

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

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



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

SIMBOLOGÍA UTILIZADA:

N°	Símbolo	Descripción
1	[ABC] / [.....]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / [.....]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	<div>Importante</div> <ul style="list-style-type: none"> • Abc 	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	<div>Advertencia</div> <ul style="list-style-type: none"> • Abc 	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	<div>Importante para la Entidad</div> <ul style="list-style-type: none"> • Xyz 	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

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

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

INSTRUCCIONES DE USO:

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

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

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

CONCURSO PÚBLICO N° 02-2023-UNC

**CONTRATACIÓN DE SERVICIO DE INTERNET 2.5 GBPS
ADMINISTRADO EN ALTA DISPONIBILIDAD PARA LA
SEDE CENTRAL Y FILIALES DE LA UNIVERSIDAD
NACIONAL DE CAJAMARCA¹**

¹ En respuesta a la consulta 1

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.

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.mp.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.

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

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 Digitales²). 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*

² 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. PENALIDADES

3.5.1. 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.

3.5.2. 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.

3.6. 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.

3.7. 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.

3.8. 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 CAJAMARCA
RUC N° : 20148258601
Domicilio legal : AV. ATAHUALPA N° 1050 – CAJAMARCA
Teléfono: : (+51)076 599220
Correo electrónico: : logistica@unc.edu.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la CONTRATACIÓN DEL SERVICIO DE INTERNET 2.5 GBPS ADMINISTRADO EN ALTA DISPONIBILIDAD PARA LA SEDE CENTRAL Y FILIALES DE LA UNIVERSIDAD NACIONAL DE CAJAMARCA.³

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante MEMORANDO N° 160-2023-DIGA-UNC el 11 de Agosto del 2023.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios

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.

³ En respuesta a la consulta 1

1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

El plazo máximo para la entrega del servicio de acceso a internet con su respectivo equipamiento (router, seguridad perimetral, optimizador de ancho de banda, otros) es 120 días calendarios contados a partir del día siguiente de la firma de contrato.

El plazo de la prestación del servicio materia de la presente convocatoria se prestará por un periodo de 24 meses, contados a partir de la fecha de activación solicitada por parte de la entidad. La fecha de activación será posterior a la suscripción del acta de conformidad de la implementación o instalación de servicio.

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/ 5.00 en Caja de la Oficina de Tesorería de la Universidad Nacional de Cajamarca.

Importante

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

1.10. BASE LEGAL

- Ley N°31638 Ley de Presupuesto del Sector Público para el Año Fiscal 2023.
- Ley N° 31639 Ley de Equilibrio Financiero del Presupuesto del Sector Público para el Año Fiscal 2023.
- Texto Único Ordenado de la Ley N° 30225 Ley de Contrataciones del Estado, aprobado por el Decreto Supremo N° 082-2019-EF, y sus modificatorias.
- Decreto Supremo N° 344-2018-EF, Reglamento de la Ley de Contrataciones del Estado y sus modificatorias.
- Decreto Legislativo N° 1272 que modifica la Ley N° 27444, Ley del Procedimiento Administrativo General.
- Código Civil

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

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos⁴, la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

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

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

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

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

Advertencia

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

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

⁴ La omisión del índice no determina la no admisión de la oferta.

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

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

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

Importante

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

2.2.1.2. Documentos para acreditar los requisitos de calificación

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

2.2.2. Documentación de presentación facultativa:

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

Advertencia

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

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

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

⁶ 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 – PIDE⁷ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación⁸ (**Anexo N° 12**).
- i) Detalle de los precios unitarios del precio ofertado⁹.
- j) Datasheet oficial de los equipos router en inglés o español.
- k) La impresión de página web del fabricante o con una carta del fabricante que verifique que los modelos propuestos para router no se encuentran en estado de end-of-life o end-of-sale o end-of-support.
- l) Datasheet oficial de los equipos Next Generation Firewall en inglés o español.
- m) Link público del fabricante que verifique que los modelos propuestos para los equipos Next Generation Firewall no se encuentran en estado de end-of-life o end-of-sale o end-of-support.
- n) Documentación pública de la página web del fabricante para comprobar el requerimiento de throughput de los equipos Next Generation Firewall en inglés o español.
- o) Carta del fabricante que acredite que el proveedor cuenta con la plataforma AntiDDos.
- p) Datasheet de la plataforma AntiDDos.
- q) Carta del fabricante que acredite que el proveedor cuenta con un servicio de Ciberdefensa.
- r) Datasheet de servicio de Ciberdefensa.
- s) Carta del fabricante o partner local o mayorista establecido en el Perú para los equipos Router, Next Generation Firewall, Ancho de Banda, al momento del contrato, donde establezca que los componentes ofertados deben ser nuevos y de primer uso.
- t) Datasheet oficial de los equipos Administración de Ancho de Banda en inglés o español.
- u) Link público del fabricante que verifique que los modelos propuestos para los equipos Administración de Ancho de Banda no se encuentran en estado de end-of-life o end-of-sale o end-of-support.
- v) Datasheet oficial de la solución de respaldo en la nube en inglés o español.

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*

⁷ 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/>

⁸ En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

⁹ Incluir solo en caso de la contratación bajo el sistema a suma alzada.

REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2> opción consulta de empresas acreditadas en el REMYPE.

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

Importante

- Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.
- De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya¹⁰.
- 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 AV. ATAHUALPA N° 1050 EN LA OFICINA GENERAL DE LOGISTICA EDIFICIO 1S – 109 – CIUDAD UNIVERSITARIA, en el horario de 8:00 a.m a 2:45 p.m.

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).

Incorporar a las bases o eliminar, según corresponda.

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en pagos periódicos mensualizados.

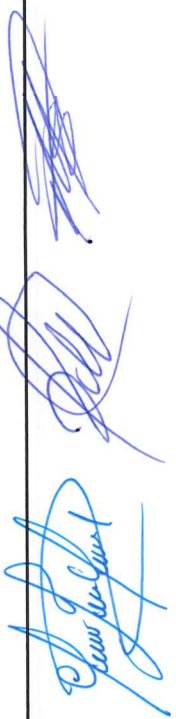
Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Informe del funcionario responsable de la Oficina de Tecnologías de La Información, emitiendo la conformidad de la prestación efectuada.

¹⁰ Según lo previsto en la Opinión N° 009-2016/DTN.

- Comprobante de pago.

La documentación podrá ser presentada en la mesa de partes de la UNC sito en Av. Atahualpa 1050 (Ciudad Universitaria) en horario de 07:00 am a 2:45 pm o en los siguientes correos en forma electrónica: oficinainformatica@unc.edu.pe y logistica@unc.edu.pe (los documentos pertinentes serán tramitados en horario de oficina).



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

"SERVICIO DE INTERNET 2.5 GBPS ADMINISTRADO EN ALTA DISPONIBILIDAD PARA LA SEDE CENTRAL Y FILIALES DE LA UNIVERSIDAD NACIONAL DE CAJAMARCA"



1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de internet 2.5 Gbps administrado en alta disponibilidad para la Sede Central y filiales de la Universidad Nacional de Cajamarca.²

2. FINALIDAD

La Oficina de Tecnologías de Información tiene como funciones entre otras evaluar necesidades y oportunidades de ampliación de las tecnologías de información a nivel institucional; así como, conducir el uso racional y óptimo de los recursos informáticos en la Universidad. Un recurso fundamental es el Internet, la red de redes que permite interconectar la Universidad con el mundo con el fin de compartir servicios e información.

La Universidad accede a internet mediante una conexión de fibra óptica con un ancho de banda de 500Mbps en el campus de sede central y de 20Mbps para el campus universitario de cada una de las Filiales. El ancho de banda fue contratado en septiembre del 2020 en tiempos de Pandemia del Covid 19, temporada en la cual la población se encontraba en cuarentena y en el caso de la Universidad los estudiantes y docentes realizaban sus actividades académicas de manera virtual; de manera similar los servidores de la Universidad realizaban sus labores de manera remota y excepcionalmente algunas horas de manera presencial. En ese entonces los estudiantes, docentes y servidores realizaban sus actividades académicas y administrativas conectados mediante el internet en casa sin consumir el internet Institucional.

El regreso a la presencialidad ha traído consigo el uso intensivo de las tecnologías de información aplicados a los nuevos modelos académicos de enseñanza aprendizaje y nuevos modelos de trabajo en entornos colaborativos; modelos que hacen uso intensivo de datos en forma de video, audio y streaming en las actividades académicas como el dictado de clases, proyección de videos, emisión de audios, acceso a recurso académicos entre otros y en el trabajo administrativo cotidiano las reuniones virtuales, capacitaciones en línea, acceso a sistemas gubernamentales, trabajo colaborativo; estos nuevos paradigmas de enseñanza y trabajo han llevado al colapso el ancho de banda de la universidad, que en hora punta se puede apreciar una degradación y lentitud del servicio de internet en el campus de la Universidad debido al acceso masivo de aproximadamente 5000 estudiantes, 600 docentes y 800 servidores que se conectan de manera concurrente desde más de un dispositivo físico y/o dispositivo móvil.

¹ En respuesta a la consulta 1

² En respuesta a la consulta 1



Con el fin de mejorar el servicio de internet se pretende ampliar el ancho de banda de 0.5Gbps a 2.5Gbps en el campus de la sede central y en cada filial, ampliar el ancho de banda de 20Mbps a 100Mbps, acción que beneficiará a una población estudiantil de al menos 12000 estudiantes de pregrado y posgrado, 900 docentes, 600 administrativos y a la población en general que hace uso de los servicios de tecnologías de información que la Institución ofrece.

3. OBJETIVOS DE LA CONTRATACIÓN

✓ Objetivo General

Contratar servicio de internet línea dedicada a 2.5Gbps en la sede central y a 100Mbps en cada una de las filiales.

✓ Objetivos Específicos

Contratar los servicios de un proveedor de comunicaciones que brinda los siguientes servicios:

- Servicio de acceso principal y de contingencia a Internet de banda ancha a través de línea dedicada.
- Servicio de Red Privada Virtual.
- Servicio de Seguridad Perimetral en alta disponibilidad.
- Servicio de administración de ancho de banda.
- Servicio de mitigación de ataques de denegación de servicio.
- Servicio de respaldo en la nube.

4. ANTECEDENTES

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, y sus modificatorias.
- Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital.
- Licenciamiento institucional.
- Soportar con tecnología las condiciones básicas de calidad mínimas exigibles a las Universidades que permitan el licenciamiento de programas y el licenciamiento institucional.
- Decreto Legislativo N.° 1496. Artículo 3, que modifica el artículo 47 de la Ley Universitaria (Ley N.° 30220), sobre las modalidades para la prestación del servicio educativo. La Ley Universitaria establece la modalidad presencial, semipresencial y a distancia o no presencial para la prestación del servicio educativo en el contexto pandémico. Tiene por objeto ampliar el acceso a la educación de calidad y adecuar la oferta universitaria a las diversas necesidades educativas.

La Universidad Nacional de Cajamarca publica información a través del portal web institucional como parte del cumplimiento de la Ley de transparencia y



acceso a la información pública, así mismos realiza registro de información en aplicativos webs de otras instituciones del estado en cumplimiento de normativa vigente, lo que hace necesario contar con acceso a internet para cumplir con tal fin. Asimismo, el ancho de banda del servicio de internet y su tecnología tienen un papel preponderante en la calidad de los servicios Académicos y Administrativos en relación a la velocidad de subir y bajar información.

5. ALCANCES DEL SERVICIO A CONTRATAR.

Para soportar la capacidad de 2.5Gbps, se requiere:

Tabla 1 Ítems del Servicio

ITEM	DESCRIPCIÓN	CANTIDAD
01	Servicio de acceso principal y de contingencia a Internet de banda ancha mediante Fibra Óptica	1
02	Servicio de Red Privada Virtual	1
03	Servicio de Seguridad Perimetral en alta disponibilidad.	1
04	Servicio de Protección contra ataques de denegación de servicio	1
05	Servicio de administración de ancho de banda	1
06	Servicio de respaldo en nube	1

6. CARACTERÍSTICAS Y CONDICIONES:

➤ CARACTERÍSTICAS DEL SERVICIO DE INTERNET

- ✓ Enlace de Internet simétrico con un ancho de banda mínimo de 2.5 Gbps, con un Overbooking 1:1.
- ✓ El Overbooking solicitado de 1:1 corresponde desde la puerta de enlace del router de internet de la Universidad Nacional de Cajamarca hasta la puerta de enlace del proveedor conectado directamente a el(los) proveedor(es) de Internet.
- ✓ El servicio de acceso dedicado a internet deberá contar con una alta disponibilidad en modo activo – pasivo, el enlace de contingencia se activará en caso de falla del enlace principal. Se requiere que la



contingencia se garantice al menos en la última milla que es desde el punto de presencia del postor hasta la puerta de enlace del router de internet de la Universidad Nacional de Cajamarca, el cual se debe proveer de dos nodos distintos y con el mismo ancho de banda que el enlace principal, cabe aclarar que nodo hace referencia al punto de presencia del postor donde tenga infraestructura propia y equipo de acceso.

- ✓ El medio de transporte deberá ser 100% fibra óptica para el enlace principal y de contingencia, desde el punto de presencia del proveedor hasta el Data Center de la Universidad. Dentro del Campus de la Universidad deberá ser totalmente canalizado y subterráneo en todo su recorrido. Se precisa que el proveedor deberá asumir todos los costos de la infraestructura que considere.
- ✓ Los enlaces de internet principal y contingencia para la Universidad Nacional de Cajamarca deberán venir de distintos nodos.
- ✓ Se podrá usar las ducterías subterráneas existentes para realizar el tendido de fibra del enlace principal y enlace de contingencia.
 - Ductería 1(Puerta principal - DataCenter): Aproximadamente 290mts de ductería subterránea.
 - Ductería 2(Puerta los patos - DataCenter): Aproximadamente 480mts de ductería subterránea.

Una vez terminado el servicio contratado toda la infraestructura de obra civil adicional instalada para el tendido de fibra óptica pasara a ser propiedad de la Universidad Nacional de Cajamarca.

- ✓ El proveedor podrá agendar una cita para verificar el recorrido de la ductería y/o realizar un análisis del estado de la infraestructura del Datacenter de la Universidad con el fin de precisar de mejor manera su propuesta. El proveedor deberá evaluar en su estudio de campo el recorrido de fibra óptica en la Universidad y será responsable de la implementar la infraestructura y adecuaciones necesarias hasta llegar al Data Center, no generando costos adicionales a la entidad.³
- ✓ El tendido de fibra óptica y componentes deben ser nuevos y de primer uso.
- ✓ El Proveedor deberá proveer los router de propósito dedicado y demás equipos necesarios, para realizar la conexión a internet, este equipo deberá tener las siguientes características como mínimo:
 - Routing: BGP, OSPF, RIP, Rutas estáticas y enrutamiento basado en rutas y políticas.
 - Capacidad de memoria RAM o DRAM de 8 GB. La memoria FLASH 2 GB.

³ En respuesta a la consulta 6



- En ningún caso se podrá presentar soluciones que estén en etapa de obsolescencia o que hayan anunciado su End-of-life o dejen de ser fabricadas, comercializadas y/o soportadas durante todo el tiempo que se brinde el servicio. Esto deberá ser respaldado por la impresión de página web del fabricante o con una carta del fabricante.⁴
- Este y los demás equipos o accesorios necesarios para la provisión del servicio deberán ser nuevos y de primer uso, provistos en calidad de alquiler, los cuales serán instalados y configurados por el proveedor.
- Se deberá entregar el datasheet oficial del equipo propuesto en los documentos para el perfeccionamiento del contrato en inglés o español.⁵
- ✓ El equipo router debe ser de una marca de prestigio internacional y deberá soportar la integración con una arquitectura SD-WAN. El equipo será otorgado en calidad de alquiler y demás accesorios necesarios para realizar la conexión a internet.⁶
- ✓ El Proveedor instalará y configurará todos los equipos, dispositivos y/o componentes necesarios para la puesta en funcionamiento del servicio sin que esto implique costo adicional para La Universidad Nacional de Cajamarca.
- ✓ El Postor deberá contar con salida 100% fibra óptica al Backbone Internacional de Internet con mínimo 02 operadores internacionales que le proporcione cada uno enlace de 10 Gbps o más.
- ✓ El Proveedor deberá tener disponibilidad de protocolo de ruteo IP V4 / IP V6.
- ✓ El protocolo de transporte del Backbone del postor debe ser MPLS.
- ✓ El postor deberá proveer de mínimo 32 direcciones IPv4 públicas de Internet. Dentro de las 32 IPs a entregar se consideran las IPs para configuración como: IP del Router, la IP de la red y la IP de broadcast. Así mismo los registros DNS, es decir la pronta inscripción de nuestros dominios en los servidores del proveedor.
- ✓ El postor deberá considerar un pool de al menos 256 IPv6 públicas.
- ✓ El proveedor deberá considerar el equipamiento necesario hasta el ingreso al puerto óptico y/o RJ45 del Switch LAN y DMZ de la Universidad Nacional de Cajamarca para iniciar el servicio.
- ✓ El proveedor deberá poseer servidores DNS redundantes y distribuidos geográficamente en locales distintos.

⁴ En respuesta a la observación 8

⁵ En respuesta a la consulta 9, 74, 212

⁶ En respuesta a la observación 268, consulta 144



- ✓ El proveedor deberá brindar una plataforma WEB con la funcionalidad mínima para la gestión del registro de subdominios, para la cual brindará un usuario y contraseña luego de la inscripción de los dominios DNS o el proveedor deberá presentar un procedimiento de atención en 30 minutos a través de un sistema de generación de ticket (mediante correo electrónico o llamada telefónica) con un tiempo máximo de atención de 02 horas para el registro de subdominios.⁷
- ✓ El protocolo de comunicación será TCP/IP.
- ✓ El prestador del servicio opcionalmente pertenecerá al NAP (Network Acces Point) Perú u tendrá un acceso al NAP a través de un miembro integrante activo y 100% operativo del NAP.⁸
- ✓ El servicio de Internet deberá ser brindado las veinticuatro (24) horas del día, los siete (7) días de la semana, los trescientos sesenta y cinco (365) días del año, con una disponibilidad mínima mensual de 98.88%. el servicio podría verse afectado por causas externas ajenas al operador, en estos casos, cualquier afectación al servicio deberá poder ser reportada a las centrales de atención del prestador del servicio a fin de darle la atención correspondiente.
- ✓ En relación al porcentaje de disponibilidad, se precisa que el cumplimiento de la obligación de la calidad requerida, se restringe al cumplimiento de las normas regulatorias vigentes emitidas por el Ministerio de Transportes y Telecomunicaciones y el OSIPTEL (Decreto Supremo N° 013-93-TTC - Texto Único Ordenado de la Ley de Telecomunicaciones y demás normas vigentes), reconociéndose que el servicio podría verse afectado por causas externas ajenas al operador; supuesto en el cual la afectación del servicio deberá ser reportada a las centrales de atención que el proveedor indiquen, a fin de darle la atención correspondiente, sin que ello genere la aplicación de ninguna penalidad.
- ✓ El Proveedor deberá reparar o reemplazar sin costo alguno los equipos o componentes que sean necesarios para asegurar la prestación del servicio siempre y cuando la falla de estos no sea imputable a la Universidad Nacional de Cajamarca. En los casos en que la entidad sea responsable de la avería o interrupción, estas no serán consideradas para el cálculo de indisponibilidad del servicio.
- ✓ Por otro lado, se indica que en caso la avería o falla ocurra dentro de las instalaciones de la UNC por uso negligente de la entidad, el costo de los bienes que se provisionarán para subsanar la avería será asumido por la entidad.

⁷ En respuesta a la observación 12

⁸ En respuesta a la consulta 213, 227



- ✓ Para la imputación de responsabilidades por la existencia de averías en el servicio (corte, caída o degradación del servicio), se evaluará previamente si estas deberán recaer sobre el proveedor o sobre la Entidad, siendo que, de comprobarse que la referida contingencia fue originada por la Entidad o por un hecho ajeno a las partes (caso fortuito o fuerza mayor), no se generará ningún tipo de penalidad en contra del proveedor ni se le imputará ningún incumplimiento.

➤ **SERVICIO DE RED PRIVADA VIRTUAL – RPV**

- ✓ Universidad Nacional de Cajamarca requiere contratar un proveedor de telecomunicaciones que brinde el servicio de transmisión de datos a nivel local y nacional para que interconecte sus sedes remotas con su sede principal ubicado en Cajamarca a través de enlaces privados.
- ✓ Las tecnologías a emplear deben asegurar una comunicación confiable, íntegra y segura.
- ✓ El local donde concurrirán todas las conexiones de las Sedes Remotas tanto local como nacional será el que está ubicado en la Sede Principal sito en Av. Atahualpa Km. 3 - Cajamarca.
- ✓ El servicio de transmisión de datos en la sede principal deberá contar con una alta disponibilidad en modo activo-pasivo, el enlace de contingencia se activará en caso de falla del enlace principal. Se requiere que la contingencia se garantice al menos en la última milla y con el mismo ancho de banda que el enlace principal.
- ✓ Los equipos deberán ser instalados en las sedes remotas y principal, para el cual la entidad deberá considerar las conexiones y/o instalaciones eléctricas necesarias para la alimentación de los equipos Routers entre otros que el proveedor instalará.
- ✓ Para las líneas de transmisión de datos se debe considerar configuración de clases de servicio (Cos) de los equipos. Las clases de servicio se da en el siguiente orden de prioridad: Voz/Video, Datos Críticos y Datos no Críticos; los valores de ancho de banda por cada tipo de tráfico a priorizar en las configuraciones de Cos se coordinarán conjuntamente con personal encargado de Universidad Nacional de Cajamarca, los cuales deberán soportar y garantizar adecuadamente una comunicación a nivel de Voz, Video y Datos, para lo cual el proveedor deberá realizar las configuraciones y priorizaciones necesarias para llegar a la configuración ideal. Los circuitos a contratar permitirán a los usuarios de las oficinas



remotas interactuar con toda la red de la Universidad Nacional de Cajamarca.

- ✓ La Universidad Nacional de Cajamarca necesita conectar ocho (8) locales remotos con necesidades de consumo de ancho de banda iguales, en función al tráfico que generan sus equipos hacia las oficinas principales y la carga de usuarios que atienden, en tal sentido se establece los siguientes valores de anchos de banda mínimos solicitados.
- ✓ El Servicio de transmisión de datos debe tener una disponibilidad mínimo de 98.50% en la sede principal y para las sedes remotas una disponibilidad mínima de 98.50%. y El proveedor de servicio debe garantizar una transmisión segura, íntegra y confiable de la voz, video y datos desde la sede remotas hacia la Sede Principal, considerando como factor crítico en el transporte de la información, una trayectoria privada separada de la red pública de Internet.
- ✓ La última milla para las sedes remotas deberá ser provista por fibra óptica (FO), todos los componentes instalados deberán ser nuevos y de primer uso.⁹
- ✓ El proveedor de servicios debe asegurar el 100% de ancho de banda contratado por Universidad Nacional de Cajamarca podrá realizar pruebas de esfuerzo en las líneas dedicadas para verificar que se cumplan los valores solicitados, y El proveedor no podrá emplear el Internet como medio de transporte para la interconexión de la sede. No se aceptará una solución basada en túneles a través de Internet.
- ✓ La tecnología WAN a emplear por el proveedor deberá ser MPLS y los enlaces de transmisión de datos deben definir clases de servicio para asegurar su óptimo desempeño, así como un óptimo tratamiento a los servicios sensibles a retardos, tales como voz, video, datos críticos y otros que se definan, y Los circuitos privados no deberán ser filtrados por la empresa proveedora del servicio.
- ✓ La Universidad Nacional de Cajamarca proporcionará espacio en el gabinete de comunicaciones para alojar los equipos que serán instalados por el proveedor.

⁹ En respuesta a la consulta 10



Tabla 2. Ubicación de Gabinetes de Comunicaciones¹⁰

PROVINCIA	DISTRITO	LOCAL	DIRECCIÓN	LATITUD	LONGITUD	ANCHO DE BANDA DE BANDA PROYECTADO (Mbps) REDISTRIBUIDO	ANCHO DE BANDA DE BANDA PROYECTADO (Mbps) REDISTRIBUIDO
1 CAJAMARCA	CAJAMARCA	CAMPUS UNC	AV. ATAHUALPA 1050 ALTURA DE KM 3.	-7.167098°	-78.495602°	1700	(SUJETO A DEMANDA DE LA FILIALES)
2 CAJABAMBA	CAJABAMBA	CAJABAMBA	CASERIO PAMPA GRANDE S/N	-7.60848°	-78.06042°	100	150
3 CELENDÍN	CELENDÍN	CELENDÍN	SHUITUTE S/N - CHACAPAMPA	-6.857032°	-78.142122°	100	150
4 HUALGAYOC	BAMBAMARCA	BAMBAMARCA	LA BANDA S/N EX. PECUARIA	-6.675417°	-78.521472°	100	150
5 CHOTA	CHOTA	CHOTA	AV. AGRICULTURA N° 144	-6.561333°	-78.646444°	100	150
6 JAEN	JAEN	CAMPUS JAEN	JR. MARIETA S/N	-5.716460°	-78.801970°	100	150
7 JAEN	JAEN	OFICINAS JAEN	JR. BOLIVAR NS 1342	-5.708428°	-78.807814°	100	150
8 CAJAMARCA	CAJAMARCA	CENTRO DE IDIOMAS	Jr. dos de mayo 334	7.158416932702338	78.517716534655	100	150
9 CAJAMARCA	CAJAMARCA	CENTRO PRE UNIVERSITARIO	José Gálvez 191	-7.15951	78.52492	100	150
TOTAL						2.5 Gbps	

- ✓ La Universidad Nacional de Cajamarca tendrá la posibilidad de solicitar al proveedor una redistribución de los anchos de banda RPV, a necesidad de la entidad.

➤ **SOLUCIÓN DE NEXT GENERATION FIREWALL**

El servicio deberá contar con una solución de seguridad perimetral, para ello el PROVEEDOR instalará en calidad de alquiler dos (02) equipos Next Generation Firewall, configurados en alta disponibilidad modalidad activo/standby, appliance de propósito dedicado, para garantizar un óptimo

¹⁰ En respuesta a la consulta 189, 329



servicio, el PROVEEDOR deberá proveer equipos de seguridad que sean nuevos, de primer uso y de tecnología vigente de parte de la marca a proponer, por lo cual no deberá estar en estado End-Of-Life o End-Of-Support o End-Of-Sale o similares. En caso de falla del equipo principal (Activo), el equipo Stand-by se activará hasta que se culmine la gestión del servicio de reposición con el fabricante (RMA) del equipo principal.

El proveedor deberá contar con un SOC propio o tercerizado en territorio nacional.¹¹

Cada equipo principal de la solución debe contar con las siguientes características mínimas:

➤ DESCRIPCIÓN

- Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.
- La solución tiene que ser ofrecida en alta disponibilidad, se entiende por alta disponibilidad, es decir por lo menos 2 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones.
- El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls
- El fabricante deberá tener una efectividad de seguridad mayor o igual al 97% según el último reporte de NSS Labs para Next Generation Firewall.
- La plataforma propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS.
- La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.
- Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar en estado en el sitio web del fabricante de end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado. Dicha información se presentará para la firma de contrato.
- Los equipos NGFW deberán tener soporte vigente de fábrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware

¹¹ En respuesta a la consulta 151



- Se deberá proporcionar una cuenta de acceso al portal oficial de educación del fabricante, donde la Entidad tendrá la potestad de acceder, de manera gratuita y a demanda, a cursos en línea sobre las diversas tecnologías del fabricante, así como exámenes y certificaciones. Dichos accesos serán proporcionados luego de finalizado la etapa de implementación. Se aclara que en caso las certificaciones tengan costo, esta será asumida por la entidad.
- Como parte de la propuesta, se deberá proporcionar el acceso a una herramienta que permita evaluar el nivel de adopción de buenas prácticas de configuración en el Next Generation Firewall implementado, con la finalidad de mejorar la postura de seguridad de red proporcionada por la solución. Dichos accesos serán proporcionados luego de finalizado la etapa de implementación.
- La herramienta de evaluación de buenas prácticas deberá ser específica para la configuración de Next Generation Firewall implementado, no se aceptarán portales con guías de usuarios genéricas.
- La Entidad deberá poder realizar la evaluación de buenas prácticas a libre demanda y de manera autónoma.

✓ **CAPACIDAD**

- Throughput de Prevención de Amenazas de 5 Gbps medido con tráfico productivo real (transacciones usando una mezcla de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Seguridad avanzada en DNS, Antivirus/Antimalware de red, Antispyware, AntiBot, control de amenazas avanzadas de día cero (Sandboxing), Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
- No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento



de throughput con documentación pública en la página web del fabricante.

- El equipo debe soportar como mínimo 1.3 Millones de sesiones simultáneas y 140 mil nuevas sesiones por segundo, medidos con paquetes en capa 7.
- Disco interno SSD de 480 GB o superior.
- Mínimo 12 interfaces de red 1Gbps en cobre en formato RJ45
- Mínimo 10 interfaces de red de 10Gbps en formato SFP, con posibilidad de cambiar a 1G en formato SFP cambiando solo el transceiver, se debe incluir al menos 4 SFP+ para conexión 10Gbps en fibra multimodo.
- Mínimo 4 interfaces de red de 25Gbps en formato SFP28, no es necesario la inclusión de transceivers.
- Mínimo 1 interface de red 10/100/1000 en cobre en formato RJ45 dedicada para la administración.

✓ CARACTERÍSTICAS GENERALES

- El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.
- Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.
- Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel.
- Soportar IPv4 y IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.
- Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.

✓ ALTA DISPONIBILIDAD

- Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).



- La configuración en alta disponibilidad debe sincronizar: Sesiones, Certificados de descifrado, Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red.
- Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces.
- Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.

✓ **FUNCIONALIDADES DE FIREWALL**

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

✓ **DESCIFRADO DE TRÁFICO SSL/TLS**

- Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.
- Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.



- Debe ser capaz de inspeccionar el tráfico cifrado, incluyendo el protocolo TLS 1.3.
 - Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.
 - Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS
 - Debe soportar certificados que utilicen Subject Alternative Name (SAN) y Server Name Indication (SNI).
 - Debe permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar el no descifrado de páginas con contenido sensible, mientras forzar el descifrado de páginas de clasificación de riesgo alto o medio
 - Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.
 - Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).
- ✓ **PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (DoS)**
- Debe ser posible definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood.
 - Para el caso de los SYN Flood debe ser posible utilizar SYN Cookies como medidas de defensa
 - La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor)
 - La protección contra ataques Flood deberá permitir definir al menos 3 tipos de umbrales, el primero para generar una alerta al administrador, el segundo para activar la protección y el tercero para restringir el acceso en su totalidad en base a dicha política de DoS



- Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo
- La protección contra ataques de escaneo deberá permitir definir una lista de excepciones basadas en direcciones IP origen, a los cuales no se le aplicará la protección.
- Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route
- Debe proteger contra ataques basados en protocolos No-IP en interfaces Layer 2 (como Appletalks, Banyan, VINES, Novell, SCADA), la solución deberá soportar la definición de protocolos a ser aceptados en base al formato Ethertype (Hex).
- Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia dicho equipo.

✓ CONTROL DE APLICACIONES

- Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
- Debe poder identificar y crear políticas de seguridad basadas en aplicaciones de Sistemas de Infraestructura Crítica (ICS) como addp, bacnet, modbus, dnp3, coap, dlms, iccp, iec-60870-5-104, mms-ics, rockwell, siemens, entre otros.
- Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.
- Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
- Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.
- Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto y protocolo, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.



- Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.
- Con el objetivo de identificar aplicaciones propietarias a nivel de capa 7, la solución debe permitir nativamente la creación de aplicaciones personalizadas desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante.
- Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en sus atributos.
- Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.

✓ PREVENCIÓN DE AMENAZAS

- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware, Antibot.
- Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por spyware en entornos corporativos
- Las funcionalidades de IPS, Antivirus, Antispyware y Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.
- El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus, Antispyware y Antibot.
- Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia.
- Debe incorporar una plataforma de sandbox basada en nube para el análisis de ejecutables desconocidos.
- Con el objetivo de tener la información de amenazas actualizada, la plataforma deberá ser capaz de actualizar su base de firmas en tiempo real sin afectar el performance del equipo.
- Debe soportar granularidad en las políticas de IPS, Antivirus, Antispyware y Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.



- Debe identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que el Firewall debe bloquear dichas consultas DNS.
- Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto y/o generar firmas para las aplicaciones propietarias a partir de una herramienta provista por el propio fabricante.
- Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.
- Debe soportar la creación de firmas de IPS basadas en el formato de Snort.

✓ **ANÁLISIS DE MALWARE DE DÍA CERO**

- La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.
- La plataforma de Sandboxing podrá ser ofrecido en Nube (Cloud), On-premise o ambos. Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y MacOS.
- Deberá ser capaz de analizar 1000 archivos por hora realizando análisis dinámico (es decir, no uso de firmas)
- En caso de tratarse de una plataforma de Sandboxing Cloud, deberá cumplir con los siguientes requerimientos:
- Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
- Deberá ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades terceras.
- Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II de AICPA, ISO 27001, ISO 27017 e ISO 27018.
- En caso de tratarse de una plataforma de Sandboxing On-premise, deberá cumplir con los siguientes requerimientos:
- Deberá ser desplegado en Alta Disponibilidad (Activo-Pasivo), con el objetivo de mantener los controles de ciberseguridad en caso de falla de uno de los equipos.



- Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows, MacOS, Linux y Android.
 - Debe admitir topologías de implementación en modo sniffer o en línea (in-line)
 - Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
 - El Next Generation Firewall debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB (versiones 1, 2 y 3). Tanto en IPv4 como en IPv6.
 - Debe permitir al administrador la descarga del archivo original analizado por el Sandbox.
 - Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.
 - Permitir la subida de archivos al sandbox de forma manual y vía API.
 - Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
 - La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.
- ✓ **FILTRO DE CONTENIDO WEB**
- Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
 - Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía Active Directory, LDAP en general y base de datos local.
 - Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs
 - Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing.
 - Debe contar con multi categorías de URL, que permita conocer si una web de una categoría determinada está catalogada como riesgo bajo, medio o alto.



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

✓ IDENTIFICACION DE USUARIOS

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

✓ QOS



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

✓ VPN

- Soportar VPN Site-to-Site en protocolo IPSec
- La VPN site to site debe soportar como mínimo:
 - DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
 - Autenticación MD5, SHA-1, SHA-2;
 - Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
 - Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
- Permitir aplicar QoS dentro de los túneles VPN.
- Soportar VPN client-to-site pudiendo operar usando el protocolo IPSec o SSL.
- Permitir la conexión por medio de agente instalado en el sistema operativo.
- Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
- Debe permitir definir segmentos de red para ser agregadas de forma automática y manual en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN.
- El Split Tunnel debe permitir elegir el tipo tráfico que se enrutará por el túnel VPN, basado en el nombre de la Aplicación y Dominio. Por ejemplo, la navegación a Salesforce que viaje por el túnel VPN, pero no todo el resto de tráfico de internet.
- Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
 - Antes del usuario se autentique en la estación;
 - Después de la autenticación del usuario en la estación usando Single Sign On (SSO);



- Bajo demanda del usuario;
- El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y IOS.
- La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada. La identificación de equipos colocados en cuarentena se debe basar en un ID inmutable del Cliente VPN, de tal forma que la restricción no pueda ser eludida (por ejemplo, si la cuarentena se hace a una IP, el malware puede modificar la IP del equipo para eludir la cuarentena)
- Debe ser posible colocar equipos en cuarentena de forma manual y automática.
- Debe ser posible bloquear el acceso a red de los equipos colocados en cuarentena.
- Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado, que permita validar determinadas características del equipo y en base al nivel de cumplimiento (compliance) del host permitir, denegar o limitar el acceso a los recursos de la red interna. Por lo menos se deberá poder configurar los siguientes casos de uso y una combinación de ellas:
 - Parches instalados en el cliente: según un número de parche determinado, según el nivel de criticidad del parche y proveedor del gestor de parches.
 - Antimalware instalado en el cliente: validar si se encuentra configurado con protección en tiempo real, si las firmas se encuentran actualizadas en un número determinado de días (personalizable, por ejemplo, firmas actualizadas en los últimos 2 días), validar si se ha realizado un escaneo de malware en el cliente dentro de un número determinado de días (personalizable, por ejemplo, exigir un escaneo el último día), evaluar el proveedor de la solución de antimalware.
 - Firewall de host: validar si el Firewall del host se encuentra habilitado, validar el proveedor del gestor de firewall.
 - Cifrado de disco: validar si el cliente tiene instalado un software de cifrado de disco y el proveedor de la solución de cifrado.
 - Software DLP: validar si el cliente tiene instalado un software de DLP y el proveedor de la solución de DLP.
 - Permitir añadir validaciones de aplicaciones personalizadas añadiendo la Clave de Registro (en caso de Windows) o Plist (en caso de MacOS)
 - Este control deberá estar disponible al menos para equipos Windows y MacOS, en al menos 1800 dispositivos.



- Todos los parámetros indicados deberán poder ser realizados desde la consola gráfica de la plataforma. No se aceptarán configuraciones a través de CLI.

✓ ADMINISTRACIÓN Y MONITOREO

- Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante
- Permitir exportar las reglas de seguridad en formato CSV y PDF
- Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.
- Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
- Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino)
- Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
- Contar con un módulo o vista que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.
- Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se superpongan reglas generales sobre reglas específicas (shadowing rules).
- Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.



- Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
- Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó, su IP y el horario de la alteración;
- Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.
- Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, antibot, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
- La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.

➤ **SOLUCIÓN DE ADMINISTRACIÓN DE ANCHO DE BANDA**

El PROVEEDOR, deberá entregar en calidad de alquiler una solución de administración de ancho de banda, para ello el PROVEEDOR instalará un (01) equipo (appliance) de propósito dedicado, para garantizar el óptimo servicio el PROVEEDOR deberá proveer equipo nuevo, de primer uso y de tecnología vigente, por lo cual no deberá tener ningún anuncio de fin de vida tal como End-Of-Life o End-Of-Support o End-Of-Sale o similares. La solución debe contar con las siguientes características mínimas:

- ✓ Debe ser un equipo dedicado y de propósito específico de tipo appliance (no UTM, no Firewalls, no Balanceadores, no servidores, etc) y todo el software en el equipo debe ser integrado directamente por el mismo fabricante, no se aceptará soluciones de tipo software que depende de sistemas operativos genéricos (Windows o Linux) que deben ser instalados previamente, a fin de garantizar una solución integral.
- ✓ El appliance deberá incluir licenciamiento para la administración de ancho de banda según el ancho de banda del servicio de internet (2.5Gbps de bajada y 2.5Gbps de subida) y posibilidad de soportar crecimiento hasta 6 Gbps mediante licenciamiento adicional sin necesidad de hacer cambios de equipo o hardware.
- ✓ Capacidad de soportar un mínimo de 600 mil flujos concurrentes.



- ✓ Capacidad de soportar un mínimo de 25 mil nuevas conexiones por segundo.
- ✓ Capacidad de soportar un mínimo de 800 mil paquetes por segundo.
- ✓ Dos Fuentes de energía "hot-plug" y Disco interno de 1.5TB SSD, RAID1 o superior
- ✓ El appliance debe tener mínimo 02 pares de interfaces bridge en formato fibra de 10Gbps con funcionalidad bypass integrada es decir un total de 4 Interfaces 10Gbps (fibra multimodo). Soportar al menos 2 interfaces de 10Gbps, adicionalmente a las interfaces indicadas las cuales se usarán para el control de tráfico¹². Se requiere una (01) interface de red dedicada para la administración de tipo RJ45 1Gbps con capacidad IPMI (Intelligent Platform Management Interface).
- ✓ La solución deberá estar licenciada para realizar tareas de visualización de tráfico y control de ancho de banda.
- ✓ Incluir la activación de un caché en capa de aplicación para tráfico HTTP, y opcionalmente TCP y HTTPS, a través de licenciamiento de software y no agregando componentes de hardware a la solución¹³, la función del caché consiste en reducir el tráfico repetitivo de tipo Web en el enlace gestionado.
- ✓ Debe permitir garantizar ancho de banda variable (burstable), empleando filtros de aplicaciones descubiertas o creadas, VLANs, hosts, subredes, aplicaciones o una combinación de todos.
- ✓ Debe permitir la temporización de las políticas de control, filtro y/o descarte para al menos los siguientes indicadores:¹⁴
 - Aplicaciones descubiertas
 - Usuarios o grupos de usuarios (en caso de integración con AD)
 - Hosts
 - Subredes
 - VLANs
 - Combinación de los anteriores
 - La temporización basada en día de la semana y hora del día.
- ✓ Debe permitir la división y asignación del ancho de banda agregado (circuito virtual) empleando un mecanismo de asignación dinámica por IP de host (externo o interno) permitiendo la distribución compartida y equitativa del recurso virtual (circuito virtual), la limitación del número de hosts y la asignación de ancho de banda manual.

¹² En respuesta a la consulta 61

¹³ En respuesta a la consulta 64

¹⁴ En respuesta a la consulta 196



- ✓ Debe permitir la configuración de cuotas de transferencia por usuario o host. Las cuotas deben ser asignadas en volumen de KB o MB o GB o TB., con temporización diaria, semanal y mensual¹⁵. El sistema de control debe permitir asignar acciones concretas (descarte, limitación de ancho de banda) a usuarios o host que transgredan la cuota asignada.
- ✓ Debe permitir limitar la cantidad de sesiones establecidas permitiendo implementar un control de admisión basado en al menos las siguientes condiciones:
 - Aplicación
 - Grupo de aplicaciones
 - Hosts o subred IP
 - VLAN
 - Combinación de los criterios anteriores
- ✓ Debe tener la capacidad de aplicar las políticas de control de ancho de banda para las nuevas conexiones como también para las conexiones existentes, de tal forma que le permita al administrador establecer acciones que actúan inmediatamente sobre el tráfico después de su activación.
- ✓ Opcionalmente la solución podrá tener un sistema auto-protección y/o detección de incongruencias de las políticas configuradas en diferentes niveles jerárquicos de la configuración.¹⁶
- ✓ Debe descubrir 3000 servicios de aplicaciones en forma automática con la inclusión de:
 - BitTorrent, eDonkey, Ares, Gnutella, Thunder, Winny, incluyendo protocolos P2P Encriptados
 - Servicios de voz como Skype empresarial (Skype for Business) y Skype diferenciando entre voz y video, GoogleTalk, Fring
 - Streaming de Audio y Video MPEG, AVI, MP3, Silverlight, YouTube, Vimeo, QUIC, Netflix y Quicktime reconocidos como aplicaciones aun cuando se emplee HTTP
 - Servicios de descargas vía Web, como Directdownload
 - Aplicaciones empresariales como SAP, Salesforce, Office365, LotusNotes, Microsoft Exchange, Citrix
 - Aplicaciones en dispositivos móviles como Whatsapp, facetime, Line, Viber y Spotify

¹⁵ En respuesta a la consulta 65

¹⁶ En respuesta a la consulta 114



- ✓ Debe permitir la personalización de los nombres de los aplicativos y debe poder expresarse los nombres de los filtros agregados manualmente en un lenguaje determinado (mínimo español e inglés) por el cliente.
- ✓ Debe permitir la agrupación de aplicaciones según su naturaleza y criticidad según se requiera. Ejemplo; YouTube, Facebook, Twitter dentro de un grupo de recreación, HTTP y HTTPS (a ciertos portales) dentro de Navegación. Los nombres de estos grupos deben ser posible de ser creados en español e inglés.
- ✓ Debe poder ser integrado con sistemas de autenticación Windows Active Directory de forma que sea posible obtener reportes por nombre de usuario, así como la capacidad de asignar políticas de control empleando esta información.
- ✓ Debe soportar la exportación de información a aplicaciones de colección externa a través de NetFlow versiones 1, 5 y 9. Donde el puerto de envío UDP sea configurable.
- ✓ Debe permitir acceso a estadísticas almacenadas vía SQL con la opción de poder configurar direccionamiento IP que permita únicamente el ingreso a estas consultas para evitar accesos indeseados.
- ✓ Debe permitir el monitoreo en tiempo real de al menos:
 - Aplicaciones presentes en el enlace
 - Conversaciones IP en el enlace
 - Hosts presentes en el enlace
 - Usuarios (en caso se integre con AD)
 - Estadísticas de rendimiento como latencia transaccional
- ✓ Debe descubrir y reportar conversaciones IP existentes en el enlace incluyendo como mínimo los siguientes parámetros:
 - IPs origen y destino
 - Servicio de aplicación empleado
 - Nombre del usuario (en caso se integre con AD)
 - Throughput y flujos
- ✓ Visibilidad para aplicaciones TCP de las siguientes condiciones de rendimiento transaccional:
 - Información de tráfico retransmitido
 - Retardo transaccional de servidor
 - Retardo transaccional de red
 - Jitter reportado
 - Perdidas entrantes y salientes
 - Round trip time (RTT)



- ✓ Visibilidad de al menos la siguiente información respecto del tráfico de sesiones:
 - Cantidad de sesiones
 - Sesiones TCP rechazadas por el servidor
 - Sesiones TCP ignoradas por el servidor
 - Sesiones TCP abortadas por el cliente
- ✓ Debe permitir en la misma consola (UI) hacer drill down para al menos, desde un grupo de aplicación detectado, determinar los hosts de los participantes
- ✓ Debe reportar estadísticas de rendimiento TCP, indicando valores de transmisión y retransmisión para aplicaciones TCP en forma tabular y gráfica.
- ✓ Debe permitir la correlación de variables de rendimiento generando un valor único indicador de rendimiento, sobre el cual debe permitirse la configuración de umbral de alarma, las variables para considerar en el cálculo de valor único como mínimo son las siguientes:
 - Pérdida de paquetes
 - Retardo transaccional de servidor
 - Retardo transaccional de red
 - Jitter reportado
 - Round trip time (RTT)
- ✓ Visibilidad para tráfico de voz/videoconferencia sobre IP, al menos la siguiente información:
 - IPs origen y destino
 - Jitter
 - Pérdida
 - Latencia
 - MOS
 - r-Factor
- ✓ Empleando tráfico ICMP, debe permitir la evaluación del retardo de la respuesta de un host permitiendo parámetros como:
 - Dirección del host
 - Umbral de latencia
 - Tamaño de envío en bytes
 - Duración en segundos de la violación de umbral para el envío de una alarma
- ✓ Almacenamiento de datos históricos en el mismo appliance para posterior generación de reportes tabulares y gráficos de la utilización del ancho de banda hasta un mínimo de doce (12) meses atrás.



- ✓ El software y recursos para el manejo de reportes y consola de gestión debe ser provisto en el mismo appliance como una capacidad integrada sin necesidad de utilizar hardware ni software adicional ni depender de soluciones externas o en nube.
- ✓ Debe permitir la creación de reportes considerando:
 - Top 10 grupos de aplicaciones
 - Top 10 aplicaciones individuales
 - Top 10 URLs visitados
 - Top 10 hosts (internos y externos)
 - Top 10 usuarios (en caso se integre con AD)
- ✓ El sistema debe presentar la información requerida en gráficos circulares y en adición información tabular para extender el análisis más allá de 10 aplicaciones.
- ✓ Debe contar con el servicio de reposición de hardware para atención de cambio en máximo 48hrs del requerimiento del cambio en caso de falla del equipo por unidad similar o superior.

➤ **SERVICIO DE CIBERDEFENSA**

El proveedor, deberá entregar un servicio de ciberdefensa propio o de un tercero, operado por su CyberSOC opcionalmente certificado ISO 27001 en gestión de incidentes, gestión de cambios y ciberseguridad¹⁷. Este servicio deberá permitir mediante el análisis de logs de la solución de seguridad propuesta (Firewall), permita realizar investigaciones y escalar incidentes con las siguientes características:

- ✓ Capas adicionales como analítica de comportamiento de usuarios (UBA o UEBA¹⁸), orquestación, automatización y respuesta de seguridad (SOAR), para procesar múltiples eventos de seguridad y mecanismos de detección propietarios basados en Inteligencia artificial totalmente integrados al servicio, con el objetivo de validar y dar seguimiento a las investigaciones de ciberseguridad, el proveedor deberá entregar un Portal web seguro con doble factor de autenticación para revisar las investigaciones.
- ✓ El portal debe actuar como una interfaz gráfica de usuario (GUI) que muestre investigaciones que fueron realizadas por los componentes (SIEM, UBA o UEBA¹⁹, SOAR, I.A.), es decir que la herramienta cuenta con la auditoria de usuarios que realizaron cambios en la misma.

¹⁷ En respuesta a la observación 166, 128

¹⁸ En respuesta a la consulta 157, 158, 159

¹⁹ En respuesta a la consulta 157, 158, 159



- ✓ Capas adicionales al SIEM como analítica de comportamiento de usuarios (UBA o UEBA²⁰), orquestación, automatización y respuesta de seguridad (SOAR), para procesar múltiples eventos de seguridad y mecanismos de detección propietarios basados en Inteligencia artificial totalmente integrados al servicio.
- ✓ Monitoreo 24x7 identificando amenazas cibernéticas que puedan afectar la operación.
- ✓ Inteligencia de amenazas mediante actualizaciones de indicadores de compromiso (IOC) de múltiples fuentes que incluyen indicadores internos extraídos de eventos, comunidades de código abierto, redes sociales, inteligencia técnica y/o inteligencia procedente de la Deep y Dark Web. Las fuentes de inteligencia de amenazas deberán ser enviadas al gestor de eventos de la seguridad de la información para correlacionar y generar detecciones.
- ✓ Caza de amenazas sobre el gestor de eventos de seguridad, identificando, evaluando y mejorando la capacidad de detección mediante búsqueda exhaustiva de ciber-amenazas y actividades maliciosas.
- ✓ Respuesta y mitigación de incidentes en tiempo real ante ciber-amenazas.
- ✓ Optimización de procesos consistentes de desarrollo y aprendizaje que incluyan optimización de reglas, actualizaciones y sugerencias de implementación de nuevas tecnologías de detección de amenazas cibernéticas.
- ✓ La Inteligencia de amenazas debe comprobar todas las comunicaciones salientes; alertar sobre la comunicación con la IP, dominios y URL maliciosos; y finalizar la conexión inmediatamente, todo esto sucede en tiempo real.
- ✓ Investigación forense de procesos en curso de presuntas actividades maliciosas y amenazas cibernéticas incluyendo el análisis post mortem de incidentes verificados, identificando el origen del ataque, la causa raíz y proporcionar información sobre quién inició el ataque. Mínimo de 4 horas mensuales de ser requerido.
- ✓ El servicio deberá tener la capacidad de integrarse a cualquier solución de seguridad, fuente de registro y Endpoint.
- ✓ Configuración personalizable de notificaciones vía email (notificaciones, recomendaciones, acciones pendientes, nuevas investigaciones, escalamiento de una investigación en curso, modificación del estado de una investigación en curso). Opcionalmente se podrán realizar notificaciones vía email personalizables por tipo (incidente, alerta, ticket

²⁰ En respuesta a la consulta 157, 158, 159



o vulnerabilidad), por categoría (disponibilidad, performance, cambio, seguridad u otro) y por severidad (bajo, medio, alto o crítico).²¹

- ✓ La solución deberá ser capaz de aprender o ser retroalimentado tomando como referencia a incidentes históricos o base de datos externas, para conocer nuevas vulnerabilidades de un sistema, con el fin de mejorar la prevención, detección y combate de futuras amenazas en forma automática.²²
- ✓ Este servicio opcionalmente podrá tener la capacidad de ser retroalimentado por un emisor externo de incidentes para que de esta manera no sea juez ni parte en la emisión de investigaciones, a fin de asegurar la imparcialidad y permitir que la entidad pueda dar seguimiento de los tiempos de resolución y atención del postor.²³
- ✓ El almacenamiento de datos históricos para posterior generación de reportes u otros se deberá brindar hasta un mínimo de doce (12) meses atrás.²⁴

➤ **CARACTERÍSTICAS DEL SERVICIO DE MITIGACIÓN DOS/DDOS EN LA NUBE DEL PROVEEDOR DE SERVICIOS**

El proveedor deberá brindar una solución en nube del servicio de Anti – DDoS, considerando que el ataque debe de quedar en la plataforma del operador y no afectar el ancho de banda de internet contratado por la entidad.

La solución deberá ser de tipo appliance, de tecnología específica para la mitigación de ataques de denegación de servicios, no se aceptarán soluciones en las que la protección DDoS sea una funcionalidad adicional de equipos Firewall, NextGeneration Firewalls, Application Delivery Controllers, Routers u otros equipos de seguridad o redes

Las características que debe de cumplir el servicio son:

- ✓ La solución deberá tener una capacidad de mitigación de ataque de 20 Gbps como mínimo.
- ✓ La solución deberá ser de tipo Stateless
- ✓ La solución deberá tener una arquitectura de protección "Always On" y derivación sobre una misma plataforma, para el cual deberá contar con equipo dedicado que inspeccione el tráfico; y en caso de ataques volumétricos superiores al umbral de 40 Gbps, el proveedor deberá contar con algún mecanismo para su mitigación garantizando como mínimo 10 Gbps exclusivos para la universidad.

²¹ En respuesta a la consulta 330

²² En respuesta a la consulta 24, 160, 293

²³ En respuesta a la consulta 24, 160, 293

²⁴ En respuesta a la consulta 17



- ✓ La solución propuesta deberá contar con escenario de alta disponibilidad (redundancia de equipo y redundancia de Data Center) como mínimo para la arquitectura por derivación de tráfico, esto con la finalidad de garantizar la disponibilidad del servicio.
- ✓ La solución deberá tener un sistema de creación automática de firmas en tiempo real para la protección frente a ataques emergentes (se aceptará también que las firmas se creen automáticamente en el centro de investigación del fabricante y estos sean desplegados en los equipos del fabricante a nivel global.)
- ✓ Opcionalmente, deberá contar con protección contra ataques encriptados SSL.²⁵
- ✓ La solución evaluará y gestionará el comportamiento patrones de tráfico anormales para evitar ataques y al mismo tiempo permitir el paso del tráfico de usuarios legítimos, sin reducir su velocidad o mediante el uso de umbrales personalizables.²⁶
- ✓ Opcionalmente, la solución podrá contar con IPS incorporado.²⁷
- ✓ La solución de mitigación de ataques DDoS debe soportar al menos los siguientes tipos de túneles: VLAN Tagging y GRE, y opcionalmente L2TP, MPLS y GTP.²⁸
- ✓ El proveedor debe presentar una carta del fabricante que acredite que cuenta con la plataforma AntiDDoS.

➤ **SERVICIO DE RESPALDO EN NUBE**

- ✓ La solución podrá opcionalmente contar con una certificación de continuidad del negocio en los procesos de conectividad.²⁹
- ✓ Modalidad Software como Servicio (SaaS Software as a Service), la cual debe encontrarse en un centro de datos o en la nube³⁰. La disponibilidad del almacenamiento en este centro de datos debe ser de mínimo de 99.9% para garantizar la alta disponibilidad de este.
- ✓ La interacción del servicio de almacenamiento con la infraestructura del local la UNIVERSIDAD NACIONAL DE CAJAMARCA se podrá realizar a través del ancho de banda solicitado en el presente requerimiento entre la UNIVERSIDAD NACIONAL DE CAJAMARCA y la nube como contingencia. Por lo indicado, se podrá enviar información (servidores virtuales, estaciones de trabajo, medios de almacenamiento, carpetas, bases de

²⁵ En respuesta a la observación 277, 310

²⁶ En respuesta a la observación 278, 334

²⁷ En respuesta a la observación 279, 311, consulta 335

²⁸ En respuesta a la consulta 280, consulta 336

²⁹ En respuesta a la observación 282, consulta 30, 31, 47, 244

³⁰ En respuesta a la consulta 283



datos y archivos de cualquier tipo) hacia el servicio de almacenamiento con fines de trasladar la información sensible de la entidad hacia un sitio externo.

- ✓ Tamaño de almacenamiento mínimo: 20 TB.
- ✓ El almacenamiento de la nube deberá ser presentado a los servidores vía protocolos estándar HTTPs y/o NFS.
- ✓ La plataforma debe contar con cifrado AES256 y/o RSA y/o militar, y protección con contraseña.³¹
- ✓ La solución de respaldo en la nube es por un periodo de 24 meses contados a partir la activación del servicio, para lo cual se deberán entregar las credenciales de acceso al correo que la entidad designe.³²
- ✓ El proveedor brindará soporte técnico, a partir del día siguiente de entregadas las credenciales de acceso al correo que la entidad designe de acuerdo a las siguientes características:
 - Soporte remoto: 7 días por 24 horas debe incluir feriados, sábados y domingos.
 - Registrar incidentes por sistema de tickets reportados por correo electrónico, el proveedor deberá indicar la dirección de correo electrónico al cual se reportarán, dicho correo deberá ser comunicado a la Oficina de Tecnologías de la Información.

7. DISPONIBILIDAD

El servicio de Internet y seguridad perimetral deberán ser brindado las 24 horas del día, los siete (7) días de la semana, los trescientos sesenta y cinco (365) días del año con una disponibilidad de:

- ✓ Servicio de Internet mensual debe ser de mínimo 98.50% o superior.
- ✓ Servicio de seguridad gestionada la disponibilidad debe ser mínimo de 93.33 % mensual o superior.
- ✓ En caso de falla total del servicio de seguridad gestionada y/o servicio de optimización de ancho de banda, el postor deberá brindar como mínimo la continuidad del servicio de internet.
- ✓ Servicio de optimización de ancho de banda la disponibilidad debe ser mínimo de 93.33 % mensual o superior.
- ✓ Servicio de Red privada virtual mensual debe ser de mínimo 98.50% o superior en la sede principal.
- ✓ Servicio de Red privada virtual mensual debe ser de mínimo 96.50% o superior en las sedes remotas.

³¹ En respuesta a la consulta 3.18

³² En respuesta a la consulta 4.2, 287



8. ATENCIÓN DE AVERÍAS O FALLAS

- ✓ Se entenderá por avería a una interrupción total del servicio, cabe precisar que no se considerará para el cálculo de penalidades por indisponibilidad del servicio las averías parciales y/o degradaciones del servicio, no obstante, el proveedor tiene que brindar los recursos necesarios a tiempo completo durante el horario normal de trabajo para restaurar el servicio a niveles satisfactorios y teniendo como plazo máximo de tiempo de reparación total de las degradaciones del servicio 48 horas.
- ✓ Toda actividad o provisión de bienes que tenga que ejecutar el proveedor para subsanar la avería serán sin costo alguno para Universidad Nacional de Cajamarca, salvo el caso en que la avería sea imputable a la Universidad Nacional de Cajamarca.
- ✓ Se entenderá por Tiempo de Atención, al tiempo transcurrido desde que la universidad comunica la avería al postor hasta que el postor brinde un ticket de atención a la entidad por la avería. Este tiempo no deberá exceder de dos (02) horas.
- ✓ Se entenderá por Tiempo de Subsanación, al tiempo transcurrido entre la entrega del ticket por parte del postor una avería, hasta la subsanación de la misma a satisfacción de la Universidad. Este tiempo no deberá de exceder de ocho (08) horas para el Servicio de Internet, veinte y cuatro (24) horas para el servicio de Red Privada Virtual y cuarenta y ocho (48) horas para los Servicios de Seguridad Perimetral y Optimización de Ancho de Banda en la sede principal, salvo averías que impliquen rotura de fibra óptica cuyo plazo de subsanación podría tomar un tiempo adicional de ocho (8) horas, sin que esto signifique supuesto de penalidad.³³
- ✓ En caso de falla total del servicio de seguridad gestionada (caída de ambos equipos), el postor deberá subsanar el servicio en un plazo no mayor a 48 horas.³⁴
- ✓ El tiempo de subsanación para el servicio de Red Privada Virtual para las sedes remotas no deberá exceder de 24 horas, salvo averías que impliquen rotura de fibra óptica cuyo plazo de subsanación podría tomar un tiempo adicional de ocho (8) horas, sin que esto signifique supuesto de penalidad.
- ✓ El tiempo de subsanación de averías no aplica solo en los siguientes casos, siendo responsable el postor de garantizar el menor tiempo para la reposición del servicio:

³³ En respuesta a la consulta 340

³⁴ En respuesta a la consulta 176



- Cualquier demora por no poder contactar con el representante técnico de la Universidad Nacional de Cajamarca en el sitio de incidencia o si este no puede brindar acceso al sitio o lugar de incidencia.
 - Cualquier error en la información proporcionada por la Universidad Nacional de Cajamarca que pueda afectar el rápido despliegue del recurso humano o material del proveedor.
 - Cuando no se cuente con condiciones climatológicas favorables y con luz para realizar trabajos en altura.
 - Razones de fuerza mayor (ej. Inaccesibilidad del sitio o localidad debido a desastres, bloqueo de carreteras, permisos de autoridades de Gobierno, otros.)
- ✓ El proveedor deberá contar con un Centro de Atención de Averías o Mesa de Ayuda única que atenderá todas las averías del servicio contratado, reparación o asistencia técnica, permitiendo un adecuado control, reparación o asistencia técnica, gestión y seguimiento de la misma, debiendo indicar número telefónico, correo electrónico, y opcionalmente una plataforma de acceso web para el registro de averías de ser el caso (con acuse de recibo)³⁵. El proveedor del servicio deberá contar con un número 0800 gratuito para la atención de las llamadas.
 - ✓ El proveedor deberá proporcionar la información de los contactos respectivos (datos del personal técnico, número de teléfonos y/o correos electrónicos y/o direcciones web) y un cuadro de escalamiento comercial, de post-venta y atención de averías y/o asistencia técnica.
 - ✓ La Universidad Nacional de Cajamarca podrá efectuar llamadas de servicio de lunes a domingo incluyendo feriados desde las 00:00 hasta las 24:00 horas.
 - ✓ El proveedor deberá contar con un centro de atención de llamadas de reparación o asistencia técnica instalado de tal manera que le asegure a la Universidad Nacional de Cajamarca que se encuentra en condiciones de cumplir con lo estipulado en las bases.
 - ✓ Los servicios de soporte no deben tener límites de horas por intervención ni cantidad de intervenciones mensuales, dándose por atendido un problema cuando es solucionado en su totalidad y a satisfacción de la Universidad.
 - ✓ El proveedor dejará un informe técnico del servicio prestado.
9. GARANTÍA
- ✓ Se establece que el plazo de responsabilidad de vicios ocultos será de un (01) año, teniendo en cuenta que se computará a partir de otorgada la conformidad

³⁵ En respuesta a la consulta 98



de culminación del servicio total (24 meses) por parte de la entidad (de acuerdo con el art. 50 de la Ley de Contrataciones del Estado).³⁶

- ✓ La garantía incluye el reemplazo de las partes (por repuestos originales) o de todo el equipo o accesorios parte de la solución de ser necesario, con instalación incluida.
- ✓ Todos los servicios a los que está obligado el proveedor para cumplir con la garantía serán sin costo adicional para la entidad. Toda falla en la solución ofertada, deberá ser asumida por el proveedor durante el periodo de garantía.
- ✓ En ningún caso se aceptarán componentes, equipos, u otros accesorios para de la solución que estén en etapa de obsolescencia o que hayan anunciado su End-of-life o dejen de ser fabricadas, comercializadas y/o soportadas durante todo el tiempo que se brinde el servicio. Esto deberá ser respaldado por la documentación necesaria al momento de la firma del contrato. Si algún componente parte de la solución durante el tiempo que se brinde el servicio, pasase a la condición de obsolescencia o que hayan anunciado su End-of-life o dejen de ser fabricadas, comercializadas y/o soportadas deberá ser reemplazado por el proveedor hasta un plazo máximo de 60 días.³⁷

10. INSTALACIÓN

- ✓ El proveedor será el responsable de la instalación, configuración, puesta en funcionamiento y soporte de la solución ofertada, para lo cual deberá proveer y contemplar todos los bienes, servicios, obras civiles necesarios para el correcto funcionamiento de los mismos.
- ✓ Los componentes que formen parte de la solución ofertada deben ser nuevos y de primer uso, no se aceptarán licencias recicladas o de segundo uso. Será sustentado con carta del fabricante o partner local o mayorista establecido en el Perú para los equipos Router, Next Generation Firewall, Ancho de Banda, al momento del contrato.³⁸
- ✓ La solución debe implementar la alta disponibilidad y tolerancia a desastres, además de mantener un equilibrio de carga dinámico y automático para cumplir con las condiciones de rendimiento necesarias.
- ✓ El proveedor deberá configurar los equipos y políticas de seguridad y de optimización desde cero en coordinación con el personal de la Oficina de Tecnologías de Información.
- ✓ Instalar todos los componentes, accesorios u otros que sean necesarios para el correcto y total funcionamiento del servicio, sin que esto implique gasto adicional para la Universidad.

³⁶ En respuesta a la consulta 4, 121, 218, 230

³⁷ En respuesta a la observación 8

³⁸ En respuesta a la consulta 166



- ✓ El proveedor debe incluir en su propuesta, todos los costos de carácter complementario (traslados, seguros, o cualquier otro necesario para el servicio).
- ✓ Todos los trabajos y acciones a realizar se deberán ejecutar en horarios que se deben coordinar directamente con la Oficina de Tecnologías de Información, a fin de garantizar las labores académicas y administrativas de la UNC.

11. INSPECCIÓN Y PRUEBAS

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

12. CAPACITACIÓN

Capacitaciones Oficiales³⁹

- ✓ El postor debe considerar 04 capacitaciones oficiales en la marca de los equipos propuestos para la solución. 02 capacitaciones oficiales en tópicos distintos sobre seguridad gestionada para 04 persona y 02 capacitaciones oficiales en tópicos distintos sobre optimización de aplicaciones para 04 persona; las cuales se pueden brindar en los 6 primeros meses posteriores a la activación del servicio.
- ✓ Las capacitaciones oficiales serán brindadas por trainers certificados de la marca o por un centro autorizado por la misma.

³⁹ En respuesta a la observación 167, 170, consulta 102, 103, 246, 247, 248



- ✓ Las capacitaciones podrán darse de manera virtual o podrán brindarse en forma presencial, si la capacitación presencial se brinda en un lugar diferente a la ciudad de Cajamarca, el proveedor deberá asumir todos los costos que incurran la capacitación, alojamiento, traslado o movilidad, alimentación de los participantes.
- ✓ La oportunidad de las capacitaciones y los horarios serán coordinados con la Oficina de Tecnologías de la Información.
- ✓ Al final de la capacitación el proveedor en coordinación con el equipo de TI fijará la fecha para que los colaboradores capacitados brinden su examen de certificación con cero costos para la entidad. El método de certificación podrá brindarse de forma virtual o presencial, si se brinda en un lugar diferente a la ciudad de Cajamarca, el proveedor deberá asumir todos los costos que incurran la capacitación, alojamiento, traslado o movilidad, alimentación de los participantes.

Otras capacitaciones

- ✓ El postor deberá diseñar un plan de capacitación adicional para el personal de la UNC (mínimo de 20 personas), el cual deberá ser en idioma español; netamente técnico en el uso configuración y administración de los equipos y aplicaciones que forman parte de la solución, seguridad perimetral gestionada, optimización de aplicaciones parte de la solución ofertada con un mínimo de 40 horas. La capacitación se realizará en los 30 primeros días posteriores a la activación del servicio. El temario será coordinado con la Oficina de Tecnologías de Información.
- ✓ Las capacitaciones podrán ser presenciales o virtuales.
- ✓ El instructor deberá ser certificado en la solución de la marca de los equipos adquiridos.⁴⁰
- ✓ La fecha de inicio y horario de la capacitación será coordinada entre el área usuaria y la empresa ejecutora.
- ✓ Se debe entregar certificado de participación, indicando en el certificado el nombre completo del participante, nombre del curso de la solución ofertada, las fechas en las que se realizó la capacitación, además del número de horas.
- ✓ Se deberá entregar el material en digital, y opcionalmente en físico.
- ✓ En el caso que el curso se dicte de manera presencial en un lugar diferente a las instalaciones de la UNC, el postor deberá incluir todos los gastos de transporte, alojamiento y alimentación.

13. PLAZO DE ENTREGA E INSTALACIÓN

El plazo máximo para la entrega del servicio de acceso a internet con su respectivo equipamiento (router, seguridad perimetral, optimizador de ancho de banda, otros)

⁴⁰ En respuesta a la consulta 168



es ciento veinte (120) días calendarios contados a partir del día siguiente de la firma del contrato.

14. PLAZO DE EJECUCION DEL SERVICIO

El plazo del servicio de Internet será de 24 meses, contados a partir de la fecha de activación solicitada por parte de la entidad. La fecha de activación será posterior a la suscripción del acta de conformidad de la implementación o instalación de servicio.⁴¹

15. CONFORMIDAD

La Conformidad de la solución instalada será emitida por la Oficina de Tecnologías de la Información.

16. LUGAR DE ENTREGA:

La solución será instalada y configurada en concordancia a la Tabla 2. Ubicación de Gabinetes de Comunicaciones:

- ✓ En los ambientes del Centro de Datos de la Universidad Nacional de Cajamarca: Ambiente 1B-201 Ciudad Universitaria; Av. Atahualpa Nro. 1050 – Carretera Baños del Inca - Cajamarca.
- ✓ En filiales en el campus de cada filial de la Universidad.
- ✓ En locales de la UNC correspondientes al centro de idiomas y CEPUNC.

17. CONFIDENCIALIDAD

El proveedor debe guardar absoluta reserva de la información privilegiada que conociera en el ejercicio de las labores o actividad funcional; no revelando ni en forma oral, ni escrita, ni por cualquier otro medio, hechos, datos, procedimientos y documentación de acceso restringido (secreta, reservada y/o confidencial), incluso aún después de culminar el servicio materia del presente proceso.

18. SISTEMA DE CONTRATACIÓN

Suma alzada.⁴²

19. FORMA DE PAGO

El pago se efectuará en soles de manera mensual previa informe de conformidad otorgada por la Oficina de Tecnologías de Información, se realizará de acuerdo al monto de la propuesta económica del postor adjudicado con la presentación del comprobante de pago⁴³. La documentación podrá ser presentada en la mesa de partes de la UNC sito en Av. Atahualpa 1050 (Ciudad Universitaria) en horario de

⁴¹ En respuesta a la observación 112, 363, consulta 11, 173, 250

⁴² En respuesta a la observación 364, consulta 137

⁴³ En respuesta a la consulta 130



07:00 am a 2:45 pm o en los siguientes correos en forma electrónica: oficinainformatica@unc.edu.pe y logistica@unc.edu.pe (los documentos pertinentes serán tramitados en horario de oficina)⁴⁴.

20. ENTREGABLES Y DOCUMENTACIÓN

- ✓ Entrega y registro de todos los elementos hardware necesarios.
- ✓ Entrega y registro de todo el elemento software necesarios.
- ✓ Diagrama del Diseño de toda la solución.
- ✓ Topología de Red de la solución.
- ✓ Listado direcciones IPV4 e IPV6.
- ✓ Especificaciones técnicas de los equipos.
- ✓ Manuales de usuario de cada equipo (de ser posible en español).
- ✓ Se entregarán credenciales de acceso a los equipos de seguridad perimetral, optimizador de ancho de banda u otras soluciones implementadas. Al menos 2 usuarios para los diferentes componentes de la solución.⁴⁵
- ✓ Se deberán remitir hasta un plazo máximo de 05 días calendarios luego de realizada la instalación del servicio.⁴⁶
- ✓ Así mismo precisar que con el propósito de tener un panorama cronológico de las actividades a ejecutar se deberá remitir previamente al inicio del proceso de instalación el cronograma de actividad a ejecutar.

21. INFORMES PERIÓDICOS

- ✓ Información de incidencias, detalle de atención de averías (siempre que existan), en un plazo máximo de entrega 03 días calendarios concluido el mes de brindado el servicio al correo: oficinainformatica@unc.edu.pe.⁴⁷
- ✓ Entrega de informes en forma mensual de los servicios gestionados, en un plazo máximo de entrega 03 días calendarios concluido el mes de brindado el servicio al correo: oficinainformatica@unc.edu.pe.⁴⁸

22. PENALIDADES

Si el proveedor incurre en retraso injustificado en la ejecución del presente contrato, la Universidad Nacional de Cajamarca, le aplicará en todos los casos una penalidad por cada día calendario de atraso, hasta por un monto máximo equivalente al diez (10%) del monto contractual.

⁴⁴ En respuesta a la consulta 77, 78

⁴⁵ En respuesta a la consulta 20, 174, 306, 309

⁴⁶ En respuesta a la consulta 109

⁴⁷ En respuesta a la consulta 110

⁴⁸ En respuesta a la consulta 85,86



La penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula.

$$\text{PENALIDAD DIARIA} = \frac{0.10 \times \text{MONTTO}}{F \times \text{PLAZO EN DÍAS}}$$

Donde F tiene los siguientes valores:

. Para plazos menores o iguales a sesenta (60) días, para bienes, servicios en general, consultorías y ejecución de obras: $F = 0.40$

. Para plazos mayores a sesenta (60) días:

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

Tanto el monto como el plazo se refieren, según corresponda, al contrato o ítem que debió ejecutarse o, en caso que estos involucraran obligaciones de ejecución periódica, a la prestación parcial que fuera materia de retraso.

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

Se considera justificado el retraso, cuando el proveedor acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. Esta calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.

Cuando se llegue a cubrir el monto máximo de la Penalidad. La Universidad Nacional de Cajamarca podrá resolver la Orden de Servido parcial o totalmente por incumplimiento mediante la remisión de Carta Simple suscrita por el funcionario de igual o superior nivel de aquel que suscribió la Orden de Servicio.

Otras Penalidades⁴⁹:

La aplicación de otras penalidades, referidas al incumplimiento de las diversas obligaciones a cargo del postor, cuyas consideraciones están definidas en el Artículo 163° del Reglamento de la Ley de Contrataciones y Adquisiciones del Estado.

La entidad al detectar una avería, comunicará al postor la notificación del incidente para realizar las correcciones necesarias, de persistir la avería, se aplicará lo descrito en la siguiente tabla.

⁴⁹ En respuesta a la consulta 231



N°	INFRACCIÓN	FORMULAR DE CÁLCULO	PROCEDIMIENTO
1	Averías parciales o degradación del servicio por un lapso mayor a 48 horas.	$2\% \times M \times D$	INFORME DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
2	Avería Interrupción total del servicio en la sede central por un lapso mayor a 16 horas.	$5\% \times M \times D$	INFORME DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
3	Avería Interrupción total del servicio en filiales o sedes remotas por un lapso mayor a 32 horas.	$3\% \times M \times D$	INFORME DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
4	Avería o interrupción total del servicio de optimización de Ancho de Banda por un lapso mayor a 48 horas.	$3\% \times M \times D$	INFORME DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
5	Avería o interrupción total del servicio (falla de ambos equipos) de seguridad gestionada por un lapso mayor a 48 horas.	$5\% \times M \times D$	INFORME DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

M= Monto mensual

D= Días con avería o interrupción de servicio

Las penalidades antes señaladas se deducirán en pago del mes posterior a ocurrido el incidente.

En caso de caída de 1 enlace y/o equipo de internet, RPV, seguridad, no se considerará para el cálculo de penalidades, dado que se garantiza la continuidad del servicio a través del enlace y/o equipo secundario.



3.2. REQUISITOS DE CALIFICACIÓN⁵⁰

B.3	CALIFICACIONES DEL PERSONAL CLAVE
B.3.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>Jefe de Proyecto: Ingeniero titulado en Electrónica y/o Sistemas y/o Telecomunicaciones y/o Redes y Telecomunicaciones y/o Informática con especialización en Redes y Comunicaciones. Con habilitación y colegiatura vigente.⁵¹</p> <p><u>Acreditación:</u></p> <p>El Título Profesional será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: http://www.titulosinstitutos.pe/, según corresponda.</p> <p>En caso el 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.</p>
B.3.2	CAPACITACIÓN
	<p><u>Requisitos:</u></p> <p>Con Certificación "ITIL Foundation Certificate in IT Service Management" o Certificación PMP(Project Management Professional).</p> <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de la certificación y/o constancia de certificación.</p>
B.4	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>2 años en implementación y/o instalación y/o configuración de: Redes de Comunicaciones y/o Redes de Datos y/o Implementación de Comunicaciones en Datacenter y/o Fibra óptica y/o Comunicaciones Unificadas y/o Telefonía IP y/o Soluciones de Seguridad Perimetral y/o Administrador de Ancho de Banda y/o Soluciones de Ciberseguridad y/o Red Privadas Virtuales del personal clave requerido como Jefe de Proyecto.⁵²</p> <p><u>De presentarse experiencia ejecutada paralelamente (trasape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el período traslapado.</u></p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente, demuestre la experiencia del personal propuesto.</p> <p>Importante</p> <ul style="list-style-type: none"> 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.

⁵⁰ En respuesta a la consulta 226

⁵¹ En respuesta a la observación 356, consulta 88

⁵² En respuesta a la consulta 90, 138



	<ul style="list-style-type: none"> Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas. Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.
C	<p>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</p> <p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 3 500,000.00 (tres millones quinientos mil con 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran servicios similares a los siguientes: servicio de internet para instituciones o empresas y/o seguridad perimetral y/o optimizador de ancho de banda y/o instalación de servicio de internet mediante fibra óptica y/o interconexión mediante fibra óptica y/o comunicación mediante fibra óptica y/o servicios de interconexión de datos con fibra óptica y/o servicios de telecomunicaciones con fibra óptica.¹³</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 pago¹⁴, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <p>En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p>

¹³ En respuesta a la observación 354, consulta 91, 139, 228, 229, 272

¹⁴ 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 fehacencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"

()

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

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

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

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

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

Importante

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

Importante

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



Importante

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

**CAPÍTULO IV
FACTORES DE EVALUACIÓN**

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

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

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
<u>Evaluación:</u> Se evaluará considerando el precio ofertado por el postor. <u>Acreditación:</u> Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).	La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $P_i = \frac{O_m \times PMP}{O_i}$ 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 [88] puntos

Importante para la Entidad

De conformidad con el artículo 51 del Reglamento, adicionalmente, se **pueden** consignar los siguientes factores de evaluación, según corresponda a la naturaleza y características del objeto del procedimiento, su finalidad y a la necesidad de la Entidad:

Esta nota deberá ser eliminada una vez culminada la elaboración de las bases, así como los factores de evaluación que no se incluyan.

C.	
E. INTEGRIDAD EN LA CONTRATACIÓN PÚBLICA	
<u>Evaluación:</u> Se evaluará que el postor cuente con certificación del sistema de gestión antisoborno <u>Acreditación:</u> Copia simple del certificado que acredita que se ha implementado un sistema de gestión antisoborno acorde con la norma ISO 37001:2016 o con la Norma Técnica Peruana equivalente (NTP-ISO 37001:2017). El certificado debe haber sido emitido por un Organismo de Certificación acreditado para dicho sistema de gestión, ya sea ante el INACAL (antes INDECOPI) u otro organismo acreditador que cuente con reconocimiento internacional. ¹¹ El referido certificado debe corresponder a la sede, filial u oficina	(Máximo 2 puntos) Presenta Certificado ISO 37001 [2] puntos No presenta Certificado ISO 37001 0 puntos

¹¹ Sea firmante/signatario del Acuerdo de Reconocimiento Mutuo (MLA) del International Accreditation Forum-IAF (<http://www.iaf.nu>) o del InterAmerican Accreditation Cooperation-IAAC (<http://www.iaac.org.mx>) o del European co-operation for Accreditation-EA (<http://www.european-accreditation.org/>) o del Pacific Accreditation Cooperation-PAC (<http://www.apec-pac.org/>).

<p>a cargo de la prestación¹², y estar vigente¹³ a la fecha de presentación de ofertas.</p> <p>En caso que el postor se presente en consorcio, cada uno de sus integrantes, debe acreditar que cuenta con la certificación para obtener el puntaje.</p>	
<p>H. MEJORAS A LOS TÉRMINOS DE REFERENCIA</p>	
<p><u>Evaluación:</u> Mejora 1 SERVICIO DE RESPALDO EN NUBE <u>Evaluación:</u> Se evaluará la sostenibilidad operativa del centro de datos donde se brindará el servicio de respaldo en nube. <u>Acreditación:</u> Copia Simple de certificado o carta o cualquier otro documento emitido por el UP TIME INSTITUTE que acredite que el Centro de Datos del postor desde donde brindará el servicio de respaldo en nube cuenta con certificación en Sostenibilidad Operativa.</p> <p>Mejora 1 SERVICIO DE SISTEMA DE SEGURIDAD (APTs) Con el fin de garantizar la seguridad contra amenazas persistentes avanzadas (APTs) y malware en general que es capaz de evadir las defensas de seguridad convencional, se realizara un servicio de escaneo de amenazas persistentes con el fin de detectar, analizar, adaptar y responder a amenazas especializadas y de permitir proactivamente una administración en tiempo real. Asimismo, esta herramienta deberá cumplir las siguientes características mínimas:</p> <ul style="list-style-type: none"> • La solución deberá de ser un appliance dedicado, nuevo, de primer uso y de tecnología vigente de parte de la marca a proponer, por lo cual no deberá estar en estado End-Of-Life o End-Of-Support o End-Of-Sale o similares durante todo el tiempo de la contratación. • Deberá de soportar como mínimo 1Gb de throughput. • Debe utilizar motores de detección especializados, reglas de correlación y aislamiento personalizado para detectar todos los aspectos de un ataque dirigido, no solo de malware. • Debe tener una lista de vigilancia que ayude a proteger a los dispositivos de mayor riesgo en la red • Ser capaz de analizar más de 105 protocolos de red (HTTP, SMTP, POP3, FTP, IRC, etc) que ayude a identificar cualquier medio de infección • Debe tener una consola de información en tiempo real que permita dar visibilidad en cualquier momento, con la posibilidad de visualizar información de mínimo 12 meses.¹⁴ • La solución debe permitir hacer sandboxing para poder reflejar un entorno específico del lado usuario. • Deberá de poder soportar como mínimo 2 sistemas operativos en un entorno controlado, la solución debe soportar como mínimo Windows y Linux; y mínimo de 2 máquinas virtuales.¹⁵ • La solución de sanboxing debiera de ser personalizable. • La solución de sanboxing deberá de ser local.¹⁶ • Debe ser capaz de detectar tráfico C&C y actividad Backdoor así como no discriminar entre sistemas operativos diferentes. 	<p>(Máximo 10 puntos)</p> <p>Mejora 1 : [1] puntos</p> <p>Mejora 1 : [8] puntos</p>

¹² En el certificado debe estar consignada la dirección exacta de la sede, filial u oficina a cargo de la prestación.

¹³ Se refiere al periodo de vigencia que señala el certificado presentado.

¹⁴ En respuesta a la consulta 348

¹⁵ En respuesta a la consulta 346

¹⁶ En respuesta a la consulta 347

- Debe ser capaz de monitorear aplicaciones no aprobadas dentro de las políticas internas del usuario (P2P, chat en IRC, multimedia, etc).
- Debe ser capaz de detectar movimientos laterales, malware avanzado (de día cero o desconocido), comportamientos de ataques humanos y otros mediante herramientas o motores de detección propietarios.
- Se deberá de entregar como mínimo 02 usuarios para el acceso a la consola de administración de la solución.¹⁷
- Capacidad de gestión de mínimo 80 segmentos de la red de la entidad, para un mínimo de 2000 dispositivos.¹⁸
- El servicio deberá ser compatible a la infraestructura de la entidad y a los componentes que forman parte de la solución a contratar, se deberán incluir todos los componentes, accesorios, u otros para el funcionamiento del servicio, sin generar costo adicional a la entidad.¹⁹

Mejora "2": [2] puntos

Acreditación:

Presentar datasheet de la solución propuesta en inglés o español. En caso alguna especificación técnica no aparezca en el datasheet, se podrá presentar adicionalmente una carta emitida por el partner local confirmando el cumplimiento.²⁰

Mejora 2

SISTEMA O PLATAFORMA DE ANÁLISIS DE VULNERABILIDADES.²¹

Brindar un sistema o plataforma de escaneo de vulnerabilidades con el objetivo de mejorar las políticas de seguridad de la entidad.

La solución deberá tener las siguientes características:

- Capacidad de escaneo para todas las IP's públicas (ipv4 e ipv6) ofrecidas en los términos de referencia.²²
- Capacidad de escaneo de mínimo 80 segmentos de la red de la entidad, para un mínimo de 2000 dispositivos.²³
- Deberá permitir crear mapeos de la red.
- Deberá permitir escanear las vulnerabilidades en la red.
- Permitir generar reportes de mapeo y escaneo, y estos puedan ser exportados en PDF o CVS.²⁴
- Deberá de enviar un email de alerta con un sumario del número de nuevas vulnerabilidades detectadas.
- Deberá poder clasificar las vulnerabilidades y riesgos en varios niveles de criticidad.
- Deberá poder administrar múltiples usuarios.
- Podrá ser ofrecido como una solución en la nube o mediante la instalación de un appliance en el datacenter de la UNC. El sistema deberá ser compatible a la infraestructura de la entidad y a los componentes que forman parte de la solución a contratar, se deberán incluir todos los componentes, accesorios, u otros para el funcionamiento de este sistema, sin generar costo adicional a la entidad.

Acreditación:

Presentar datasheet de la solución propuesta en inglés o español. En caso alguna especificación técnica no aparezca en el datasheet, se podrá presentar adicionalmente una carta emitida por el partner local

¹⁷ En respuesta a la consulta 343

¹⁸ En respuesta a la consulta 295, 296

¹⁹ En respuesta a la consulta 180,181, 349

²⁰ En respuesta a la consulta 183

²¹ En respuesta a la consulta 299

²² En respuesta a la consulta 185, 281

²³ En respuesta a la consulta 281

²⁴ En respuesta a la consulta 297, 298

confirmando el cumplimiento.²⁵

Importante

- De conformidad con la Opinión N° 144-2016-OSCE/DTN, constituye una mejora, todo aquello que agregue un valor adicional al parámetro mínimo establecido en las especificaciones técnicas o términos de referencia, según corresponda, mejorando su calidad o las condiciones de su entrega o prestación, sin generar un costo adicional a la Entidad.
- En este factor se pueden incluir aspectos referidos a la sostenibilidad ambiental o social, tales como el compromiso de que durante la ejecución del contrato se verifiquen condiciones de igualdad de género o de inclusión laboral de personas con discapacidad; el uso de equipos energéticamente eficientes o con bajo nivel de ruido, radiaciones, vibraciones, emisiones, etcétera; la implementación de medidas de ecoeficiencia; el uso de insumos que tengan sustancias con menor impacto ambiental; la utilización de productos forestales de fuentes certificadas, orgánicos o reciclados, el manejo adecuado de residuos sólidos, entre otros.

PUNTAJE TOTAL

100 puntos²⁶

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.

²⁵ En respuesta a la consulta 186

²⁶ Es la suma de los puntajes de todos los factores de evaluación.

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 PAGO²⁷

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, 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

²⁷ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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 ACCESORIAS²⁸

"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 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

²⁸ 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.

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

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

En el caso que corresponda, consignar lo siguiente:

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

Importante

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

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

Importante

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

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

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

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 CONTROVERSIAS²⁹

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

²⁹ 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).

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 Digitales³⁰.

³⁰ 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° 1-2023-UNC
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 ³¹	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 servicios³²

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.

³¹ 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.

³² 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° 1-2023-UNC

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 ³³		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ³⁴		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ³⁵		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.

³³ 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.

³⁴ Ibidem.

³⁵ Ibidem.

4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios³⁶

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.

³⁶ 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° 1-2023-UNC
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° 1-2023-UNC
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° 1-2023-UNC
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° 1-2023-UNC
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° 1-2023-UNC**

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] [%]³⁷

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]³⁸

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%³⁹

[CONSIGNAR CIUDAD Y FECHA]

³⁷ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

³⁸ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

³⁹ 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° 1-2023-UNC
Presente.-

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

CONCEPTO	PRECIO TOTAL
TOTAL	

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

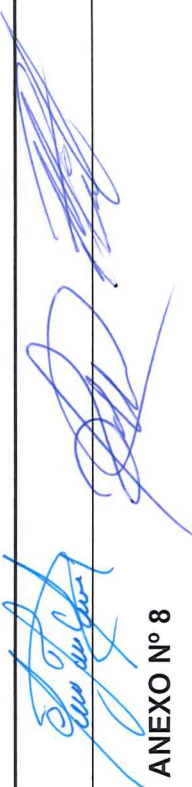
[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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



ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 1-2023-UNC
Presente.-

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ⁴⁰	FECHA DE LA CONFORMIDAD DE SER EL CASO ⁴¹	EXPERIENCIA PROVENIENTE ⁴² DE:	MONEDA	IMPORTE ⁴³	TIPO DE CAMBIO VENTA ⁴⁴	MONTO FACTURADO ACUMULADO ⁴⁵
1										
2										
3										
4										

⁴⁰ 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.

⁴¹ Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho período.

⁴² 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".

⁴³ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

⁴⁴ 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.

⁴⁵ Consignar en la moneda establecida en las bases.

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP 40	FECHA DE LA CONFORMIDAD DE SER EL CASO 41	EXPERIENCIA PROVENIENTE 42 DE:	MONEDA	IMPORTE 43	TIPO DE CAMBIO VENTA 44	MONTO FACTURADO ACUMULADO 45
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° 1-2023-UNC
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

ANEXO N° 12

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

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 1-2023-UNC
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.