica o telecomunicaciones o sistemas o informática o computación o electrónica o Industrial o redes y comunicación.</p> <p><b>ESPECIALISTA DE SEGURIDAD (01 Persona)</b> Técnico y/o título universitario en electrónica o telecomunicaciones o sistemas o informática o computación o electrónica o Industrial o redes y comunicación.</p> <p><u>Acreditación:</u></p> <p>El BACHILLER O TÍTULO PROFESIONAL será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link.</p>

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Humberto J. Huamanga Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
CIPN 122146



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

<https://enlinea.sunedu.gob.pe/> o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: <https://titulosinstitutos.minedu.gob.pe/>, según corresponda.

**Importante para la Entidad**

*El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.*

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

**B.3.2 CAPACITACIÓN**

Requisitos:

**JEFE DE PROYECTO (01 Persona)**

- Capacitación de mínimo 20 horas en gestión de proyectos y certificado de PMP vigente (Project Management Profesional)
- Capacitación de mínimo 20 horas en ITIL v4 y certificado ITIL v4

**GESTOR DE PROYECTO C (01 Persona)**

- Capacitación de mínimo 20 horas en ITIL v4 y certificado ITIL v4
- Capacitación de mínimo 20 horas en gestión de proyectos y certificado PMP vigente.

**ESPECIALISTA DE REDES (01 Persona)**

- Certificado del equipo router vigente
- Capacitación de mínimo 20 horas en redes
- Certificado ITIL v4

**ESPECIALISTA DE SEGURIDAD (01 Persona)**

- Certificado del equipo de seguridad firewall ofertado vigente
- Capacitación de mínimo 20 horas en seguridad.
- Capacitación de mínimo de 20 horas en redes.

Acreditación:

Se acreditará con copia simple de CONSTANCIAS, CERTIFICADOS, U OTROS DOCUMENTOS

**Importante**

*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.*

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Hiram J. Anticona Paila  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
DPM 822145



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

**B.4 EXPERIENCIA DEL PERSONAL CLAVE**

Requisitos:

**JEFE DE PROYECTO (01 Persona)**

Experiencia mínima de 05 años en Gestión de proyectos y/o servicios de telecomunicaciones tales como internet y/o transmisión/ comunicación/ enlace/ interconexión de datos y/o telefonía y/o seguridad.

**GESTOR DE PROYECTO (01 Persona)**

Experiencia mínima de 05 años en Gestión de proyectos y/o servicios de telecomunicaciones tales como internet y/o transmisión/ comunicación/ enlace/ interconexión de datos y/o telefonía y/o seguridad.

**ESPECIALISTA DE REDES (01 Persona)**

Experiencia mínima de 03 años en implementación de proyectos de redes

**ESPECIALISTA DE SEGURIDAD (01 Persona)**

Experiencia mínima de 03 años en implementación de proyectos de seguridad

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

Acreditación:

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

**Importante**

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

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA  
Ing. Humberto Pareda Paililla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
DPT. 122145





UNSCH

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a <b>S/ 2,400,000.00 (DOS MILLONES CUATROCIENTOS MIL CON 00/100 SOLES)</b>, 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 <b>SERVICIO DE INTERNET; Y/O SERVICIO DE INTERCONEXIÓN Y/O SERVICIO DE CONEXIÓN Y/O SERVICIO DE COMUNICACIÓN Y/O SERVICIO DE DATOS; Y/O SERVICIO DE TELEFONÍA DIGITAL Y SERVICIO DE LÍNEA DEDICADA DE ACCESO A INTERNET.</b></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>1</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 <b>Anexo N° 8</b> referido a la Experiencia del Postor en la Especialidad.</p> <p>En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p> <p>Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.</p> <p>Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el <b>Anexo N° 9</b>.</p>

<sup>1</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 si se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
31  
Ing. Huérfano J. Benavente Patilla  
JEFE DE TECNOLOGÍAS DE LA INFORMACIÓN  
CHUMVILLA



UNSC

OFICINA DE  
TECNOLOGÍAS DE  
LA INFORMACIÓN

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.*

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA  
Ing. Humberto J. Patilla  
JEFE DE TECNOLOGÍAS DE INFORMACIÓN  
CUIV 122343



#### 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.		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
<u>Acreditación:</u>  Se acreditará mediante el documento que contiene el precio de la oferta ( <b>Anexo N° 6</b> ).		
		<b>100 puntos</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.*





## 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>10</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>10</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 ULTIMO 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>11</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 ULTIMO 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>11</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 accesorias 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>12</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>13</sup>.*

<sup>12</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>13</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° 2-2024-UNSCH-CS-1**

Presente.-

El que se suscribe, [.....], postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE <sup>14</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.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios<sup>15</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>14</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>15</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° 2-2024-UNSCH-CS-1**

Presente.-

El que se suscribe, [...], representante común del consorcio [CONSIGNAR EL NOMBRE DEL CONSORCIO], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Datos del consorciado 1				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE <sup>16</sup>		Sí	No	
Correo electrónico :				

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

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE <sup>18</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:

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.

<sup>16</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>17</sup> Ibídem.

<sup>18</sup> Ibídem.





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>19</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>19</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° 2-2024-UNSCH-CS-1**  
Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

#### **Importante**

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



### ANEXO N° 3

#### DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores

**COMITÉ DE SELECCIÓN**

**CONCURSO PÚBLICO N° 2-2024-UNSCH-CS-1**

Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el servicio de [CONSIGNAR OBJETO DE LA CONVOCATORIA], de conformidad con los Términos de Referencia que se indican en el numeral 3.1 del Capítulo III de la sección específica de las bases y los documentos del procedimiento.

[CONSIGNAR CIUDAD Y FECHA]

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

#### **Importante**

*Adicionalmente, puede requerirse la presentación de documentación que acredite el cumplimiento de los términos de referencia, conforme a lo indicado en el acápite relacionado al contenido de las ofertas de la presente sección de las bases.*



#### ANEXO N° 4

#### DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores

**COMITÉ DE SELECCIÓN**

**CONCURSO PÚBLICO N° 2-2024-UNSCH-CS-1**

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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





## ANEXO N° 5

### PROMESA DE CONSORCIO

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

Señores

**COMITÉ DE SELECCIÓN**

**CONCURSO PÚBLICO N° 2-2024-UNSCS-CS-1**

Presente.-

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

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

a) Integrantes del consorcio

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

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

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

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

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

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [%]<sup>20</sup>

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

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

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%<sup>22</sup>

[CONSIGNAR CIUDAD Y FECHA]

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

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

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



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

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

**Importante**

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



## ANEXO N° 6

### PRECIO DE LA OFERTA

Señores  
**COMITÉ DE SELECCIÓN**  
**CONCURSO PÚBLICO N° 2-2024-UNSCH-CS-1**  
Presente.-

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

CONCEPTO	PRECIO TOTAL
<b>TOTAL</b>	

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

[CONSIGNAR CIUDAD Y FECHA]

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

#### Importante

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

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

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores  
**COMITÉ DE SELECCIÓN**  
**CONCURSO PÚBLICO N° 2-2024-UNSCH-CS-1**  
Presente.-

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

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

<sup>23</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>24</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>25</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>26</sup> Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

<sup>27</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>28</sup> Consignar en la moneda establecida en las bases.



Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP <sup>23</sup>	FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>24</sup>	EXPERIENCIA PROVENIENTE <sup>25</sup> DE:	MONEDA	IMPORTE <sup>26</sup>	TIPO DE CAMBIO VENTA <sup>27</sup>	MONTO FACTURADO ACUMULADO <sup>28</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° 2-2024-UNSCH-CS-1**  
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

#### **Importante**

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

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

ANEXO N° 12

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

**(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)**

Señores

**COMITÉ DE SELECCIÓN**

**CONCURSO PÚBLICO N° 2-2024-UNSCH-CS-1**

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.*