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

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

Firmado digitalmente por MARTINEZ VALENCIA Robinson Jean FAU 20537630222 soft
Motivo: Soy el autor del documento
Fecha: 21.04.2025 18:24:28 -05:00

FIRMA DIGITAL

Firmado digitalmente por: OLORTEGUI PEREZ ERWIN ELIAS FIR 70019474 hard
Motivo: Soy el autor del documento
Fecha: 21/04/2025 20:44:06-0500

***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 | **Importante**<br>• *Abc* | Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores. |
| 4 | *Advertencia*<br>• *Abc* | Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores. |
| 5 | **Importante para la Entidad**<br>• *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<br>Izquierda: 2.5 cm Derecha: 2.5 cm |
| 2 | Fuente | Arial |
| 3 | Estilo de Fuente | Normal: Para el contenido en general<br>Cursiva: Para el encabezado y pie de página<br>Para las Consideraciones importantes (Ítem 3 del cuadro anterior) |
| 4 | Color de Fuente | Automático: Para el contenido en general<br>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<br>11 : Para el nombre de los Capítulos.<br>10 : Para el cuerpo del documento en general<br>9 : Para el encabezado y pie de página<br>Para el contenido de los cuadros, pudiendo variar, según la necesidad<br>8 : Para las Notas al pie |
| 6 | Alineación | Justificada: Para el contenido en general y notas al pie.<br>Centrada : Para la primera página, los títulos de las Secciones y nombres de los Capítulos) |
| 7 | Interlineado | Sencillo |
| 8 | Espaciado | Anterior : 0<br>Posterior : 0 |
| 9 | Subrayado | Para los nombres de las Secciones y para resaltar o hacer hincapié en algún concepto |

***INSTRUCCIONES DE USO:***

1. *Una vez registrada la información solicitada dentro de los corchetes sombreados en gris, el texto deberá quedar en letra tamaño 10, con estilo normal, sin formato de negrita y sin sombrear.*

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

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

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

## CONCURSO PÚBLICO Nº 005-2025/MC

## PRIMERA CONVOCATORIA

## CONTRATACIÓN DEL SERVICIO DE ACCESO A INTERNET, SEGURIDAD PERIMETRAL GESTIONADA, TELEFONÍA E INTERCONEXIÒN DE DATOS

# DEBER DE COLABORACIÓN

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

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

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

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

# SECCIÓN GENERAL

# DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

# CAPÍTULO I
# ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

## 1.1. REFERENCIAS

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

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

## 1.2. CONVOCATORIA

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

## 1.3. REGISTRO DE PARTICIPANTES

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

**Importante**

- *Para registrarse como participante en un procedimiento de selección convocado por las Entidades del Estado Peruano, es necesario que los proveedores cuenten con inscripción vigente y estar habilitados ante el Registro Nacional de Proveedores (RNP) que administra el Organismo Supervisor de las Contrataciones del Estado (OSCE). Para obtener mayor información, se puede ingresar a la siguiente dirección electrónica: www.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.*

## 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 Nº 27269, Ley de Firmas y Certificados Digitales[1]). 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*

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

*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 accesoria, 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:*<br><br>*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).*<br><br>*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.*<br><br>*3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.*<br><br>*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.*<br><br>*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.*<br><br>*De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza).*<br><br>*Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.* |

### 3.4. EJECUCIÓN DE GARANTÍAS

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

### 3.5. ADELANTOS

La Entidad puede entregar adelantos directos al contratista, los que en ningún caso exceden en conjunto del treinta por ciento (30%) del monto del contrato original, siempre que ello haya sido previsto en la sección específica de las bases.

### 3.6. PENALIDADES

### 3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

### 3.6.2. OTRAS PENALIDADES

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

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

## 3.7. INCUMPLIMIENTO DEL CONTRATO

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

## 3.8. PAGOS

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

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

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

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

***Advertencia***

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

## 3.9. DISPOSICIONES FINALES

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

# SECCIÓN ESPECÍFICA

## CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

# CAPÍTULO I
# GENERALIDADES

## 1.1. ENTIDAD CONVOCANTE

| | | |
|---|---|---|
| Nombre | : | **MINISTERIO DE CULTURA** |
| RUC Nº | : | 20537630222 |
| Domicilio legal | : | Av. Javier Prado Este N° 2465 – San Borja |
| Teléfono: | : | 618 – 9393 Anexo 2401 |
| Correo electrónico: | : | serviciot587@cultura.gob.pe |

## 1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la CONTRATACIÓN DEL SERVICIO DE ACCESO A INTERNET, SEGURIDAD PERIMETRAL GESTIONADA, TELEFONÍA E INTERCONEXIÓN DE DATOS.

## 1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Formato N° 2 - Aprobación de Expediente de Contratación N° 28-2025, de fecha 16 de abril de 2025.

## 1.4. FUENTE DE FINANCIAMIENTO

RECURSOS ORDINARIOS

**Importante**

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

## 1.5. SISTEMA DE CONTRATACIÓN

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

## 1.6. DISTRIBUCIÓN DE LA BUENA PRO

NO CORRESPONDE

## 1.7. ALCANCES DEL REQUERIMIENTO

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

## 1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

Los servicios materia de la presente convocatoria se prestarán en el plazo de 1,096 (Mil noventa seis días calendario) lo que equivale a treinta y seis (36) meses y deberá iniciar el 08 de agosto del 2025 y luego de suscrita el Acta de Implementación del servicio por parte del contratista y el área usuaria que es la Oficina General de Estadísticas y Tecnologías de Información y Comunicaciones OGETIC, en concordancia con lo establecido en el expediente de contratación.

## 1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar la suma de S/ 6.80 (Seis con 80/100 soles) en la ventanilla de caja de la Oficina de Tesorería, ubicada en el primer piso de la Sede Central del Ministerio de Cultura, sito en la Av. Javier Prado Este N.° 2465 – San Borja – Lima. Luego podrán recoger lo solicitado en la Oficina de Abastecimiento (piso 3 del mismo edificio).

**Importante**

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

## 1.10. BASE LEGAL

- Ley Nº 32185 de Ley de Presupuesto del Sector Público para el Año Fiscal 2025.
- Ley de 32 186 de Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2025.
- Decreto Supremo N° 082-2019-EF – Texto Único Ordenado de la Ley N° 30225, Ley de Contrataciones del Estado, y su Reglamento.
- Ley N.° 30225 – Ley de Contrataciones del Estado.
- Decreto Supremo Nº 344-2018-EF, Reglamento de la Ley de Contrataciones del Estado.
- Decreto Supremo N° 004-2019-JUS – Texto Único Ordenado de la Ley N° 27444 – Ley del Procedimiento Administrativo General.
- Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública, aprobado por Decreto Supremo N° 043-2003-PCM.
- Ley N ° 29783 - Ley de Seguridad y Salud en el Trabajo.
- Código Civil y normas Concordantes.
- Directivas y Opiniones del OSCE.
- Cualquier otra disposición legal vigente que permita desarrollar el objeto de la convocatoria, que no contravenga lo regulado por la Ley de Contrataciones del Estado.

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

# CAPÍTULO II
# DEL PROCEDIMIENTO DE SELECCIÓN

## 2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

**Importante**

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

## 2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos[2], 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 Nº 1)**

b) Documento que acredite la representación de quien suscribe la oferta.

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

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

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

**Advertencia**

*De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE[3] 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 Nº 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 Nº 3**)

e) Declaración jurada de plazo de prestación del servicio. **(Anexo Nº 4)**[4]

---

[2] La omisión del índice no determina la no admisión de la oferta.

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

[4] En caso de considerar como factor de evaluación la mejora del plazo de prestación del servicio, el plazo ofertado en dicho anexo servirá también para acreditar este factor.

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.

**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.

### 2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

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

**Advertencia**

*De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE[5] 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 d) y e).*

f) Domicilio para efectos de la notificación durante la ejecución del contrato.
g) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación [6] (**Anexo N° 12**).
h) Detalle de los precios unitarios del precio ofertado[7].
i) Descripción de la solución o equipamiento asociado a esta solución (Se refiere a que el postor ganador de la buena pro deberá presentar un gráfico con la arquitectura de la solución señalando las marcas y modelos de la solución ofertada).
j) carta del fabricante y/o link impreso de los módulos de seguridad, como mínimo estos: Control

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

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

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

de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs y/o el módulo dentro de la plataforma de NGFW.

k) Link público del fabricante que verifique que los modelos propuestos no están listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support.

l) 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.

Dicha herramienta mínimamente deberá contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs. Se requiere que incluya documentación pública sobre dicha herramienta explicando su alcance, la cual hace referencia a la documentación técnica pública de la marca donde se evidencia el cumplimiento de los requerimientos técnicos solicitados para el presente proyecto.
Se precisa que, los puntos que no puedan sustentarse con información pública, pueden ser sustentados con carta del fabricante y/o link impreso de los módulos de seguridad, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs.

## 2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en Mesa de Partes del Ministerio de Cultura, sito en el primer piso del edificio ubicado en Av. Javier Prado N.° 2465 – San Borja, o por medio virtual el Ministerio de Cultura pone a disposición su Plataforma Virtual de Atención a la Ciudadanía (dar clic aqui http://Plataformamincul.cultura.gob.pe/accesovirtual), la cual está habilitada las veinticuatro (24) horas del día, los (7) días de la semana. Los documentos presentados entre las 00:00 horas y las 23:59 horas de un día hábil, se considerarán como presentados el mismo día hábil. Los documentos presentados los sábados, domingos y feriados, o cualquier otro día inhábil, se considerarán presentados al primer día hábil siguiente.

## 2.5. FORMA DE PAGO

El MINISTERIO se obliga a pagar la contraprestación a EL CONTRATISTA en soles, de manera mensual y en partes iguales a la presentación de la factura respectiva y previa conformidad por parte de la Oficina General de Estadísticas y Tecnologías de Información y Comunicaciones OGETIC, de acuerdo con los plazos establecidos en la Ley de Contrataciones del Estado y, 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. Asimismo, debemos precisar que se podrá hacer un prorrateo en caso la fecha de inicio no coincida con el ciclo de facturación asignado, solo para el primer pago.

Se aceptará el ciclo de facturación que le asigne el postor ganador de la Buena Pro.

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

- Informe mensual del funcionario responsable del Oficina de General de Estadísticas y Tecnologías de la Información y Comunicaciones (OGETIC) previo informe de la Oficina Informática y Telecomunicaciones (OIT).
- Comprobante de pago mensual.

Dicha documentación se debe presentar en Mesa de Partes del Ministerio de Cultura, sito en el primer piso del edificio ubicado en Av. Javier Prado N.° 2465 – San Borja, o por medio virtual el Ministerio de Cultura pone a disposición su Plataforma Virtual de Atención a la Ciudadanía (dar clic aqui http://Plataformamincul.cultura.gob.pe/accesovirtual), donde usted podrá:

1. Ingresar su solicitud/comunicación (icono Ingreso de Documentos).
2. Recibir la respuesta a su solicitud/comunicación de manera inmediata, con alertas a su correo electrónico y número de celular, en tiempo real, previa creación de su Casilla Electrónica.
3. Conocer en tiempo real el estado de su expediente.

# 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

**SE ADJUNTA LOS TERMINOS DE REFERENCIA EN LA PARTE FINAL DE LAS BASES DE CONVOCATORIA**

## 3.2. REQUISITOS DE CALIFICACIÓN

| | |
|---|---|
| **A** | **CAPACIDAD LEGAL** |
| | **HABILITACIÓN** |
| | Requisitos:<br><br>Requisitos: Autorización vigente otorgada por el Ministerio de Transportes y Comunicaciones (MTC) para proporcionar los servicios requeridos.<br><br>**Importante**<br>*De conformidad con la Opinión N° 186-2016/DTN, la habilitación de un postor, está relacionada con cierta atribución con la cual debe contar el proveedor para poder llevar a cabo la actividad materia de contratación, este es el caso de las actividades reguladas por normas en las cuales se establecen determinados requisitos que las empresas deben cumplir a efectos de estar habilitadas para la ejecución de determinado servicio o estar autorizadas para la comercialización de ciertos bienes en el mercado.*<br><br>Acreditación:<br><br>Copia simple del documento que acredite la autorización solicitada o la publicación realizada por la autoridad competente en el Diario Oficial El Peruano, donde se indique y/o autorice que puede brindar los servicios requeridos, y/o copia simple del Certificado de Registro de Empresas Prestadoras de Servicios de Valor Añadido emitido por el Ministerio de Transporte y Comunicaciones y/u oficio del MTC con las concesiones vigentes y/o la impresión de la página web del MTC donde se visualiza las concesiones vigentes del operador y/o la publicación en el diario oficial El Peruano del otorgamiento de la concesión a favor del participante.<br><br>**Importante**<br>*En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito.* |

| | |
|---|---|
| **B** | **CAPACIDAD TÉCNICA Y PROFESIONAL** |
| **B.2** | **INFRAESTRUCTURA ESTRATÉGICA** |
| | Requisitos:<br><br>Contar con un Centro de Gestión y Control necesaria para la atención y solución de averías de los servicios solicitados, servicio de internet, servicio de líneas de telefonía, servicio de seguridad perimetral gestionada y servicio de interconexión de datos con los Museos y las DDC, se precisa que el postor deba contar con un NOC y/o SOC (propio o tercerizado) para la gestión, monitoreo y soporte en modo 24x7 para las soluciones requeridas.<br><br>Se precisa que, la infraestructura estratégica requerida es un Centro de Gestión y Control necesario para la atención y solución de averías de los servicios materia del procedimiento.<br><br>Una licencia de funcionamiento se considerará documento validado en tanto permita acreditar la disponibilidad de la infraestructura para los fines requeridos (Centro de Gestión y control para atención y solución de averías.<br><br>Se precisa que, para cumplir con dicho requisito se requiere que el contratista cuente con un NOC y SOC (propio o tercerizado) para la gestión, monitoreo y soporte en modo 24x7 para las soluciones requeridas, sin embargo, para la acreditación del cumplimiento de dicho requisito, se requiere que el postor acredite contar con un NOC y/o SOC (propio o tercerizado) para la gestión, monitoreo y soporte en modo 24x7 para las soluciones requeridas.<br><br>Acreditación: |

| | |
|---|---|
| | Copia de documentos que sustenten la propiedad, la posesión, el compromiso de compra venta o alquiler u otro documento que acredite la disponibilidad de la infraestructura estratégica requerida.<br><br>**Importante**<br><br>*En el caso que el postor sea un consorcio los documentos de acreditación de este requisito pueden estar a nombre del consorcio o de uno de sus integrantes.* |
| **B.3** | **CALIFICACIONES DEL PERSONAL CLAVE** |
| **B.3.1** | **FORMACIÓN ACADÉMICA** |
| | Requisitos:<br><br>• Jefe de Proyecto del Servicio (01): Título profesional en Ingeniería Electrónica y/o Ingeniería de Sistemas y/o Ingeniería de Redes y/o Telecomunicaciones.<br>• Especialista en Acceso a Internet e Interconexión de datos (01): Bachiller o Ingeniero titulado Electrónica y/o Sistemas y/o Redes y/o Telecomunicaciones.<br>• Especialista Seguridad perimetral (01): Técnico o Bachiller o Ingeniero titulado en Electrónica, Eléctrica, Sistemas, Telecomunicaciones, Redes y/o Comunicaciones y/o Computación e Informática y/o Informático.<br><br>Acreditación:<br><br>El GRADO DE BACHILLER O TÍTULO PROFESIONAL REQUERIDO será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: 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.<br><br>En caso EL GRADO DE BACHILLER O TÍTULO PROFESIONAL REQUERIDO no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida. |
| **B.4** | **EXPERIENCIA DEL PERSONAL CLAVE** |
| | Requisitos:<br><br>• **Jefe de Proyecto del Servicio**: Experiencia mínima de tres (03) años en implementación de servicios y/o trabajos de instalación y/o mantenimiento de internet y/o red privada VPN y/o telefonía fija y/o gestionar y/o supervisar y/o liderar la implementación de proyectos de telecomunicaciones (acceso a internet y/o transmisión de datos y/o telefonía fija) y/o liderar la implementación de Proyectos de Servicios Fijos Corporativos (transmisión de datos, Internet, Comunicaciones Unificadas y Telefonía) e infraestructura de data Center.<br>• **Especialista en Acceso a Internet e Interconexión de datos**: Experiencia mínima de dos (02) años en implementación de servicios y/o trabajos de instalación y/o mantenimiento de internet y/o red privada VPN.<br>• **Especialista Seguridad perimetral (01):** Experiencia mínima de dos (02) años en implementación de servicios y/o trabajos de instalación y/o configuración de equipos de seguridad perimetral.<br><br>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.<br><br>Acreditación:<br><br>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.<br><br>**Importante** |

| | |
|---|---|
| | • *Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el dia, 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.*<br><br>• *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.*<br><br>• *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*<br><br>• *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** | **EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD** |
| | Requisitos:<br><br>El postor debe acreditar un monto facturado acumulado equivalente a 4,500,000.00 (Cuatro 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.<br><br>Se consideran servicios similares a los siguientes: Servicios de Internet y Seguridad fijo y/o servicio internet Móvil y/o servicio de transmisión de datos y/o servicio de seguridad perimetral y/o servicio de transmisión de voz y datos y/o red de enlace de datos entre sedes y/o servicio de línea de contingencia para transmisión de datos y/o enlace dedicado de acceso a internet y/o línea de contingencia para transmisión de datos y/o servicio de internet dedicado y/o servicio de transmisión de voz y datos y/o servicio de interconexión de voz y datos.<br><br>Acreditación:<br><br>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[8], correspondientes a un máximo de veinte (20) contrataciones.<br><br>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.<br><br>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.<br><br>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. |

[8] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado:**

*"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"*
*(...)*
*"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual si se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".*

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

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

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

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

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad.

**Importante**

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

**Importante**

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

## CAPÍTULO IV
## FACTORES DE EVALUACIÓN

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

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

| FACTOR DE EVALUACIÓN | | PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN |
|---|---|---|
| **A.** | **PRECIO** | |
| | Evaluación:<br><br>Se evaluará considerando el precio ofertado por el postor.<br><br>Acreditación:<br><br>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:<br><br>$Pi = \frac{Om \times PMP}{Oi}$<br><br>i = Oferta<br>**Pi** = Puntaje de la oferta a evaluar<br>**Oi** = Precio i<br>**Om** = Precio de la oferta más baja<br>**PMP** = Puntaje máximo del precio<br><br>**100 puntos** |
| **PUNTAJE TOTAL** | | **100 puntos**[9] |

**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.*

[9] Es la suma de los puntajes de todos los factores de evaluación.

## CAPÍTULO V
## PROFORMA DEL CONTRATO

**Importante**

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

Conste por el presente documento, la contratación del servicio de [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], que celebra de una parte [CONSIGNAR EL NOMBRE DE LA ENTIDAD], en adelante LA ENTIDAD, con RUC Nº [.....], con domicilio legal en [.....], representada por [.....], identificado con DNI Nº [.....], y de otra parte [.....], con RUC Nº [.....], con domicilio legal en [.....], inscrita en la Ficha 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 Nº** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO DE SELECCIÓN] para la contratación de [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

**CLÁUSULA SEGUNDA: OBJETO**

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

**CLÁUSULA TERCERA: MONTO CONTRACTUAL**

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

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

**CLÁUSULA CUARTA: DEL PAGO**[10]

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en EL CONTRATISTA en soles, de manera mensual y en partes iguales a la presentación de la factura respectiva y previa conformidad por parte de la Oficina General de Estadísticas y Tecnologías de Información y Comunicaciones OGETIC, de acuerdo con los plazos establecidos en la Ley de Contrataciones del Estado y, 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. Asimismo, debemos precisar que se podrá haber un prorrateo en caso la fecha de inicio no coincida con el ciclo de facturación asignado, solo para el primer pago. Se precisa que, se aceptará el ciclo de facturación que asigne el postor ganador de la Buena Pro.

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

- Informe mensual del funcionario responsable del Oficina de General de Estadísticas y

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

Tecnologías de la Información y Comunicaciones (OGETIC) previo informe de la Oficina Informática y Telecomunicaciones (OIT).

- Comprobante de pago mensual.

Dicha documentación se debe presentar en Mesa de Partes del Ministerio de Cultura, sito en el primer piso del edificio ubicado en Av. Javier Prado N.° 2465 – San Borja, o por medio virtual el Ministerio de Cultura pone a disposición su Plataforma Virtual de Atención a la Ciudadanía (dar clic aquí http://Plataformamincul.cultura.gob.pe/accesovirtual), donde usted podrá, donde usted podrá:

1. Ingresar su solicitud/comunicación (icono Ingreso de Documentos).
2. Recibir la respuesta a su solicitud/comunicación de manera inmediata, con alertas a su correo electrónico y número de celular, en tiempo real, previa creación de su Casilla Electrónica.
3. Conocer en tiempo real el estado de su expediente.

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.

Debemos precisar que se podrá hacer un prorrateo en caso la fecha de inicio no coincida con el ciclo de facturación asignado, solo para el primer pago.

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

El plazo de prestación del servicio será de acuerdo al siguiente detalle:

- **Plazo de Prestación del Servicio**

  El plazo de prestación del servicio deberá ser de 1.096 (Mil noventa seis días calendario) lo que equivale a treinta y seis (36) meses, y deberá iniciar el 08 de agosto del 2025 y luego de suscrita el Acta de implementación del servicio por parte del contratista y el área usuaria que es la Oficina General de Estadísticas y Tecnologías de Información y Comunicaciones – OGETIC.

- **Plazo de Implementación de Servicio**

  El plazo de entrega para realizar la instalación, configuración y puesta en marcha del servicio será de hasta ciento veinte (120) días calendario que se computaran a partir del día siguiente de la suscripción del contrato.

  Se precisa que la Entidad garantizará los accesos y autorizaciones necesarias para la ejecución de los respectivos trabajos de implementación del servicio dentro de sus instalaciones.

  Se precia que la ausencia de facilidades de acceso y/o autorizaciones y/o facilidades técnicas requeridas imputables a la Entidad, determinará la suspensión del plazo de implementación previsto en las bases hasta que se encuentre subsanado el inconveniente, sin generar penalidad alguna al contratista.

Se precisa que el plazo de prestación del servicio será computado desde la fecha de la suscripción del Acta de Activación (Acta de Implementación del servicio) y no desde la fecha del contrato.

**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.

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

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

**CLÁUSULA NOVENA: 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 de la siguiente manera:

- La conformidad del Servicio de Implementación será emitida por la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones, previo informe de la Oficina de Informática y Telecomunicaciones quien verificará el cumplimiento del servicio y el entregable indicado líneas arriba.

- La conformidad mensual del servicio será emitida por la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones previa presentación de la factura del Contratista, así como un informe con el registro de incidencias, requerimientos, eventos del servicio internet, eventos de seguridad en general, clasificándolos en controlados, mitigados y/o aceptados.

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 cumpliese 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 DÉCIMA: 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 UNDÉCIMA: 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 tres años contados a partir de la conformidad otorgada por LA ENTIDAD.

**CLÁUSULA DUODÉCIMA: 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.*

**OTRAS PENALIDADES**

| N.º | Supuestos de aplicación de penalidad | Forma de calculo | Procedimiento |
|---|---|---|---|
| 1 | **Nivel de Disponibilidad:**<br>Sede central: Entre el 99.70% y 99.94%<br>Sedes Remotas: Entre el 99.00% y 99.49% | 5% de la renta mensual del servicio | Según informe de la OGETIC. |
| 2 | **Nivel de Disponibilidad:**<br>Sede central: Menos al 99.70%<br>Sedes Remotas: Menos a 99.00 %. | 10% de la renta mensual | Según informe de la OGETIC. |
| 3 | **Demoras en atención / Soporte Especializado**<br>Mayor a 2 horas | 10% de la renta mensual | Según informe de la OGETIC. |
| 4 | **NO Presentación del informe de Vulnerabilidades** | 10% de la renta mensual | Según informe de la OGETIC. |

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 TERCERA: 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 CUARTA: 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 QUINTA: 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 SEXTA: 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 SÉTIMA: SOLUCIÓN DE CONTROVERSIAS**[11]

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

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

Las partes acuerdan que todo litigio y controversia resultante de este contrato o relativo a éste, se

[11] 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).

resolverá mediante el arbitraje organizado y administrado por la Unidad de Arbitraje del Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú (CARC PUCP), Centro de Arbitraje de la Cámara de Comercio de Lima (CCL) y Centro de Arbitraje de la Cámara de Comercio de Americana del Perú (AMCHM), de conformidad con sus reglamentos vigentes, a los cuales las partes se someten libremente, señalando que el laudo que se emita en el proceso arbitral será inapelable y definitivo.

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 OCTAVA: 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 DÉCIMA NOVENA: 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 Nº 27269, Ley de Firmas y Certificados Digitales*[12].

[12] 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 Nº 1

### DECLARACIÓN JURADA DE DATOS DEL POSTOR

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

El que se suscribe, [.....], postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento Nº [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[13] | | Sí | | No | |
| Correo electrónico : | | | | | |

**Autorización de notificación por correo electrónico:**

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios[14]

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.*

[13] 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.

[14] 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 Nº 1

### DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
**COMITÉ DE SELECCIÓN**
**CONCURSO PÚBLICO Nº** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]
Presente.-

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

| Datos del consorciado 1 | | | | | |
|---|---|---|---|---|---|
| Nombre, Denominación o Razón Social : | | | | | |
| Domicilio Legal : | | | | | |
| RUC : | Teléfono(s) : | | | | |
| MYPE[15] | | Sí | | No | |
| Correo electrónico : | | | | | |

| Datos del consorciado 2 | | | | | |
|---|---|---|---|---|---|
| Nombre, Denominación o Razón Social : | | | | | |
| Domicilio Legal : | | | | | |
| RUC : | Teléfono(s) : | | | | |
| MYPE[16] | | Sí | | No | |
| Correo electrónico : | | | | | |

| Datos del consorciado ... | | | | | |
|---|---|---|---|---|---|
| Nombre, Denominación o Razón Social : | | | | | |
| Domicilio Legal : | | | | | |
| RUC : | Teléfono(s) : | | | | |
| MYPE[17] | | 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.

[15] 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.

[16] Ibídem.

[17] Ibídem.

4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios[18]

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.*

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

## ANEXO Nº 2

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

Señores
**COMITÉ DE SELECCIÓN**
**CONCURSO PÚBLICO Nº** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]
Presente.-

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

i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.

ii. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.

iii. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.

iv. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo Nº 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.

v. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.

vi. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.

vii. Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

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

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

## ANEXO Nº 3

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

Señores
**COMITÉ DE SELECCIÓN**
**CONCURSO PÚBLICO Nº** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

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

## ANEXO Nº 4

### DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
**COMITÉ DE SELECCIÓN**
**CONCURSO PÚBLICO Nº** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

## ANEXO Nº 5

### PROMESA DE CONSORCIO
### (Sólo para el caso en que un consorcio se presente como postor)

Señores
**COMITÉ DE SELECCIÓN**
**CONCURSO PÚBLICO Nº** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]
Presente.-

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

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

a) Integrantes del consorcio

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

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

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

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

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

| | | |
|---|---|---|
| 1. | OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] | [ % ][19] |
| | [DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1] | |
| 2. | OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] | [ % ][20] |
| | [DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2] | |
| | TOTAL OBLIGACIONES | 100%[21] |

[CONSIGNAR CIUDAD Y FECHA]

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

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

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

.....

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

.....

**Consorciado 2**
**Nombres, apellidos y firma del Consorciado 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 Nº 6

### PRECIO DE LA OFERTA

Señores
**COMITÉ DE SELECCIÓN**
**CONCURSO PÚBLICO Nº** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]
Presente.-

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

| CONCEPTO | PRECIO TOTAL |
|---|---|
| | |
| **TOTAL** | |

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

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

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

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

| **Importante para la Entidad** |
| --- |
| *Si durante la fase de actos preparatorios, las Entidades advierten que es posible la participación de proveedores que gozan del beneficio de la exoneración del IGV prevista en la Ley Nº 27037, Ley de Promoción de la Inversión en la Amazonía, incluir el siguiente anexo:* |

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

## ANEXO Nº 7

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

Señores
**COMITÉ DE SELECCIÓN**
**CONCURSO PÚBLICO Nº** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento que gozo del beneficio de la exoneración del IGV previsto en la Ley Nº 27037, Ley de Promoción de la Inversión en la Amazonía, dado que cumplo con las condiciones siguientes:

1.- Que el domicilio fiscal de la empresa[22] se encuentra ubicada en la Amazonía y coincide con el lugar establecido como sede central (donde tiene su administración y lleva su contabilidad);

2.- Que la empresa se encuentra inscrita en las Oficinas Registrales de la Amazonía (exigible en caso de personas jurídicas);

3.- Que, al menos el setenta por ciento (70%) de los activos fijos de la empresa se encuentran en la Amazonía; y

4.- Que la empresa no presta servicios fuera de la Amazonía.

[CONSIGNAR CIUDAD Y FECHA]

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

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

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

## ANEXO N° 8

### EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

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

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

| N° | CLIENTE | OBJETO DEL CONTRATO | N° CONTRATO / O/S / COMPROBANTE DE PAGO | FECHA DEL CONTRATO O CP [23] | FECHA DE LA CONFORMIDAD DE SER EL CASO[24] | EXPERIENCIA PROVENIENTE[25] DE: | MONEDA | IMPORTE[26] | TIPO DE CAMBIO VENTA[27] | MONTO FACTURADO ACUMULADO [28] |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | | | |
| 2 | | | | | | | | | | |
| 3 | | | | | | | | | | |
| 4 | | | | | | | | | | |

[23] Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.

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

[25] Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Al respecto, según la Opinión N° 216-2017/DTN "*Considerando que la sociedad matriz y la sucursal constituyen la misma persona jurídica, la sucursal puede acreditar como suya la experiencia de su matriz*". Del mismo modo, según lo previsto en la Opinión N° 010-2013/DTN, "*... en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad incorporada o absorbida, que se extingue producto de la fusión; asimismo, si en virtud de la escisión se transfiere un bloque patrimonial consistente en una línea de negocio completa, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante podrá emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe*".

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

[27] El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.

[28] Consignar en la moneda establecida en las bases.

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

[CONSIGNAR CIUDAD Y FECHA]

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

## ANEXO Nº 9

## DECLARACIÓN JURADA
## (NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
**COMITÉ DE SELECCIÓN**
**CONCURSO PÚBLICO Nº** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

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

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

**ANEXO N° 12**

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

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

Señores
**COMITÉ DE SELECCIÓN**
**CONCURSO PÚBLICO Nº** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]
Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

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

# TÉRMINOS DE REFERENCIA Nº 0003-2025-OIT-OGETIC-SG/MC

| | |
|---|---|
| **Área Usuaria** | Oficina de Informática y Telecomunicaciones |
| **Meta Presupuestaria:** | 0178 |
| **Actividad del POI:** | Mantenimiento de Infraestructura Tecnológica |

## 1. DENOMINACIÓN DE LA CONTRATACIÓN

**SERVICIO DE ACCESO A INTERNET, SEGURIDAD PERIMETRAL GESTIONADA, TELEFONÍA E INTERCONEXIÓN DE DATOS**

## 2. FINALIDAD PÚBLICA

Los servicios por contratar permitirán el acceso a internet a una velocidad adecuada, seguridad perimetral gestionada, líneas de telefonía y la interconexión de los Museos de Lima y las DDC a nivel nacional con la posibilidad de compartir aplicativos, servicios de red, comunicaciones y soporte: optimizando de esta manera servicios informáticos en beneficio directo de los usuarios y colaboradores de la institución.

## 3. OBJETIVO

El Ministerio de Cultura requiere contratar a una empresa especializada en Telecomunicaciones que le brinde el servicio de enlace dedicado para acceso a internet mediante un enlace simétrico con políticas de priorización de tráfico, servicio de seguridad perimetral gestionada, servicio de líneas de telefonía, servicios de interconexión de datos con los Museos de Lima y las DDC. El servicio se contratará bajo la modalidad de 24 x 7 por un periodo de treinta y seis (36) meses.

## 4. DESCRIPCIÓN DE LOS SERVICIOS REQUERIDOS

| ITEM | UNIDAD MEDIDA | DESCRIPCIÓN DE LOS SERVICIOS |
|---|---|---|
| 01 | Servicio | SERVICIO DE ACCESO A INTERNET, SEGURIDAD PERIMETRAL GESTIONADA, TELEFONÍA E INTERCONOEXIÓN DE DATOS:<br>- SERVICIO DE ACCESO A INTERNET<br>- SERVICIO DE SEGURIDAD PERIMETRAL GESTIONADA<br>- SERVICIO DE LINEAS DE TELEFONÍA<br>- SERVICIO DE INTERCONEXIÓN DE DATOS CON 12 SEDES DE LIMA Y 22 SEDES DE PROVINCIA A NIVEL NACIONAL |

Se solicitarán para la implementación las cartas del fabricante y/o distribuidor autorizado para los routers, firewall, convertir de fibra, gestor de ancho de banda, WAF y otros que se consideren durante la ejecución del servicio, indicando que deberán ser de última generación, nuevos y sin uso y con vigencia tecnológica, las mismas deberán indicar un enlace (link público) que demuestre que no tienen anuncio de "End Of live" ni

Firmado digitalmente por ÑIQUEN CUMPA Jose Carlos FAU 20537630222 soft
Motivo: Doy V° B°
Fecha: 25.02.2025 17:34:37 -05:00

Firmado digitalmente por RAMOS VARGAS Robert Enrique FAU 20537630222 soft
Motivo: Doy V° B°
Fecha: 25.02.2025 17:33:15 -05:00

Firmado digitalmente por MARTINEZ VALENCIA Robinson Jean FAU 20537630222 soft
Motivo: Doy V° B°
Fecha: 25.02.2025 17:29:53 -05:00

Firmado digitalmente por PALACIOS SAMAN Hatemm Omar FAU 20537630222 soft
Motivo: Doy V° B°
Fecha: 25.02.2025 17:25:50 -05:00

"End of Support" podrán ser distintas a las indicadas en los requerimientos técnicos debiendo tener la misma referencia al fin de soporte y fin de vida del equipamiento ofertado.

Para la imputación de responsabilidades por la existencia de daños irreparables de los equipos o defectos de fabricación, el contratista deberá preparar un reporte en el que acredite o descarte los 'defectos de fabricación' o 'daño irreparable' no imputable al Ministerio, siendo que, de comprobarse que el referido daño fue originado por un uso negligente imputable al usuario, será la Entidad quien asuma los costos adicionales por la mencionada contingencia.

Una vez finalizado el plazo contractual, se procederá a la devolución del total de los equipos con un periodo de gracia de 60 días como máximo, luego que le hayan sido entregados y/o instalados bajo cualquier modalidad distinta a la venta (incluyendo routers, switches y/o cualquier otro de propiedad del Contratista) sin más desgaste que el de su uso normal y diligente, en caso de pérdida o robo será asumido el costo de los mismos, cabe señalar que, en caso del deterioro, considerando que los accesorios tienen una vida útil corta, la Entidad no asumirá el costo por estos.

Se deberá considerar una capacitación de mínimo 24hrs, podrá ser no oficial, dentro de los 60 días de la implementación del servicio de cada equipo y servicios involucrados en el presente servicio, podrá ser impartida por el especialista propuesto por el postor, siempre y cuando cuente con la certificación de trainner de la marca ofertada., para un mínimo de 4 personas incluyendo un certificado oficial físico de la capacitación realizada por cada equipo, La capacitación podrá ser de manera remoto y/o presencial previa coordinación con la Entidad.

Se deberán considerar todos los equipos de comunicaciones de alto performance (Switches) necesarios para las conexiones de fibra y/o cobre de los equipos de seguridad, a fin de contar con el óptimo funcionamiento de la solución, para posteriormente realizar las conexiones al equipo Core del Ministerio de Cultura.

La solución de seguridad deberá ser integral y deberá contar con una única plataforma (incluido el licenciamiento de ser necesario) para la reportería y monitoreo de todos los equipos de seguridad, así como la generación de reportes personalizados con un único dashboard intuitivo para la visualización de la solución integral.

### 4.1 SERVICIO DE ACCESO A INTERNET SEDE CENTRAL

Para brindar el servicio de internet la red del Contratista deberá garantizar lo siguiente:

- El backbone de la red local del Contratista deberá ser redundante y se deberá contar con un enlace de contingencia en la salida internacional.
- El Contratista deberá tener disponibilidad de protocolo de IPv4 e IPv6.

- Redundancia en los equipos de enrutamiento de forma automática.
- Redundancia en el Backbone
- Redundancia en los servicios DNS en el mismo local o locales diferentes.
- Redundancia con diferentes operadores en los enlaces de salida internacional hacia internet.

Las características técnicas mínimas del servicio de acceso a internet son:

- En la sede Central del Ministerio de Cultura se tendrá el acceso a internet centralizado, con un ancho de banda de 1000 Mbps.
- La solución deberá soportar un incremento del 30% para el servicio, en caso de requerirse un incremento, se realizará la modificación del contrato, de acuerdo a lo establecido en la Ley de Contrataciones del Estado y su Reglamento.
- La dirección del centro de datos donde se implementará el servicio de Internet es en la Sede Central del Ministerio de Cultura – Quinto piso Av. Javier Prado Este 2465 – San Borja – Lima.
- El medio de transporte para la sede central deberá ser fibra óptica propia, no tercerizada o rentada a terceros, desde la sede Central del Ministerio de Cultura hasta el Nodo IP más próximo del Contratista.
- El servicio del internet deberá tener un enlace principal y un enlace redundante, se precisa que el enlace redundante es un enlace pasivo y que el ancho de banda es de 1000 Mbps, debiendo activar de manera automática en caso de cualquier incidente con el enlace principal.
- El Contratista deberá asegurar que el enlace principal y el enlace redundante tengan recorridos distintos y que ambos salgan de puntos de presencia distintos y nodos de acceso distinto, así mismo en el local de Ministerio de Cultura deberá contar 01 equipo enrutador por cada enlace, ello para asegurar la disponibilidad del servicio de esta sede. Se precisa que los equipos enrutadores deberán ser nuevos, sin uso y de tecnología vigente.
- Se precisa que la última milla para el enlace principal y redundante deberá brindarse a través de fibra óptica en todo su recorrido; el ingreso a la sala de datos de la entidad tanto para la fibra principal y de respaldo podrán ser por un mismo canalizado.
- Se deberá garantizar un overbooking de 1:1 para accesos a los contenidos nacionales e internacionales.
- Se deberá entregar 64 direcciones IPv4 publicas estáticas y 32 direcciones IPv6, escalable con la capacidad de aumentar hasta el doble de acuerdo a los requerimientos de la Entidad y sin costo adicional para el MINCUL, si podrán ser admitidas de un pool distintos y no necesariamente consecutivas; considerar que dentro del pool solicitado se encuentra las IP's de red, broadcast y Gateway a utilizar para poner en marcha la solución.
- El Contratista deberá contar con al menos 1 proveedor TIER 1 con enlaces redundantes cuya capacidad sume 30 Gbps. Se aceptarán dos (02) salidas internacionales distintas de 10Gbps cada uno, para contingencia y redundancia. El Contratista deberá describir su conexión y su llegada hacia el TIER 1.
- El documento será entregado por contratista al día siguiente de

culminada la implementación o al inicio del servicio.

- El contratista deberá asegurar la calidad de la conexión al NAP.
- La red del operador deberá tener implementada en su red (dentro del país) o a través del proveedor internacional de internet una solución de protección DDoS de propósito específico, que deberá proteger y asegurar el tráfico de la Entidad de 1000 Mbps, de manera que el tráfico malicioso sea inspeccionado a través de dicho equipamiento instalado en la red del operador.
- La solución de protección DDoS deberán contar con una protección mínima para la Entidad de al menos de 4Gbps de tráfico malicioso.

## 4.2 SERVICIO DE SEGURIDAD PERIMETRAL GESTIONADA

El Contratista deberá brindar el servicio de seguridad perimetral de la red del Ministerio de Cultura del tipo 24 x 7 durante el tiempo de prestación del servicio.
Las funcionalidades mínimas brindadas en el servicio de seguridad gestionada son:

- Firewall
- Enrutamiento
- VPN IPSEC
- VPN SSL
- IPS
- Prevención de fuga de información (DLP)
- Filtrado de Contenido web (por aplicaciones, URL y categorías WEB)
- Administrador de Ancho de banda
- Antimalware (incluido AntiSpyware y AntiRansonware)
- AntiSpam

Todos los requerimientos indicados hacen referencia al conjunto de soluciones indicados en el Anexo A, que conforman el servicio de seguridad gestionada, es decir 02 equipos de seguridad perimetral, solución cloud de seguridad de correo electrónico, 01 equipo administrador de ancho de banda, 01 equipo de seguridad para aplicaciones WEB y servicio de seguridad de protección avanzada para Endpoints y alguno que se considere a fin de mejorar la seguridad y soportar el tráfico del MINCUL.

La solución deberá incorporar todos los equipos, con las licencias necesarias de ser el caso, para garantizar la seguridad auto gestionada del servicio, así como los equipos necesarios para segmentar el ancho de banda por servicios, sin dejar de considerar los reportes que se necesiten revisar para optimizar la gestión. Es importante que el dimensionamiento a realizar sea acorde a los 1000 Mbps de acceso a internet a contratar y la cantidad de enlaces a conectar. Los equipos deben estar instalados en la sede central del Ministerio de Cultura.

**SERVICIO DE MONITOREO DE ENLACES.**
El Contratista deberá incluir en la solución una herramienta web segura (HTTPS) de monitoreo de los enlaces con las siguientes características:

- ✓ Debe incluir el suministro del hardware y software requerido para uso exclusivo de la herramienta de monitoreo, así como también todas las licencias necesarias para su óptimo funcionamiento, el cual debe ser instalado en la Sede Principal del Ministerio o implementado en la nube o en la red del proveedor en territorio nacional (debe monitorear todos los routers que se instalarán como parte del presente servicio). El contratista deberá cumplir con la confidencialidad y respetar la privacidad de información del Ministerio de Cultura.
  En caso de que el software requiera licencias para el acceso a la herramienta web de monitoreo, se solicita que se considere como mínimo dos (02) licencias.
  La herramienta de monitoreo podrá ser brindada desde la nube del contratista siempre y cuando cumpla con las demás características del Servicio de Monitoreo de Enlaces.
- ✓ Debe permitir el monitoreo del desempeño de cada router, debe mostrar en una pantalla resumen: alarmas recientes, disponibilidad, tiempo de respuesta, pérdida de paquetes. Asimismo, deberá presentar gráficas de utilización de CPU, utilización de memoria y/o buffer.
- ✓ Capacidad de visualización de la red usando la integración de Google map o similar, que permita visualizar la localización geográfica de los equipos implementados.
- ✓ Soporte NetFlow (versión 5, 7 y 9), jFlow, sFlow, cFlowd. Soporte NBAR (opcional), IPFlow o NetStream.
- ✓ Tráfico: Presentación del volumen, velocidad, utilización y paquetes, en presentación gráfica de tiempo y permita la generación del Informe de Planificación de Capacidad, así mismo se considerará que la solución permita generar informes sobre la información histórica sobre el uso de ancho de banda para que la entidad pueda usar la información como referencia para saber el estado de su enlace. Las mediciones deben actualizarse a 1, 5 o 10 minutos y las cuales deben ser configurables por el usuario.
- ✓ Visibilidad del Consumo de Ancho de Banda diferenciado por tipo de tráfico (mínimo tres Clases de Servicio) para todos los enlaces de datos.
- ✓ Los reportes que se obtengan deben ser en horas, diarios, semanales y mensuales, debemos indicar que la herramienta de monitoreo será para los enlaces de internet y los enlaces de datos de todas las sedes de la entidad, referidos al almacenamiento de logs o históricos para la herramienta de monitoreo.
- ✓ La herramienta de Monitoreo podrá tener granularidad no mayor a 5 minutos para la data almacenada en la base de datos que debe ser incluida y para el periodo de al menos seis (06) meses con el objetivo de tener reportes granulares y realizar comparativos mensuales para el sustento y planificación de la capacidad.
- ✓ En caso de ofertar una solución ON PREMISE debe permitir crear diagramas topológicos detallados de la Red en tiempo real, así como guardar el historial de los registros, descubrir como

mínimo, los siguientes tipos de equipos (Router, Switches L2, Switches L3, Firewall, Load Balancers, WAN Optimizer, WAPs).

- ✓ La solución debe recopilar la información de los equipos descubiertos por SNMP capturando como mínimo: Dirección IP, Marca, Modelo y debe permitir exportar esta información del inventario de los equipos descubiertos en un archivo Excel/PDF. Asimismo, debe permitir documentar la información recopilada y deberá exportarla en un archivo PDF.

**SERVICIO DE ANÁLISIS DE VULNERABILIDADES**

- ✓ El proveedor deberá realizar el servicio de Análisis de Vulnerabilidades y Pen Testing externo e interno con una frecuencia semestral y deberá ser realizado dentro de cada semestre.
- ✓ Para brindar este servicio el proveedor deberá contar con sus propias herramientas y licencias de software necesarias.
- ✓ El informe de vulnerabilidades será un requisito indispensable para que se otorguen las conformidades del servicio de internet.
- ✓ El informe deberá contener el tipo de vulnerabilidad, los servicios y/o servidores afectados, evidencias y recomendaciones para la mitigación de la(s) posible(s) vulnerabilidad(es) encontrada(s) como parte del análisis.

<u>Servicio de Vulnerabilidades Externo</u>

- Se deberá hacer un escaneo de red detectando las posibles vulnerabilidades informáticas de hasta setenta (70) aplicaciones de la entidad.
- Se debe incluir el análisis de vulnerabilidades de los servidores que albergan dichas aplicaciones.
- Se deberá entregar un informe después de cada servicio.
- El informe de vulnerabilidades será tanto técnicos como ejecutivos, debiendo ser entregados por separado.
- Se realizará desde la perspectiva de un usuario anónimo en internet, es decir sin privilegios y sin conocer nombres de usuarios o contraseñas.
- Se deberá realizar las siguientes actividades: Reconocimiento, Escaneo de Puertos, Identificación de Servicios Activos (TCP/IP), Identificación de Sistemas Operativos, Identificación de Vulnerabilidades y Verificación y Revisión de Sistemas de Confianza.

<u>Servicio de Vulnerabilidades Interno</u>

- Se deberá identificar y documentar todos los vectores de ataque que permitan una prueba de penetración exitosa, debiendo entregar los informes correspondientes, tanto técnicos como ejecutivos, por separado.
- Las pruebas se realizarán desde la perspectiva de un usuario anónimo en la LAN, es decir sin privilegios y sin conocer nombres de usuarios o contraseñas.
- Se deberá realizar las siguientes actividades: Revisión de la red interna de la OGETIC, Revisión del servidor de BBDD Oracle de la OGETIC, Revisión del servidor de correo

electrónico (MS Exchange Server), Revisión del servidor de directorio activo (Active Directory) y servidor de Aplicación (cira) así como también, los servidores que alojan hasta las setenta (70) aplicaciones indicadas líneas arriba.

**SERVICIO DE CREACIÓN DE DOMINIOS Y SUBDOMINIOS**

- ✓ El contratista deberá crear los dominios de diversos tipos (cname, A, MX, TXT), podrán ser realizados de lunes a viernes en el horario de 8am - 6pm.
- ✓ El Contratista podrá brindar acceso a un portal web para la realizar los cambios de las publicaciones DNS de forma inmediata, sin embargo, el proveedor asegurará la asistencia técnica en el momento en que se requiera.
- ✓ El requerimiento de cambios de publicaciones DNS será realizado a demanda y por el personal técnico de la entidad, mediante coordinaciones con el NOC y/o correo electrónico.

## 4.3 SERVICIO DE LINEAS DE TELEFONÍA

- Se deberá habilitar el servicio de telefónica corporativa para la sede central mediante 01 enlace tipo SIP TRUNK o también se aceptarán 4 primarios tipo E1, para la comunicación con la red de telefonía pública de mínimo 100 canales de voz para llamadas entrantes y salientes desde los anexos de la sede, este enlace deberá ser habilitado y configurado por el Contratista (Actualmente la central cuente con puerto ethernet disponible para recibir la Interconexión SIP y otro puerto LAN que se conecte con la entidad para el uso de sus anexos). Los canales de voz podrán ser usados para llamadas entrantes y salientes al mismo tiempo.
- Deberá brindar una disponibilidad mínima de 99.5% para la troncal SIP
- El enlace del tipo SIP TRUNK y/o SIPv2 deberá ser compatible con la central telefónica de la entidad de marca: DENWA, modelo: Advanced Plus - versión: 3.3.1.20120316 --- Firmware: actualización 099 (La central telefónica del Ministerio cuenta con puerto de red ethernet disponible para recibir la Interconexión SIP y otro puerto LAN para la conexión a la entidad para el uso de sus 800 anexos aproximadamente).
- Las sedes de Lima y Provincia cuentan con anexos telefónicos registrados en la misma Central, así como también una troncal hacia otra Central instalada en el Ministerio.
- Toda configuración que se requiera en la central telefónica estará a cargo de la entidad. Sin embargo, la compatibilidad y funcionalidad en el servicio es compartida.
- El Contratista deberá asignar 50 DID (Direct Inward Dial).
- El recibo físico no deberá incluir los detalles de llamadas por medidas de seguridad y también él envió de recibos podrá ser por medio electrónico a fin de contribuir con la reducción de la huella de carbono.
- El detalle de llamadas del recibo del servicio de telefonía deberá ser entregado en formato digital adjunto al comprobante de pago físico o forma electrónica, conteniendo lo siguiente:

- ✓ En los canales de voz, se debe contemplar como origen el número cabecera (DID).
- ✓ Detalle de duración de las llamadas entrantes y salientes
- ✓ Detalle de origen y destino de llamadas.
- ✓ Detalle de costos de las llamadas realizadas.

- El Contratista deberá entregar de forma mensual el reporte de tráfico de llamadas de enlace de voz y además del consumo de la bolsa de minutos consumido mensualmente. Este reporte deberá ser presentado en formato digital, Excel y/o PDF, en un plazo máximo de quince (15) días calendario, luego de culminado el servicio mensual.
- Respecto a la bolsa de minutos que se requiere, el Contratista deberá considerar dicha bolsa a precio preferencial en forma mensual para el tiempo que dure el contrato.

| Tipo de llamadas | Minutos mensuales |
|---|---|
| Discado Directo Local (Todos los operadores) | 30.000 |
| Discado Directo Nacional (Todos los operadores) | 4.000 |
| Discado Directo Internacional (fijo y móvil) | 500 |
| Discado Celular (Todos los operadores) | 30.000 |

- El consumo de los minutos adicionales establecidos en la bolsa, deberán considerarse con el mismo precio por minuto de la bolsa asignada y deberán ser facturadas en recibos independientes al servicio de telefonía.

- El Contratista deberá ejecutar el servicio de portabilidad numérica sin costo adicional para la entidad, ello con la finalidad de no ver afectada la numeración actual con la que cuenta la entidad (La cabecera PBX principal tendrá configurada la cabecera 16189393 y los demás números se configurarán como DIDs en el cual se incluye los números de la cabecera PBX CIT).

  La entidad toma conocimiento de que la activación del servicio dependerá de la culminación exitosa del trámite de portabilidad numérica.

  La entidad coordinará con el contratista el tiempo de entrega de la documentación requerida para la portabilidad numérica en base a lo establecido a la Ley de Portabilidad Numérica - Ley 28999, asimismo, la entidad es responsable de proporcionar la documentación para realizar la portabilidad numérica de acuerdo a lo establece a la normativa.

  La entidad proporcionará al contratista los siguientes documentos:

  1. Relación de líneas a portar con su respectivo minutos y servicios,
  2. Constancia de no adeudo emitida por su operador actual,

3. Último recibo de su operador actual cancelado a la fecha,
4. Voucher de pago de este último recibo,
5. Formato de Portabilidad firmado.

- El Contratista deberá tener en cuenta que la tarificación y/o facturación deberá realizarse utilizando la unidad de medida de tiempo del minuto con excepción de las llamadas móviles que será al segundo.

## 4.4 SERVICIO DE INTERCONEXIÓN DE DATOS CON LAS 12 SEDES DE LIMA Y 22 SEDES EN PROVINCIAS A NIVEL NACIONAL

- Habilitar los enlaces de interconexión de datos para las doce (12) sedes de Lima y las veintidós (22) sedes en provincia a nivel nacional, con la sede Central para las siguientes direcciones.

  Las coordinaciones técnicas serán realizadas previo a la implementación del equipamiento, por lo cual la entidad dispondrá de personal dedicado a la atención de dicha implementación.

  Asimismo, es necesario contar con una distribución a demanda según la necesidad del MINCUL, a fin de aumentar el ancho de banda de alguna sede, quitando el ancho de banda de otra sede.

**Cuadro: Sedes Lima**

| ITEM | DISTRITO | DIRECCIÓN | DESCRIPCIÓN | MEDIO DE ACCESO | VELOCIDAD GARANTIZADA 100% |
|---|---|---|---|---|---|
| 1 | Ate | Carretera central, km 4.5 | Museo de sitio "Arturo Jiménez Borja" - Puruchuco | Fibra Óptica | 15 Mbps |
| 2 | San Isidro | Nicolas Rivera 201 (esq. Calle Salamanca y Ab. Del Rosario) | Museo de Sitio Huallamarca | Fibra Óptica | 15 Mbps |
| 3 | Lurín | Km. 31 de la Antigua Panamericana Sur | Museo de Sitio de Pachacamac | Fibra Óptica | 20 Mbps |
| 4 | Rímac | Mirador del Cerro San Cristóbal | Museo de Sitio Mirador Cerro San Cristóbal | Fibra Óptica | 10 Mbps |
| 5 | Lima | Paseo de la Republica 250 | Museo del Arte Italiano de Lima | Fibra Óptica | 15 Mbps |
| 6 | Lima | Jr. Washington 1936 - 1946 | Casa Museo Jose Carlos Mariátegui | Fibra Óptica | 15 Mbps |

| ITEM | DISTRITO | DIRECCIÓN | DESCRIPCIÓN | MEDIO DE ACCESO | VELOCIDAD GARANTIZADA 100% |
|---|---|---|---|---|---|
| 7 | Pueblo Libre | Plaza Bolívar s/n (Frente a la Municipalidad) | Museo Nacional de Arqueología Antropología e Historia del Perú | Fibra Óptica | 20 Mbps |
| 8 | Lima | Av. Alfonso Ugarte 650 | Museo de la Cultura Peruana | Fibra Óptica | 15 Mbps |
| 9 | Lima | Jr. Conde de Superunda 169 | Casa de la Gastronomía Peruana | Fibra Óptica | 10 Mbps |
| 10 | Miraflores | Bajada San Martin 151, Miraflores | Lugar de la memoria, la tolerancia y la Inclusión social | Fibra Óptica | 20 Mbps |
| 11 | Pueblo Libre | Entre la cuadra 12 y 13 Av. Mariano Cornejo | Complejo arqueológico "Mateo Salado" | Fibra Óptica | 10 Mbps |
| 12 | Callao | Jr. Salaverry N° 208 Callao | DDC Callao | Fibra Óptica | 15 Mbps |

**Cuadro: Sedes Provincia**

| N° | DIRECCIÓN DESCONCENTRADA DE CULTURA | DOMICILIO DDC | MEDIO DE ACCESO * | VELOCIDAD GARANTIZADA 100% |
|---|---|---|---|---|
| 1 | Amazonas | Jr. Ayacucho N° 908 Plaza Mayor, Chachapoyas, Amazonas | Fibra Óptica | 15 Mbps |
| 2 | Ancash | Av. Luzunaga N° 780 Plaza de Armas, Huaraz, Ancash | Fibra Óptica | 15 Mbps |
| 3 | Ancash – Museo Nacional Chavín | Av. 17 de Enero, Prolongación Norte S/N | Fibra Óptica | 15 Mbps |
| 4 | Apurímac | Jr. Puno 603, 5 PISO, Frente al Gobierno Regional de Apurímac | Fibra Óptica | 15 Mbps |
| 5 | Arequipa | Av. Ramon Castilla N° 745 Cayma, Arequipa | Fibra Óptica | 15 Mbps |
| 6 | Ayacucho | Av. Independencia N° 502. Huamanga, Ayacucho | Fibra Óptica | 15 Mbps |
| 7 | Cajamarca | Jr. Belén N° 631 Conjunto Monumental Belén Cajamarca | Fibra Óptica | 15 Mbps |

| N° | DIRECCIÓN DESCONCENTRADA DE CULTURA | DOMICILIO DDC | MEDIO DE ACCESO * | VELOCIDAD GARANTIZADA 100% |
|---|---|---|---|---|
| 8 | Huancavelica | Jr. 05 de Agosto Lote 49 Manzana L barrio de San Cristóbal-Huancavelica | Fibra Óptica | 15 Mbps |
| 9 | Huánuco | Jiron 28 de julio 1454 | Fibra Óptica | 15 Mbps |
| 10 | Ica | Av. Ayabaca 895 Urb. San Isidro, Ica | Fibra Óptica | 15 Mbps |
| 11 | Junín | Av. Huancavelica 917 el tambo Huancayo, Jr. julio C. Tello con Huancavelica la misma esquina | Fibra Óptica | 15 Mbps |
| 12 | Lambayeque | Av. Luis Gonzales N° 345, Chiclayo Lambayeque | Fibra Óptica | 15 Mbps |
| 13 | Loreto | Malecón Tarapacá N°382 2do Piso Iquitos, Loreto | Fibra Óptica | 15 Mbps |
| 14 | Madre de Dios | Jr. Gonzales Prada N° 222 Tambopata, Madre de Dios. | Fibra Óptica | 15 Mbps |
| 15 | Moquegua | Calle Ayacucho N° 530, Plaza de Armas Moquegua | Fibra Óptica | 15 Mbps |
| 16 | Pasco | Av. 1ro de mayo Mz. A - Lote 22 AA. HH TUPAC AMARU - chaupimarca - Pasco- Pasco | Fibra Óptica | 15 Mbps |
| 17 | Piura | Av. Richard Cushing N° 197 Urb. Club Grau, Piura Cercado, Piura | Fibra Óptica | 15 Mbps |
| 18 | Puno | Jr. Deústua 630, Complejo Cultural "Casa Conde Lemos", Puno | Fibra Óptica | 15 Mbps |
| 19 | San Martin | Jr. Oscar Benavides N° 380, Moyobamba San Martin | Fibra Óptica | 15 Mbps |
| 20 | Tacna | Calle San Martin N° 405, Tacna | Fibra Óptica | 15 Mbps |
| 21 | Tumbes | Calle Jacinto Seminario Mz. 25 Lot 4 Urb. Andrés Araujo Morán, Tumbes | Fibra Óptica | 15 Mbps |
| 22 | Ucayali | Jr. Libertad 218-Calleria | Fibra Óptica | 15 Mbps |

***Se aceptará acceso de Fibra Óptica o inalámbrico, siempre y cuando este sea de banda debidamente licenciada o satelital asegurando el ancho de banda solicitado.***

- Los enlaces de datos deberán ser simétricos 1:1 y deberán garantizar el 100% del ancho de banda requerido.
- Para las sedes de provincia el medio de acceso en caso sea de medio satelital, se deberá garantizar un ancho de banda mínimo del 70% de subida y bajada, pudiendo ser asimétricos.
- El servicio dedicado de datos de la sede central que recibe todas las conexiones de las sedes remotas deberá tener un ancho de banda como mínimo de 510 Mbps y adicionalmente deberá tener un enlace de contingencia de 510 Mbps ambos de fibra óptica. El enlace principal y de contingencia deberá estar en la modalidad "activo/en espera" y deberán de funcionar de manera automática.
  Los routers para el enlace de datos deben ser independientes (principal y contingencia) al enlace de internet, con la finalidad de asegurar la disponibilidad de ambos servicios.
- Para la interconexión de las sedes remotas de difícil acceso o por sus condiciones geográficas, para la conexión del Punto de Presencia (POP) de acceso al backbone, el postor podrá utilizar como transporte enlaces microondas y/o satelitales.
- El backbone del servicio de transmisión de datos para la interconexión de redes desde ser de propiedad del Contratista.
- El backbone del Contratista para el servicio de interconexión de redes debe estar implementado en Fibra Óptica y no debe ser rentado a terceros.
- Los enlaces deberán ser simétricos y dedicados sin utilizar esquemas de acceso compartido o acceso del tipo asimétrico. Estos enlaces deberán disponer de capacidad de crecimiento de ancho de banda para las ampliaciones que desee hacer la entidad.
- El crecimiento de ancho de banda máximo será del 30% del servicio de Internet y de datos.
- El enlace dedicado de la sede Central deberá tener redundancia en acceso y equipo para asegurar la disponibilidad del servicio, para ello se debe contar con un router para el enlace principal y un router para el enlace backup o de contingencia.
- La Entidad puede proporcionar un switch de capa 2 para la conexión de ambos puertos (principal y secundario) en caso de ser necesario.
- Tecnología de transporte Metro Ethernet o MPLS en el Backbone del Contratista para verificar este requerimiento deberá describir la tecnología y topología de la solución a implementar incluyendo las soluciones de equipos y marcas propuestas, la misma que se presentará para la implementación.
- Interface UTP-Ethernet para la conexión con la LAN en la Oficina principal de la entidad.
- El servicio no deberá contener filtros de ninguna clase, con lo cual se asegurará el funcionamiento de cualquier tipo de aplicación o puerto que se ejecute sobre el protocolo TCP/IP.
- El nivel del servicio (SLA) requerido para el servicio de Internet e Interconexión VPN son los siguientes:
  - Sedes en Lima: 99.95% para los servicios de acceso a Internet y red datos en alta disponibilidad (activo – pasivo)
  - Sedes en Provincia: 99.50% para sedes que cuentan con enlace

de datos
- Perdida de paquetes IP: =<1% (Esto aplica únicamente a las interconexiones de datos, no para el Internet).

- El servicio proporcionado debe contar con una herramienta de Gestión para monitoreo según lo descrito líneas arriba en la sección "Servicio de Monitoreo de Enlace".
- Registro DNS de los servicios internet del Ministerio de Cultura.
- El Contratista deberá poseer servidores DNS redundantes y distribuidos en locales distintos.
- Se precisa que los últimos dos puntos mencionados, están referidos al servicio de internet y no al servicio de interconexión de datos.
- La entidad cuenta con al menos dos puertos ethernet disponibles en el Switch LAN de la entidad para la conexión del servicio.
- El contratista únicamente será responsable de entregar el enlace de internet y red privada virtual (rpv) hasta el puerto RJ45 disponible y habilitado en el switch de cada sede donde se llevarán los trabajos, siendo responsabilidad de la Entidad donde está incluido el realizar trabajos de puntos de red, puntos de energía eléctrica y configuración del switch LAN
- El Proveedor deberá dejar el cableado ordenado y etiquetado a fin de mantener el orden de los equipos instalados.
- El Proveedor deberá considerar las regletas eléctricas, bandejas y ordenadores necesarios para la instalación de sus equipos.
- La entidad cuenta con al menos 3 RU (Rack Unit) disponibles en los gabinetes y/o racks, con al menos un punto de energía para la instalación de los equipos.
- Para la sede principal, los accesos de los enlaces deberán ser subterráneas y con ducteria, con la finalidad de asegurar la integridad del recorrido del enlace hasta el Centro de Datos. Para las sedes remotas, el acceso de los enlaces podrá ser por vía aérea y/o ductería.

## 5. CONSIDERACIONES GENERALES PARA LA IMPLEMENTACIÓN

El Contratista realizará la implementación fuera del horario de la oficina de lunes a viernes de 5:00 PM a 7:00 AM, previa coordinación con el área usuaria y la Oficina Informática y Telecomunicaciones. Para el caso de fines de semana (sábado y domingo) o feriados, el Contratista podrá realizar los trabajos en el horario diurno (7:00 AM a 07:00 PM) y nocturnos (7:00 PM a 7:00 AM) de hasta 12 horas, previa coordinación con el área usuaria y la Oficina Informática y Telecomunicaciones.

## 6. CONFIDENCIALIDAD

El Contratista se compromete a mantener en reserva y no revelar a tercero alguno sin autorización previa del Ministerio de Cultura, la información que le sea suministrada por este último.

La obligación de confidencialidad no aplicará a la información que:

- Resulte accesible al público por causa distinta del incumplimiento de la obligación de confidencialidad por la parte receptora.
- Haya sido publicada con anterioridad a la fecha de la firma de contrato.

- Se encuentre en poder de la Parte receptora y no esté sujeta a cualquier otro impedimento o restricción puesto de manifiesto a la otra Parte en el momento de la revelación o luego de ella.
- Sea recibida a través de terceros sin restricciones y sin que implique incumplimiento del Contrato.
- Sea independientemente desarrollada por la Parte receptora, siempre que no se hubiese utilizado para ello la información confidencial proporcionada por la otra Parte.
- Deba ser revelada para dar cumplimiento de una orden de naturaleza judicial o administrativa, en cuyo caso la Parte receptora deberá informar a la otra Parte en forma inmediata a la sola recepción de la citada orden.

Asimismo, la obligación de confidencialidad no resulta aplicables en los siguientes supuestos:

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

## 7. ATENCIÓN DE AVERIAS O FALLAS

- Una avería es una interrupción parcial o total del servicio, así como un decremento en la calidad del mismo. Se aceptarán las siguientes exclusiones propuestas para la calidad de servicio:

  - En situaciones de catástrofe, vandalismo, robos y eventos naturales (terremotos, desplazamientos, lluvias, huaycos) u otros excepcionales como los causados por accidentes en el local como aniego, incendio, derrumbe.
  - Interrupción o degradación del servicio causado por negligencia, error u omisión de cliente. (Manipulación de cables, cambios en configuración de equipos).
  - Interrupción o degradación del servicio causado por falla en los equipos de propiedad y responsabilidad del cliente (Switches LAN, UPS)
  - Falla o suspensión eléctrica en la localidad.
  - En caso no exista facilidades para el transporte (huelgas en carretera, deslizamientos, disponibilidad de medios de transporte,

restricciones gubernamentales, emergencias sanitarias, aislamiento focalizado, inmovilización social, rondas campesinas y/o pobladores que no permitan el ingreso a sus localidades u otro ocasionado por terceros).
- Eventos de avería masiva causada por terceros.

- Las actividades o provisiones de bienes que ejecute el Contratista para subsanar una avería serán sin costo alguno para la entidad a excepción de que la avería sea imputable al Ministerio de Cultura.
- El Contratista deberá contar con un Centro de Operaciones de Red propio a cargo de la atención de los casos referidos a la red.
- El Contratista deberá contar con un SOC certificado en la ISO27001, dicho SOC puede ser propio o tercerizado para las atenciones de todos los casos de seguridad.
- El tiempo de atención de una avería no deberá ser mayor de 30 minutos (el cual hace mención al tiempo de creación del ticket de cualquier solicitud sea seguridad gestionado o del servicio de enlace de Internet y servicio de datos), tiempo transcurrido desde que se reporta la avería hasta que el Contratista responda para iniciar el diagnóstico.

  El tiempo de atención de cualquier tipo de avería será computado a partir de la generación de un ticket de atención, luego de producido el incidente.

- En caso de falla de los equipos de las sedes de Lima el tiempo de solución de la avería o interrupción reportada en cualquiera de los enlaces o cambio temporal por un equipo equivalente o superior, no deberá ser mayor a seis (06) horas después de generado el ticket de atención.
- Cabe señalar que, para en el caso de reemplazo de un equipo equivalente o superior, este será mientras dure el proceso RMA (reparación) con el fabricante y no excederá de sesenta (60) días calendario de diagnosticado la necesidad del cambio de equipo.
- El tiempo de solución de avería o interrupción también debe ser acatado por el servicio de seguridad gestionada, servicio de Internet y datos. El contratista podrá brindar un equipamiento SPARE en caso lo crea necesario para cumplir con los SLA's establecidos.
- En caso de falla de equipos en provincias el tiempo de solución de la avería o interrupción reportada en cualquiera de los enlaces o cambio temporal por un equipo equivalente o superior no deberá ser mayor a veinticuatro (24) horas después de generado el ticket de atención.
- Cabe señalar que, para en el caso de reemplazo de un equipo equivalente o superior, este será mientras dure el proceso RMA (reparación) con el fabricante y no excederá de sesenta (60) días calendario de diagnosticado la necesidad del cambio de equipo.
- Para los casos de degradación de Servicio se brindará cuatro (04) horas contabilizadas después de la entrega del ticket de atención.
- En Lima y provincias, para la subsanación de avería ante factores externos al proveedor (vandalismos, corte de fibra u otras situaciones similares) se brindará 08 horas adicionales para la subsanación a los tiempos indicados en los párrafos anteriores
- Se precisa que el tiempo de solución de la avería o interrupción

reportada está referida a todos los equipos contemplados en el presente servicio.

- El ministerio de cultura reportará las averías a un único número telefónico el cual será una ventanilla única que atenderá todas las averías del servicio contratado, permitiendo un adecuado control, gestión y seguimiento de la misma, debiendo indicar número telefónico. El Contratista deberá contar un número gratuito para la atención de las llamadas el cual deberá ser atendido de manera inmediata y con atención personalizada a fin de dar registro a la avería.
- Todas las incidencias deberán ser registradas y reportadas en los entregables mensuales.
- En caso el contacto de la entidad registrado en el ticket de avería no esté disponible, demore en responder y/o se presenten demoras de permisos de accesos para la atención del incidente y problema por parte de la entidad, este tiempo será considerado como parada de reloj, el cual no será considerado como parte del tiempo de respuesta de acuerdo a los SLA's propuestos. Asimismo, se aplicará la parada de reloj en aquellas sedes donde el horario de atención de las sedes administrativas se encuentre limitado y el contratista no pueda atender la avería por las limitantes de tiempo de atención de algunas sedes de la entidad.
- En caso de averías masivas no imputables al contratista, se aplicará el tratamiento según lo establecido en las normativas de los Servicios Público de Telecomunicaciones relacionadas, sin que ello genere la aplicación de ninguna penalidad, entre ellas la Resolución de Consejo Directivo N° 123-2014-CD/OSIPTEL que aprueba el Reglamento General de Calidad de los Servicios Públicos de Telecomunicaciones.

## 8. SOPORTE ESPECIALIZADO

- El Contratista deberá brindar soporte especializado para los requerimientos e incidentes suscitados en la Entidad, ya sea como cambios de configuración, cambio de políticas de seguridad, buenas prácticas, recomendaciones reportes, entre otros, sobre todos los equipos de seguridad perimetral ofertados, los mismos que serán registrados y presentados en el entregable mensual.
- El Contratista deberá brindar un teléfono directo con la persona especializada u otro equivalente de contacto gratuito para la atención del soporte solicitado 24x7 los 365 días del año, así como también un correo electrónico, el cual luego de generar el ticket de soporte y/o incidente, se tendrá como plazo máximo de dos (02) horas para requerimientos de baja complejidad como configuraciones, modificaciones de políticas entre otros requerimientos básicos en los equipos de seguridad perimetral y que sean reportados para la solución del mismo. En caso de que dichos requerimientos sean de alta complejidad, a ser indicado por el contratista, o genere un impacto en la disponibilidad del servicio, se realizará una evaluación previa e informada, en coordinación con el personal técnico de la entidad, siendo los niveles de atención de la siguiente forma:

  Incidencia severidad 1: Falla de hardware o software que involucre caída del servicio causando impacto critico en las operaciones vía internet del cliente. Tiempo máximo de solución: 02 horas.

Incidencia severidad 2: Degradación en la calidad del servicio, impacto significativo en las operaciones vía internet del cliente. Tiempo máximo de solución: 02 horas.

Incidencia severidad 3 y requerimientos: Problemas de menor impacto, consultas de tipo operativo, se incluye también cambios de configuración. Tiempo máximo de solución: 02 horas.

- Las herramientas de monitoreo deberán ser personalizadas en coordinación con el área usuaria.
- El área usuaria deberá tener acceso en modo consulta del tratamiento de los incidentes y/o requerimientos, los mismos que deberán atenerse en el momento en que se solicitan (estos requerimientos ingresarán por el canal regular 0800 y/o por correo electrónico).

## 9. PERFIL, CERTIFICACIONES Y ACTIVIDADES DEL PERSONAL CLAVE

### 10.1. PERFIL DE LOS PROFESIONALES:

Debemos indicar que por la complejidad de las diversas actividades del presente Proyecto es que se debe considerar profesionales independientes para los siguientes perfiles:

a) Jefe de Proyecto del Servicio (01): Título profesional en Ingeniería Electrónica y/o Ingeniería de Sistemas y/o Ingeniería de Redes y/o Telecomunicaciones.
b) Especialista en Acceso a Internet e Interconexión de datos (01): Bachiller o Ingeniero titulado Electrónica y/o Sistemas y/o Redes y/o Telecomunicaciones.
c) Especialista Seguridad perimetral (01): Técnico o Bachiller o Ingeniero titulado en Electrónica, Eléctrica, Sistemas, Telecomunicaciones, Redes y/o Comunicaciones y/o Computación e Informática y/o Informático.

### 10.2. CERTIFICACIONES:

a) Jefe de Proyecto del Servicio (01), deberá contar con certificado PMP o un diplomado en Gerencia de Proyectos, el cual se acreditará mediante copia simple de constancias, certificados, certificación PMP activa o similares debiendo incluir los nombres y apellidos del profesional y el nombre de la Entidad u organización que emite el documento.

b) Especialista Seguridad perimetral (01), deberá contar con Certificación técnica o cursos en al menos 02 tecnologías a ser instaladas en el centro de datos del Ministerio: equipos de seguridad Firewalls y/o Administrador de Ancho de Banda y/o WAF, las cuales se acreditarán con copia simple de constancias y/o certificados y/u otros documentos, según corresponda.

### 10.3. ACTIVIDADES A DESARROLLAR:

a) Jefe de Proyecto del Servicio (01), estará a cargo del seguimiento de cada una de las actividades realizadas del especialista durante la puesta en marcha de la contratación.
b) Especialista en Acceso a Internet e Interconexión de datos (01), estará a cargo de las actividades de la implementación de los servicios de Internet y e interconexión de sedes, entre otros, durante la puesta en marcha de la contratación.
c) Especialista Seguridad perimetral (01), estará a cargo de las actividades de la implementación de toda la seguridad perimetral, instalación, configuración y fase de pruebas de los equipos de la puesta en marcha de la contratación.

## 10. DOCUMENTOS PARA LA SUSCRIPCION DEL CONTRATO

El ganador de la Buena Pro deberá presentar lo siguiente:

- ✓ Indicar los países que no están incluidos en la bolsa de destinos internacionales tanto fijos como móviles.
- ✓ Plan de trabajo de implementación del servicio el cual incluirá el cronograma de instalación, presentación del diagrama matriz de riesgo entre otros.
- ✓ Relación de las personas de contacto responsable del servicio de implementación, número telefónico, celular, correo electrónico, además del nivel de escalamiento.
- ✓ Documentos de acreditación del personal clave de acuerdo a lo señalado en el numeral 10.2 de los términos de referencia.
- ✓ Documento señalando el contacto gratuito y el correo electrónico.

## 11. ENTREGABLES POR EL SERVICIO DE IMPLEMENTACION

Deberá existir previamente una presentación del Plan de Trabajo, así como una reunión de Inicio de Proyecto. Una vez culminada la instalación, configuración y pruebas se suscribirá el Acta de Implementación del servicio, para ello el Contratista deberá entregar la siguiente documentación técnica:

- ✓ Arquitectura implementada en la sede central, por cada Museo y DDC.
- ✓ Topología general de la red de la sede central con los Museos y DDC.
- ✓ Descripción de la tecnología y topología de toda la solución implementada (las soluciones de equipos y marcas), que incluya la Tecnología de transporte Metro Ethernet o MPLS en el Backbone del Contratista.
- ✓ Cartas del fabricante para los routers, firewall, gestor de ancho de banda y WAF, indicando que los equipos o productos entregados para este proceso son nuevos y de primer uso, asimismo, deberá indicar un enlace (link público impreso o digital) que los equipos cuentan con vigencia tecnológica, es decir, no tienen anuncio de "End Of live" ni "End of Support".
- ✓ Actas de instalación de los equipos de comunicaciones por cada servicio y puntos de ubicación física (Museos de Lima y DDC)
- ✓ Relación de equipos implementados por servicio y ubicación física (Sede Central, Museos de Lima y DDC).

La suscripción del Acta de implementación del servicio estará a cargo del comité designado para este proyecto y por el jefe del Proyecto del Contratista.

**12. ENTREGABLE MENSUAL**

Una vez iniciado el servicio el Contratista deberá entregar la siguiente documentación técnica:

- ✓ Reporte de Incidencias y/o requerimientos mensuales referidos al reporte mensual del estado del enlace de internet brindado por la herramienta de monitoreo.
- ✓ Reporte de eventos propios del servicio, así como el comportamiento de internet y de seguridad (clasificándolos en controlados, mitigados y/o aceptados).
- ✓ Acciones ejecutadas para superar y/o mantener el correcto desarrollo del servicio.
- ✓ Recomendaciones y/o consideraciones como parte del servicio a ejecutar por parte del cliente en caso sea necesario.
- ✓ Informe técnico y ejecutivo del Análisis de vulnerabilidad interno y externo cuando corresponda de manera semestral.

El mismo que deberá ser entregado en un plazo máximo de quince (15) días calendario luego de culminado el servicio mensual.

**13. PLAZO DE PRESTACION DEL SERVICIO**

El plazo de prestación del servicio deberá ser de 1.096 (Mil noventa seis días calendario) lo que equivale a treinta y seis (36) meses y deberá iniciar el 08 de agosto del 2025 y luego de suscrita el Acta de implementación del servicio por parte del contratista y el área usuaria que es la Oficina General de Estadísticas y Tecnologías de Información y Comunicaciones – OGETIC

**14. PLAZO DE IMPLEMENTACION DEL SERVICIO**

El plazo de entrega para realizar la instalación, configuración y puesta en marcha del servicio será de hasta ciento veinte (120) días calendario que se computaran a partir del día siguiente de la suscripción del contrato.

La Entidad garantizará los accesos y autorizaciones necesarias para la ejecución de los respectivos trabajos de implementación del servicio dentro de sus instalaciones.

La ausencia de facilidades de acceso y/o autorizaciones y/o facilidades técnicas requeridas imputables a la Entidad, determinará la suspensión del plazo de implementación previsto en las bases hasta que se encuentre subsanado el inconveniente, sin generar penalidad alguna al contratista.

El plazo de prestación del servicio será computado desde la fecha de la suscripción del Acta de Activación (Acta de Implementación del servicio) y no desde la fecha del contrato.

**15. FORMA DE PAGO**

El MINISTERIO se obliga a pagar la contraprestación a EL CONTRATISTA en soles, de manera mensual y en partes iguales a la presentación de la factura respectiva y previa conformidad por parte de la Oficina General de Estadísticas y Tecnologías de Información y Comunicaciones – OGETIC, de acuerdo con los plazos establecidos en la Ley de Contrataciones del Estado y, 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. Asimismo, debemos precisar que se podrá hacer un prorrateo en caso la fecha de inicio no coincida con el ciclo de facturación asignado, solo para el primer pago.

Se aceptará el ciclo de facturación que le asigne el postor ganador de la Buena Pro.

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

- Informe mensual del funcionario responsable del Oficina de General de Estadísticas y Tecnologías de la Información y Comunicaciones (OGETIC) previo informe de la Oficina Informática y Telecomunicaciones (OIT).

- Comprobante de pago mensual.

Dicha documentación se debe presentar en Mesa de Partes, sito en el primer piso del edificio ubicado en Av. Javier Prado Este 2465 – San Borja o por medio virtual el Ministerio de Cultura pone a disposición su Plataforma Virtual de Atención a la Ciudadanía (dar clic aquí), donde usted podrá:

1. Ingresar su solicitud/comunicación (icono Ingreso de Documentos).
2. Recibir la respuesta a su solicitud/comunicación de manera inmediata, con alertas a su correo electrónico y número de celular, en tiempo real, previa creación de su Casilla Electrónica.
3. Conocer en tiempo real el estado de su expediente.

**16. CONFORMIDAD**

- La conformidad del Servicio de Implementación será emitida por la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones, previo informe de la Oficina de Informática y Telecomunicaciones quien verificará el cumplimiento del servicio y el entregable indicado en el ítem 12.
- La conformidad mensual del servicio será emitida por la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones previa presentación de la factura del Contratista, así como un informe del entregable según lo indicado en el ítem 13.

**17. OTRAS PENALIDADES**

El nivel de disponibilidad del servicio se medirá mensualmente según la siguiente formula:

Nivel de disponibilidad (%) = (Tiempo total horas-Tiempo total horas no disponible) *100

Tiempo total horas

Por lo que se aplicara penalidades de acuerdo con el siguiente cuadro:

| ***Otras penalidades*** | | | |
|---|---|---|---|
| ***N°*** | ***Supuestos de aplicación de penalidad*** | ***Forma de cálculo*** | ***Procedimiento*** |
| 1 | **Nivel de Disponibilidad:**<br>Sede central: Entre el 99.70% y 99.94%<br>Sedes Remotas: Entre el 99.00% y 99.49% | 5% de la renta mensual del servicio | Según informe de la OGETIC. |
| 2 | **Nivel de Disponibilidad:**<br>Sede central: Menos al 99.70%<br>Sedes Remotas: Menos a 99.00 % | 10% de la renta mensual | Según informe de la OGETIC. |
| 3 | **Demoras en atención / Soporte Especializado**<br>Mayor a 2 horas | 10% de la renta mensual | Según informe de la OGETIC. |
| 4 | **NO Presentación del Informe de Vulnerabilidades** | 10% de la renta mensual | Según informe de la OGETIC |

Se entiende por tiempo real total no disponible, la sumatoria de todos los minutos durante los cuales el Ministerio no tuvo la disponibilidad del servicio, siendo estos minutos acumulables en forma mensual.

No se contabilizará en el tiempo de no disponibilidad las interrupciones de servicio que pudieran producirse por causas imputables al Ministerio o terceros.

Se precisa que la penalidad por la disponibilidad del servicio será descontada por el enlace en donde ocurra el incidente o avería y no en la renta mensual total del contrato.

Se precisa que las penalidades contempladas se aplicarán a todos los componentes del presente servicio.

Se precisa que en el caso que la afectación del servicio sea por causas externas al operador, no se considerará como un supuesto de penalidad.

De acuerdo con el segundo párrafo del inciso a) del numeral 2.1 del artículo 10 del Reglamento de Comprobantes de Pago; " (...) excepcionalmente, el adquirente o usuario podrá emitir una nota de débito como documento sustentatorio de las penalidades impuestas por incumplimiento contractual del proveedor, la misma que será emitida en un plazo de cinco (5) días posteriores a la solicitud del Contratista.

## 18. RESPONSABILIDAD POR VICIOS OCULTOS

El Contratista será responsable por la calidad ofrecida y por los vicios ocultos de los bienes y servicios ofertados por un plazo de tres (03) años contados a partir de la conformidad otorgada por parte del Ministerio de Cultura.

## 19. SISTEMA DE CONTRATACION

A Suma Alzada.

## 20. REQUISITOS DE CALIFICACIÓN

| | |
|---|---|
| **A** | **CAPACIDAD LEGAL** |
| | **HABILITACIÓN** |
| | Requisitos:<br>• Autorización vigente otorgada por el Ministerio de Transportes y Comunicaciones (MTC) para proporcionar los servicios requeridos<br><br>Acreditación:<br>• Copia simple del documento que acredite la autorización solicitada o la publicación realizada por la autoridad competente en el Diario Oficial El Peruano, donde se indique y/o autorice que puede brindar los servicios requeridos, y/o copia simple del Certificado de Registro de Empresas Prestadoras de Servicios de Valor Añadido emitido por el Ministerio de Transporte y Comunicaciones y/u oficio del MTC con las concesiones vigentes y/o la impresión de la página web del MTC donde se visualiza las concesiones vigentes del operador y/o la publicación en el diario oficial El Peruano del otorgamiento de la concesión a favor del participante.<br><br>**Importante**<br>*En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito.* |
| **B** | **CAPACIDAD TÉCNICA Y PROFESIONAL** |
| **B.1** | **INFRAESTRUCTURA ESTRATÉGICA** |
| | Requisitos:<br><br>Contar con un Centro de Gestión y Control necesaria para la atención y solución de averías de los servicios solicitados, servicio de internet, servicio de líneas de telefonía, servicio de seguridad perimetral gestionada y servicio de interconexión de datos con los Museos y las DDC, se precisa que el postor deba contar con un NOC y/o SOC (propio o tercerizado) para la gestión, monitoreo y soporte en modo 24x7 para las soluciones requeridas.<br><br>Se precisa que, la infraestructura estratégica requerida es un Centro de Gestión y Control necesario para la atención y solución de averías de los servicios materia del procedimiento.<br><br>Una licencia de funcionamiento se considerará documento validado en tanto permita acreditar la disponibilidad de la infraestructura para los fines requeridos (Centro de Gestión y control para atención y solución de averías.<br><br>Se precisa que, para cumplir con dicho requisito se requiere que el contratista cuente con un NOC y SOC (propio o tercerizado) para la gestión, monitoreo y soporte en modo 24x7 para las soluciones requeridas, sin embargo, para la acreditación del cumplimiento de dicho requisito, se requiere que el postor acredite contar con un NOC y/o SOC (propio o tercerizado) para la gestión, monitoreo y soporte en modo 24x7 para las soluciones requeridas.<br><br>Acreditación:<br><br>Copia de documentos que sustenten la propiedad, la posesión, el compromiso de compra venta o alquiler u otro documento que acredite la disponibilidad de la infraestructura estratégica requerida.<br><br>**Importante**<br>*En el caso que el postor sea un consorcio los documentos de acreditación de este requisito pueden estar a nombre del consorcio o de uno de sus integrantes.* |
| **B.2** | **CALIFICACIONES DEL PERSONAL CLAVE** |

| | |
|---|---|
| | **FORMACIÓN ACADÉMICA**<br><br>Requisitos:<br><br>• **Jefe de Proyecto del Servicio (01):** Título profesional en Ingeniería Electrónica y/o Ingeniería de Sistemas y/o Ingeniería de Redes y/o Telecomunicaciones.<br>• **Especialista en Acceso a Internet e Interconexión de datos (01)**: Bachiller o Ingeniero titulado Electrónica y/o Sistemas y/o Redes y/o Telecomunicaciones.<br>• **Especialista Seguridad perimetral (01)**: Técnico o Bachiller o Ingeniero titulado en Electrónica, Eléctrica, Sistemas, Telecomunicaciones, Redes y/o Comunicaciones y/o Computación e Informática y/o Informático.<br><br>Acreditación:<br><br>El GRADO DE BACHILLER O TÍTULO PROFESIONAL REQUERIDO será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: 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.<br><br>En caso EL GRADO DE BACHILLER O TÍTULO PROFESIONAL REQUERIDO no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida. |
| **B.3** | **EXPERIENCIA DEL PERSONAL CLAVE** |
| | Requisitos:<br><br>• **Jefe de Proyecto del Servicio:** Experiencia mínima de tres (03) años en implementación de servicios y/o trabajos de instalación y/o mantenimiento de internet y/o red privada VPN y/o telefonía fija y/o gestionar y/o supervisar y/o liderar la implementación de proyectos de telecomunicaciones (acceso a internet y/o transmisión de datos y/o telefonía fija) y/o liderar la implementación de Proyectos de Servicios Fijos Corporativos (transmisión de datos, Internet, Comunicaciones Unificadas y Telefonía) e infraestructura de data Center.<br>• **Especialista en Acceso a Internet e Interconexión de datos**: Experiencia mínima de dos (02) años en implementación de servicios y/o trabajos de instalación y/o mantenimiento de internet y/o red privada VPN.<br>• **Especialista Seguridad perimetral (01)**: Experiencia mínima de dos (02) años en implementación de servicios y/o trabajos de instalación y/o configuración de equipos de seguridad perimetral.<br><br>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.<br><br>Acreditación:<br><br>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.<br><br>**Importante**<br><br>• *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.*<br><br>• *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.*<br><br>• *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*<br><br>• *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** | **EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD** |
| | Requisitos:<br><br>El postor debe acreditar un monto facturado acumulado equivalente a 4,500,000.00 (Cuatro 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.<br><br>Se consideran servicios similares a los siguientes: Servicios de Internet y Seguridad fijo y/o servicio internet Móvil y/o servicio de transmisión de datos y/o servicio de seguridad perimetral y/o servicio de transmisión de voz y datos y/o red de enlace de datos entre sedes y/o servicio de línea de contingencia para transmisión de datos y/o enlace dedicado de acceso a internet y/o línea de contingencia para transmisión de datos y/o servicio de internet dedicado y/o servicio de transmisión de voz y datos y/o servicio de interconexión de voz y datos.<br><br>Acreditación:<br><br>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones.<br><br>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 Nº 6** referido a la Experiencia del Postor en la Especialidad.<br><br>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.<br><br>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.<br><br>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 de que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.<br><br>Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.<br><br>Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 7.**<br><br>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.<br><br>Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 6** referido a la Experiencia del Postor en la Especialidad.<br><br>**Importante**<br><br>• *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.*<br><br>• *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.*

## ANEXO A: PUNTO N° 01

### SERVICIO DE SEGURIDAD PERIMETRAL GESTIONADA EQUIPO DE SEGURIDAD PERIMETRAL FIREWALL DE SIGUIENTE GENERACIÓN (02)

**Características Técnicas**

**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 02 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones y funcionar de manera activo/pasivo o activo/activo.
- El fabricante debe estar como líder en el último informe de Forrester Wave Automated Malware Analysis y/o el reporte de Forrester Wave Enterprise Firewall Solution.
- El fabricante debe estar certificado por USGv6 para trabajar IPv6 tanto en Firewall como en IPS.
- La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.
- El equipo deberá soportar el tráfico de toda la Entidad y Sedes Remotas.
- Ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support, se deberá adjuntar el link público (Url, portales, datasheets) del fabricante que verifique que los modelos propuestos no están en ese listado.
- Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos por el Contratista.
- 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
- Para el perfeccionamiento del contrato, se deberá proporcionar el acceso a una herramienta adicional o módulo dentro de la plataforma de NGFW 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.
  Dicha herramienta mínimamente deberá contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs y/o sobre la plataforma y los controles de seguridad y/o basadas en algún estándar internacional, tales como ISO 27001, CIS, NIST-800, COBIT o alguna otra similar que sea aplicable.
  Se requiere que para el perfeccionamiento del contrato se incluya documentación pública sobre dicha herramienta explicando su alcance, la cual hace referencia a la documentación técnica pública de la marca donde se evidencia el cumplimiento de los requerimientos técnicos solicitados para el presente proyecto.
  Los puntos que no puedan sustentarse con información pública pueden ser sustentados con carta del fabricante y/o link impreso de los módulos de seguridad, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs y/o el módulo dentro de la plataforma de NGFW.
  La herramienta de evaluación de buenas prácticas deberá ser específica para la configuración de Next Generation Firewall implementado o módulo dentro de la plataforma de NGFW, 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 Next Generation Firewall de 21Gbps como mínimo medido con tráfico de real (transacciones http 64KB o transacciones usando una mixtura de aplicaciones y/o condiciones de pruebas empresariales). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico, asimismo el equipo deberá soportar todo el tráfico de la Entidad para su óptimo funcionamiento.
- Throughput de Threat Prevention de 20Gbps como mínimo medido con tráfico de real (transacciones http 64KB o transacciones usando una mixtura de aplicaciones y/o condiciones de pruebas empresariales), con las siguientes funcionalidades habilitadas simultáneamente: Firewall con clasificación y control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Anti-malware de red con capacidades opcionales de Antispyware o Antibot, Antispyware (o AntiBot), control de amenazas avanzadas de día cero (Sandboxing) y logging activo. 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.
- Se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, y/o link impreso de los módulos de seguridad y datasheets respaldado por la marca.
- La plataforma de hardware debe soportar como mínimo 09 millones de sesiones simultaneas y 200,000 nuevas sesiones por segundo, medidos en capa 7, por ejemplo, con paquetes HTTP y/o TCP.
- Rackeable en 1 unidades de rack como mínimo.
- Disco de estado sólido interno (opcional).
- Mínimo 4 interfaces de red 10/100/1000 en cobre, formato RJ45.
- Mínimo 4 interfaces de red 1/10G en formato SFP o SFP+ para el tráfico de datos de la red de la Entidad.
  Se deberán incluir por cada equipo solo los transceivers que sea necesario para brindar conectividad a las interfaces mínimas requeridas.
- La plataforma deberá contar con al menos 2 interfaces adicionales 10/100/1000 en cobre RJ45 y dedicadas a la sincronización de estado y configuración dentro del clúster de alta disponibilidad, se aceptará opcionalmente como mínimo 1 interfaz adicional para la sincronización de HA.

**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).
- Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC “address auto configuration” (opcional), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.
- Permitir configurar el tiempo de almacenamiento o la cantidad de entradas en cache de la tabla ARP.
- Permitir NAT de destino basado en dominio en lugar de IP. El equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino.
- Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.
- Soportar túneles GRE como punto de inicio o finalización del túnel (opcional).

- Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN y/o IPSec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel.
- Soportar IPv6 en modos de alta disponibilidad, Activo/Activo y/o Activo/Pasivo.
- Debe permitir el bloqueo de ataques de Denegación de Servicio (DoS), definiendo un umbral máximo de conexiones por segundo por tipo de paquete (SYN, ICMP, UDP).
- 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 y/o mediante el uso de sus interfaces físicas y/o sin necesidad de tener que hacer uso de contextos o dominios virtuales.

**Alta Disponibilidad**

- Soporte a configuración de alta disponibilidad Activo/Pasivo y/o Activo/Activo, opcionalmente con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).
- La configuración en alta disponibilidad debe sincronizar: Sesiones; Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y/o objetos de red; Certificados de descifrado.

**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 (el cual opcionalmente pueden ser basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.
- Permitir el agendamiento de las políticas de seguridad, se aceptará opcionalmente que la capacidad se pueda brindar desde la solución NGFW o su consola de gestión.
- Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
- Permitir añadir un comentario cada vez que se haga un cambio o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada.
- 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) el cual también se podrá brindar desde la solución NGFW o su consola de gestión.
- Debe contar con mecanismos que faciliten la optimización de reglas de seguridad:
- Mostrar la primera y última vez que se utilizó una regla de seguridad
- 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 el cual también se podrá brindar desde la solución NGFW o su consola de gestión.
- 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 permitir los algoritmos de cifrado para negociar la conexión SSL/TLS, deberá soportar como mínimo los siguientes: RSA, DHE, ECDHE y/o 3DES, AES-128-GCM, AES-128-CBC, AES-256-GCM, AES-256-CBC, MD5, SHA1, SHA256, SHA384.
- Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido
- Debe poder bloquear las sesiones cuyo certificado no es válido o el emisor no es confiable a pesar de no aplicar descifrado al tráfico SSL/TLS (opcional)
- Debe soportar certificados que utilice Subject Alternative Name (SAN).
- Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios, wildcards y/o categorías web.

- Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.

**Control de Aplicaciones**

- Reconocer por lo menos 3000 aplicaciones diferentes actuales a la fecha, 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 procesar e inspeccionar aplicaciones que utilicen HTTP/2
- Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. 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.
- Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado y/o tener una base de datos con un mínimo de 10000 aplicaciones.
- Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
- Permitir nativamente la creación de firmas personalizadas basadas en expresiones regulares de aplicaciones propietarias desde la interfaz de gestión sin la necesidad de acción por parte del fabricante y/o a través de las herramientas propias del fabricante.
- Permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad.
- Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como:
    - Tecnología utilizada en las aplicaciones (Client-Server, Browser Based, Network Protocol) y/o nivel de riesgo de las aplicaciones Nivel de riesgo de las aplicaciones.
    - Categoría y subcategoría de aplicaciones y/o aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda.

**Prevención de Amenazas**

- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus (Antimalware de red), Anti-Spyware (o Antibot) y DNS SinkHole o redirección DNS para tráfico de equipos comprometidos por spyware integrados en el propio Appliance, se aceptará que la capacidad de Antispyware sea parte del servicio de Antivirus o Antimalware.
- Las funcionalidades de IPS, Antivirus y Anti-Spyware 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 o deberá considerarse la licencia de las funcionalidades hasta 06 meses posterior a la fecha de finalización del contrato, de ser necesario, ante una probable extensión del servicio.
- Cuando se utilicen las funciones de IPS, Antivirus y Antispyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Antivirus y Antispyware habilitadas simultáneamente.
- El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware.
- Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de

todos esos ítems.

- Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
- Capacidad de inspeccionar malware y/o archivos maliciosos que se distribuye por SMB v3 en IPv4 y/o IPv6.
- Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, HTTP/2, FTP, SMB, SMTP e POP3, tanto para IPv4 como IPv6, este último podrá ser habilitado mediante una actualización de software cuando sea requerido por la entidad dentro del período de contrato.

**Prevención de Amenazas Desconocidas**

- El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis en una plataforma de tipo sandbox, la cual podrá ser en versión nube o appliance on-premise.
- En caso se trate de sandbox cloud, deberá ser una nube propia del Contratista con certificación de seguridad y privacidad de datos, como mínimo SOC Tipo 2 o FedRAMP y opcionalmente deberá garantizar un tiempo de análisis de malware de día cero no mayor a 5 minutos.
- En caso se trate de sandbox on-premise, deberá contar por lo menos con 05 máquinas virtuales de un mix de sistemas operativos para analizar el malware de la Entidad.
- Soportar el análisis de archivos maliciosos a nivel de CPU y/o en ambiente controlado como mínimo, sistema operacional Windows XP, Windows 7, Windows 10 y Windows 11, Mac OS X, Linux y Android.
- Debe tener la capacidad de enviar archivos, para ser analizados en el entorno de Sandbox.
- El Firewall debe ser capaz de integrarse al sandbox para enviar archivos sospechosos que sean descargados o subidos, como mínimo, a través de los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB.
- Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de Antivirus y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
- 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 y/o deberá ser analizado por el especialista designado por el proveedor y la marca ofertada a fin de contar con un reporte del evento suscitado.
- Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF, archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar y/o e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOSX (dmg, pkg y/o mach-o) y/o Android APKs en el ambiente controlado.
- 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 hipervisores comerciales), inyección de código a procesos permitidos y/o des habilitación de funcionalidades de seguridad del host.

**Filtro URL**

- 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 LDAP, Active Directory y/o e-Directory 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 60 categorías de URLs, incluyendo las de malware y phishing.
- Debe permitir la creación de categorías personalizadas.
- Deberá contar con una vista y/o reporte de la URL accedidas por los usuarios.
- Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas o a categorías y subcategorías.
- Debe identificar y categorizar los dominios nuevos, menores a 30 días de antigüedad y/o contar con categorías de dominios recientemente creados e inactivos.
- 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.

**Identificación de Usuarios**

- Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell directory, Exchange y base de datos local.
- Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.
- Opcionalmente podrá soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x, soluciones NAC, soluciones proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API, así como la lectura mediante WMI a equipos Windows para la identificación de direcciones IP y usuarios.
- Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.
- 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.
- Debe soportar la identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server.

**QoS.**

- Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix, por ejemplo), se requiere que la solución tenga la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones.
- Soportar la creación de políticas de QoS por: dirección de origen y destino, por usuario y grupo de LDAP/AD, 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**

- Se deberá considerar el licenciamiento correspondiente para soportar 500 túneles VPN Site-to-Site y 500 usuarios Client-To-Site.
- Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.
- La VPN IPSec 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.
- Las VPN client-to-site deben poder operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.
- Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN client-to-site.
- Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
- Debe soportar Autenticación Multi-Factor (MFA).
- Debe permitir administrar los segmentos de red en el equipo Firewall a fin de brindar los accesos al equipo que tenga instalado el agente de VPN.
- Debe permitir la configuración del Split Tunnel, de tal forma que permita elegir o excluir el tipo tráfico que se enrutará por el túnel VPN.
- Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
    - Antes del usuario se autentique en la estación;
    - Después de la autenticación del usuario en la estación usando Single Sign On (SSO);
    - Bajo demanda del usuario;
- Debe asignar una IP a cada cliente que se conecte a la VPN en formato IPv4 y/o IPv6, de forma automática mediante un pool de IP.
- El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8 y/o Windows 8.1, Windows 10, MacOS X, y dispositivos móviles.
- Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.

**Administración**

- Debe ser administrado por una consola web que pueda trabajar en varios idiomas, como mínimo inglés y español. La consola debe ser capaz de detectar errores de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).
- La administración de las políticas de seguridad debe realizarse sobre hardware dedicado para dicho propósito ya sea dentro de los mismos appliances de seguridad o mediante un servidor o appliance dedicado.
- Permitir exportar las reglas de seguridad en formato CSV y/o PDF y/o HTML.
- Debe contar con un dashboard que permita monitorear las sesiones y CPU del equipo Firewall, throughput de las interfaces, política más usada, usuario o IP que genera mayor consumo de la red.
- Debe permitir el control de acceso por roles a la gestión del equipo.
- 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 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 sobrepongan reglas generales sobre reglas específicas (shadowing rules).
- Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup).
- 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 auditoria detallados, informando de la configuración realizada, el administrador que la realizo, 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 o también la asignación de cuota de disco podrá ser a nivel de la retención de logs por un periodo de tiempo.
- Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, 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 o JSON.
- Debe permitir la desconexión manual los usuarios ante algún incidente de seguridad o mal uso de la herramienta.

## ANEXO A: PUNTO N° 02

## SOLUCIÓN DE SEGURIDAD DE CORREO ELECTRONICO. SOLUCIÓN CLOUD

**Aspectos Generales**

- La solución debe ser una plataforma 100% nube que brinde un servicio de tipo SaaS, considerando que el Ministerio de Cultura tiene aproximadamente unas 3000 cuentas de correo electrónico.
- Debe detectar el spam, phishing y APTs en los mensajes de correos electrónicos entrantes que introducen ransomware y otras amenazas avanzadas, actualizándose permanentemente.
- Debe incluir filtrado de contenido para el control de datos salientes y cifrado de correo electrónico para comunicaciones seguras.
- Debe proteger el correo electrónico en cualquier lugar donde los usuarios necesiten acceder a él, incluso en dispositivos móviles.
- Debe brindar protección contra phishing, malware y contar con DLP, la tecnología de DLP que utilice la solución, debe ser líder reconocido en el mercado por Analistas de terceros como Gartner, durante el tiempo que estuvo activo.
- El servicio SaaS Email Security estará disponible el 99.999% del tiempo
- El producto debe tener un filtrado en la nube, ahorrando ancho de banda al eliminar el spam y las amenazas en la nube
- El filtrado en la nube deberá eliminar tanto correos reconocidos como SPAM y con algún tipo de malware reconocido.
- Debe proporcionar una detección de spam del 99% o superior.
- Debe contar con una base de firmas actualizadas periódicamente con las nuevas amenazas para el bloqueo de correos maliciosos.

**Distribución e Instalación**

- Bastará con configurar los registros de intercambio de correo (MX) con los Data Centers del Servicio SaaS Email Security
- La solución debe ser capaz de integrarse con cualquier plataforma de Mensajería vía SMTP, por ejemplo, Microsoft Exchange, Lotus, Zimbra entre otras.
- Deberá poder analizar el tráfico entrante y saliente SMTP a través de la misma plataforma en la nube SaaS.

- El servicio deberá mantener en cola aquellos correos que no puedan ser entregados en caso de indisponibilidad del enlace o caída de servicio de correo on-premise
- Los componentes de Reportes y consola deben estar en la nube.

**Clustering & HA**

- La solución debe poseer Alta disponibilidad en diferentes Datacenters alrededor del mundo. Por lo menos 12 sitios distribuidos en al menos 3 continentes.
- El servicio SaaS de Email Security debe ofrecer sus funcionalidades en formato MULTITENANT Cloud. No se aceptarán, soluciones que ofrezcan sus servicios SaaS en SINGLE-TENANT Cloud (por ejemplo, VMs hosteadas o instancias de Virtual Machines por cliente)

**Características Generales**

- Tener la capacidad de generar políticas al tráfico entrante y al tráfico saliente, de forma independiente. Todas las características solicitadas a continuación se deberán contemplar para el tráfico entrante como saliente.
- Contar con múltiples opciones de respuesta:
  - Eliminar Mensaje
  - Enviar Mensaje a un recipiente especificado
  - Guardar el Mensaje en una Cuarentena
  - Enviar Notificación
- Tener la flexibilidad de establecer distintas configuraciones de seguridad de correo electrónico, como políticas, a usuarios y grupos basados en sus direcciones de correo y dominios.
- Incluir un grupo de funciones mínimas que permitan:
  - Agregar funciones de análisis de Antivirus
  - Agregar funciones de análisis de URL embedidas en el correo
  - Agregar funciones de AntiSpam
  - Agregar funciones de detectar Correos de Tipo Comercial
  - Agregar análisis de Caja de Arena
  - Agregar funciones de Disclaimer
- Poseer técnicas de filtrado de spam, basados en firmas de spam, filtrado de URL, combinación de patrones utilizados en el spam y heurístico.
- Deberá soportar SPF (Sender Policy Framework) y deberá permitir las siguientes opciones:
  - Rechazar el mail el registro SFP no existe
  - Rechazar el mail si el registro SPF no hace un match con el dominio de quién envía
  - Rechazar en caso de errores
- Contar con reglas o perfiles de filtrado por:
  - Dirección IP del correo
  - Casilla de quíen envía
  - Casilla de recipiente
  - Cantidad de Recipientes
  - Campo From:
  - Campo To:
  - Campo Cc:
  - Campo Subject:
  - Cabecera Parcial del Correo
  - Cabecera Completa del Correo
  - Texto en el cuerpo
  - Tamaño del Mensaje
  - Resultado de la validación DKIM
  - Bloqueo de Archivos

- La plataforma del antispam no deberá solicitar suscripción

**Seguridad**

- Debe proveer una solución antivirus
- Debe permitir el bloqueo de archivos por nombre, por extensión y por tipo binario al usuario de destino.
- Deberá tener la capacidad de analizar archivos adjuntos comprimidos infectados y tomar acciones correspondientes
- El motor de seguridad de esta solución deberá descomprimir los archivos adjuntos sin necesidad de recurrir a programas externos, sin alterar el cuerpo del mensaje.
- Deberá revisar al menos las siguientes categorías:
    - Categorías relacionadas con material adulto
    - Categorías de Tabaco/Alcohol
    - Categorías sobre Drogas
    - Categorías de Juegos de Azar
    - Categorías referentes a Racismo
    - Categorías de URL con problemas de seguridad
    - Categorías de Hacking
    - Categorías de Violencia
    - Categorías respecto a las Armas
    - Categorías de Amenazas Emergentes
- La base de datos deberá ser propietaria del fabricante de la solución. No se aceptarán soluciones de filtrado que no sean del propio fabricante.

**Servicios de Sandboxing**

- Permite la protección de las URL embebidas en los correos electrónicos al momento de que el usuario realice un click sobre la URL. Esto permitirá que el servicio híbrido analice las URL de los mensajes en caso de riesgos de seguridad y cada vez que el usuario haga click en la URL se ejecute un procedimiento de análisis en tiempo real de la URL ejecutada. El producto podrá dar un veredicto si es seguro ir a la URL o no mostrando un mensaje de bloqueo o advertencia al usuario final fuera o dentro de la organización sin necesidad de utilizar productos adicionales de análisis de URL. Esta solución podrá agregarse como un adicional al producto ya adquirido
- El producto podrá contar con la posibilidad de adquirir como licencia adicional un servicio de sandboxing de archivos que permitirá analizar los siguientes archivos:
    - exe
    - pdf
    - dll
    - Microsoft Office: doc/.docx/.xls/.xlsx/.ppt/.pptx
    - eml

  Y los siguientes MIME Types:
    - application/zip
    - application/x-7z-compressed
    - application/x-tar
    - application/x-gzip
    - application/x-rar
- El servicio permitirá entregar un informe de la posible amenaza y dejará en cuarentena el archivo sospechoso a la espera del veredicto final de la caja de arena.
- El servicio de caja de arena deberá ser una solución cloud y no requerirá instalación adicional de servicios

**Uso de Mecanismos de TLS**

- Deberá permitir la conexión de sesiones TLS

- Deberá permitir generar certificados o importar certificados previamente para trabajar con TLS
- Deberá establecer un orden de prioridad especificando un nivel de seguridad para determinada conexión que deben incluir:
  - Encriptar
  - Encriptar y verificar CN (Common Name)
  - Verificar (validar que el certificado es de una certificación de confianza válida)
  - Verificar y revisar CN (validar el CN y validar también si el certificado es válido)
- Deberá permitir seleccionar el tipo de encripción por conexión. Deberá incluir al menos 2 tipos
  - Medio: Utilizar suites de cifrado de 128 bits de encripción
  - Alto: Utilizar suites de desencripción con llaves mayores a 128 bits
- Deberá permitir forzar conexiones TLS tanto entrantes como salientes con los parámetros antes explicados

**Uso de Servicio de Encripción Avanzada (Opcional)**

- Deberá poseer la capacidad de realizar encripción de correo avanzada en caso de que se requiera, se hace claridad que es un servicio adicional. El servicio podrá permitir utilizar el servicio de encripción avanzada si detecta algún patrón conocido o detecta, por ejemplo, una tarjeta de crédito en algún sector del correo tales como subject, body o adjuntos.
- El servicio de encripción avanzado permitirá un correo de notificación a la tercera parte respecto a la llegada de un correo cifrado. La tercera parte podrá acceder a un portal seguro (https) mediante una contraseña y nombre de usuario y a través del portal podrá revisar el correo cifrado.
- Las acciones que podrá realizar el usuario en este portal seguro son las siguientes:
  - Ver un mensaje seguro enviado
  - Responder a un mensaje seguro que haya recibido
  - Enviar un mensaje seguro que haya recibido
  - Redactar un nuevo mensaje seguro
  - Incluir un adjunto en un mensaje seguro
  - Ver un mensaje seguro que Ud haya enviado
  - Eliminar un mensaje seguro
  - Realizar una búsqueda por alguna palabra en el mensaje

**Gestión y Reporte**

- La solución debe tener una única consola de gestión y reportes con un solo login de acceso. No se aceptarán soluciones que requieran una página de login distinta para cada funcionalidad como Email Cloud, Email Quarantine ó Phishing.
- Debe incluir al menos 35 reportes predefinidos dentro de la solución, incluyendo mínimamente:

  - Anti-malware
  - Brand impersonation
  - Bulk
  - Domain impersonation
  - Anti-malware common attachments filter
  - Mailbox intelligence impersonation
  - High confidence phishing
  - High confidence spam
  - Intra-Organization phishing
  - Malware
  - Outbound spam
  - Phishing

- Safe Attachments
- Spam
- Spoofing

- Debe tener la capacidad de construir un reporte basado en atributos que son Fácil de analizar.
- Debe permitir programar informes para la entrega en una determinada frecuencia (diaria, semanal, mensual). Los informes pueden exportarse en formato PDF y CSV. Además, debe poder enviar el informe en formato encriptado y protegido por password.
- Debe tener la opción de descargar datos de informes para que los use una solución de seguridad de información y eventos de terceros (SIEM).

## ANEXO A: PUNTO N° 03

## SERVICIO DE SEGURIDAD PERIMETRAL GESTIONADA EQUIPO ADMINISTRADOR DE ANCHO DE BANDA (01)

Se requiere una solución de optimización de ancho de banda de appliance dedicado que cumpla con las siguientes características:

- El equipo debe ser nuevo y de tecnología vigente durante todo el periodo de contrato.
- El equipo deberá soportar un rango de operación mínimo de 2000 Mbps full dúplex, pero en licenciamiento será para el ancho de banda mínimo de 1000 Mbps más el crecimiento del ancho de banda solicitado.
- En caso la entidad requiera hacer uso del crecimiento del 30% de ancho de banda adicional, se deberá incluir el licenciamiento del equipo administrador de ancho de banda correspondiente.
- El equipo debe contar con capacidad instalada para manejar como mínimo 200,000 flujos IP concurrentes de tráfico y capacidad de crear al menos 1,024 políticas independiente de la cantidad de reglas que pueda tener cada una de ellas, garantizando que el equipamiento propuesto por el postor pueda administrar el ancho de banda solicitado y a su vez la demanda de crecimiento que requiera la Entidad durante todo el tiempo de contrato.
- El equipo administrador de ancho de banda deberá contar con fuentes de alimentación de energía y almacenamiento redundantes.
  Se aceptará el equipo administrador de ancho de banda con fuentes de energía y almacenamiento sin redundancia, debido a que no afecta el servicio de Internet brindado, siempre y cuando el contratista cumpla con un SLA para reposición del servicio no mayor a 4 horas.
- El equipo deberá realizar el control de ancho de banda de entrada (Inbound) y salida (Outbound) simultáneamente, con soporte de vlans IEEE 802.1q.
- El equipo deberá soportar y entregarse configurado con direccionamiento IPv4 e IPv6.

- El equipo deberá contar con al menos 04 interfaces de 1GB RJ45 y 1 puerto 1GB para gestión. Se debe incluir los transceivers. necesarios para habilitar 4 interfaces como mínimo.
- El equipo deberá tener visibilidad de tráfico a nivel de capa 3 del modelo OSI y poder aplicar políticas desde ese nivel hasta el nivel 7.
- Reconocimiento de aplicaciones basado en firmas, donde el fabricante debe garantizar la actualización de su catálogo de firmas de forma periódica que garantice mejorar el servicio de clasificación.
- Capacidad de detectar, clasificar y controlar tráfico por direcciones o rangos de direcciones IP, usuarios, servicio (aplicación) y VLAN.
- El equipo debe contener firmas que le permitan identificar anonimizers tipo VPN o tipo TOR y/o tráfico de criptomonedas (Crypto Mining y CryptoJacking) sin necesidad de módulos adicionales.
- Gestión de ancho de banda independiente en cada sentido de la comunicación: Upstream y Downstream.
- Las políticas o reglas de control de ancho de banda deben permitir: priorización de tráfico (al menos 4 niveles de prioridades), definir un mínimo ancho de banda garantizado y un máximo ancho de banda permitido.
- El equipo debe incluir una herramienta de reportes de consumo en tiempo real e histórico del uso del ancho de banda centralizada y externa, que permita generar reportes independientes de las políticas configuradas en el sistema.
  Se aceptarán soluciones que tengan la herramienta de reportes integrada en el mismo equipo (embebida) para el equipo administrador de ancho de banda ya que no afecta las funcionalidades de la solución.
- El equipo debe contar con un Bypass interno o externo en todas sus interfaces de 1GE usadas para el servicio, excepto la interface de gestión.
- El modelo de licenciamiento de la solución de Gestión de Ancho de banda debe ser a perpetuidad, no se aceptarán modelos de suscripción, sólo será necesario renovar anualmente el soporte del equipo en caso de requerirse.
- El contratista deberá realizar las coordinaciones con la marca ante alguna eventualidad; por lo tanto, la solución debe contar con un centro de soporte o TAC del fabricante sea de tipo 24*7 y con un SLA de atención que garantice la real atención ante una eventualidad y que el lenguaje sea de preferencia en español, pero también se aceptará que dicha atención sea en inglés, tomando en cuenta que el contratista hará las coordinaciones de manera directa y servirá como intermediario a la Entidad.
- Opcionalmente se podrá aceptar que el equipo provea los siguientes parámetros de rendimiento: Retardo transaccional de red; Retardo transaccional de servidor; Variación en el retardo de la aplicación (jitter); Perdidas entrantes (eficiencia); Perdidas salientes (eficiencia); Cantidad de sesiones activas; MOS para mediciones de VoIP y videoconferencia y salud TCP (conexiones iniciadas, conexiones ignoradas por el servidor, conexiones rechazadas por el servidor, conexiones abortadas).

## ANEXO A: PUNTO N° 04

## SERVICIO DE SEGURIDAD PERIMETRAL GESTIONADA EQUIPO DE SEGURIDAD PARA APLICACIONES WEB (01)

### CARACTERÍSTICAS FISICAS Y RENDIMIENTO

- El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, para propósitos de balanceo de carga de servicios aplicaciones WAF y visibilidad SSL ya sea en modalidad on-premise a través de appliance o en modalidad de servicios de nube en modo SaaS
- En caso de ser Appliance cada equipo debe cumplir con las siguientes características:
  - Soportar un Throughput de al menos 5 Gbps, a nivel de capa de aplicaciones.
  - Soportara mínimamente 90,000 de conexiones concurrentes en HTTPS.
  - Deberá soportar mínimamente conexiones de 125 mil conexiones por segundo a nivel de capa de transporte HTTPS Soportar mínimamente 2500 transacciones por segundo SSL (RSA2K) y Soportar 2100 transacciones por segundo SSL (EC P-256 o ECDH).
  - Cada equipo debe contar con al menos las siguientes Interfaces de red:
    - Mínimo cuatro (04) puertos de 1GBbps, en formato RJ45 o SFP, por lo que deberá incluir los transceivers correspondientes, de ser necesarios.
    - Deberá soportar mínimo dos (02) interfaces de red 10Gbps en formato SFP+, para crecimiento. No incluye transceivers.
  - Memoria RAM de 16Gb como mínimo
  - Disco duro de 480 Gb, como mínimo
- Soporte de cluster HA Activo/Activo o Activo/Standby entre los dispositivos.
- En el caso que se realice a través de modalidad SaaS, se deberá considerar como mínimo una cantidad de 12 millones de Web HTTP Request mensuales, sin limitación de cantidad de subdominios y/o aplicaciones web a ser protegidas.
- En el caso que se realice a través de modalidad SaaS, el servicio WAF ofrecido por el fabricante debe tener certificación SOC 2 Type II y tener un nivel de servicio (SLA) del 99.9% mensual como mínimo.
- En el caso que se realice a través de modalidad SaaS, agradeceremos considerar que la solución ofertada debe tener las siguientes las tecnologías de protección web:
  - Web Application Protection.
  - API Security.
  - Bot Prevention.
  - File Security.
  - DDoS Prevent.

- Así mismo en caso de que el equipo sea del tipo Appliance o en modalidad de servicios de nube en modo SaaS, se deberán considerar las siguientes características según correspondan:

**FUNCIONALIDADES DE SEGURIDAD**

- La solución debe poder trabajar en modo clúster (considerando equipos del mismo modelo y deberá soportar formar clúster entre modelos diferentes) entre más de dos equipos y que sean plataformas no necesariamente idénticas (como equipos appliance físico, chasis o virtuales) con el fin de contar con un sistema a futuro altamente escalable y en demanda. Para mejorar el rendimiento de la sincronización de configuración entre los equipos que se encuentren en HA, para mejorar el rendimiento de la sincronización cuando se encuentre un modelo de alta disponibilidad (HA).
- Soporte de seguridad SSL en base a las siguientes características:
  - Debe de soportar minimante conexiones de 125 mil conexiones por segundo a nivel de capa de transporte HTTPS
  - Soportar minimamente 2500 transacciones por segundo SSL (RSA2K)
  - Soportar 2100 transacciones por segundo SSL (EC P-256 o ECDH) Soporte de cifrado AES, AES-GCM, SHA1/MD5, Camellia y de algoritmos como: RSA, Diffie-Hellman, DSA y ECC
- El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall
- Cifrado de cookies para verificar su integridad.
- La solución debe permitir la funcionalidad Proxy SSL o SSL offloading.
- Debe permitir soporte para HSTS (HTTP Strict Transport Security)
- Permitir agregar a futuro, un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías (Scanners, Exploits Windows, Denial of Service, Proxies de Phishing, Botnets, Proxies anónimos) o contar con firmas que se actualicen periódicamente.

**FIREWALL DE APLICACIONES WEB (WAF)**

- La solución debe incluir funcionalidad de Firewall de Aplicaciones (WAF) en la misma caja, no debe ser un appliance independiente (para optimización de latencias, administración, espacio en rack, energía eléctrica, soportes de fabricante).
- La funcionalidad de WAF debe permitir la personalización de la política, de manera que se pueda ajustar finamente de acuerdo al servicio específico que estará protegiendo, sus URLs, parámetros, métodos, de manera específica.
- Debe trabajar en un esquema proxy TCP reverso y/o transparente
- Debe soportar la creación automática de políticas
- La creación automática de políticas deberá unificar múltiples URLs. Debe trabajar en modo de bloqueo o en modo informativo.
- Debe trabajar con modelos de seguridad positiva y negativa o con módulos de funcionalidad de seguridad.
- Debe poder aprender el comportamiento de la aplicación automáticamente sin intervención humana
- El WAF debe permitir personalizar las páginas de bloqueo
- Debe prevenir exponer el “OS fingerprinting”
- El WAF Debe soportar:
  - Restringir protocolo y versión utilizada (protocolo TLS y las versiones aceptadas para la TLS/SSL)

  - Multi-byte language encoding
  - Validar URL-encoded characters
  - Restringir la longitud del método de request o restringir un método junto a un directorio y extensión especifica de modo que se controle los parámetros del request indistintamente a su longitud.
  - Restringir la longitud de URI solicitado o bloquear las URL o path solicitados.
  - Restringir el número de Encabezados (headers) o que la solución WAF permita el análisis y bloqueo de vulnerabilidades en las cabeceras de las solicitudes.
  - Restringir la longitud del nombre de los encabezados
  - Restringir la longitud del valor de los encabezados
  - Restringir la longitud del cuerpo (body) de la solicitud
  - Restringir la longitud del nombre y el valor de las cookies o verificar la integridad de las mismas.
  - Restringir la longitud del nombre y valor de los parámetros
  - Restringir el número de parámetros
- El WAF Debe incluir protección para XML
- El WAF debe incluir protección contra el Top 10 de ataques definidos en OWASP
- El WAF debe incluir protección contra Web Scraping
- Debe ser Session-aware es decir identificar y forzar que el usuario tenga una sesión e identificar los ataques por usuario
- Permitir la protección contra ataques del tipo CORS (Cross-Origin Resource Sharing).
- Debe permitir verificar las firmas de ataque en las respuestas del servidor al usuario o de forma alternativa se acepta que la solución WAF enmascare información sensible que provenga como respuesta del servidor.
- Debe permitir el enmascaramiento de información sensible filtrada por el servidor
- Una vez detectado un ataque de DoS deberá ser posible descartar todos los paquetes que provengan de una dirección IP u origen sospechoso
- En caso de detectarse un ataque se requiere tener la posibilidad de iniciar una captura de tráfico (tipo tcpdump) para poseer información forense.
- Debe proteger como mínimo:
  - Ataques de Fuerza Bruta
  - Cross-site scripting (XSS)
  - Cross Site Request Forgery
  - SQL injection
  - Parameter and HPP tampering
  - Sensitive information leakage
  - Session highjacking
  - Buffer overflows
  - Cookie manipulation
  - Various encoding attacks
  - Broken access control
  - Forceful browsing
  - Hidden fields manipulation
  - Request smuggling
  - XML bombs/DoS
  - Open Redirect
- Debe poder identificar y configurar URLs que generen un gran consumo de recursos en los servidores como método de protección de ataques de

denegación de servicios.
- Debe contar con protección contra BOTS.
- Debe soportar CAPTCHA o FINGERPRINt como método de prevención para mitigar ataques de denegación hacia las aplicaciones protegidas.
- El WAF debe identificar de manera única a los dispositivos por medio de Fingerprint y haciendo tracking del dispositivo.
- Todas las características solicitadas deben estar activas hasta el fin del contrato.

**ESTÁNDARES DE RED**

- Soporte VLAN 802.1q, Vlan tagging
- Soporte de 802.3ad para definición de múltiples troncales
- Soporte de NAT, SNAT
- Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.
- Soporte de Traffic Rate.
- Soporte opcional de al menos 4 instancias virtuales como mínimo.
- Debe soportar protocolos de enrutamiento BGP, RIP.
  Este punto será opcional considerando que el requerimiento principal es un equipo de seguridad WAF y no un equipo Router.

**ADMINISTRACIÓN DEL SISTEMA**

- La consola de administración solicitada podrá estar integrada en el equipo o podrá ser un appliance dedicado para la administración o software dedicado en servidor siempre y cuando no degrade el desempeño del equipo.
- La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)
- La solución debe integrarse con Directorio Activo Windows 2003 o superior de forma nativa o por LDAP.
- La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.
- La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante: Protocolo Syslog, Notificación vía SMTP y SNMP versión.2.0 o superior.
- El equipo debe contar con un módulo de administración que permita encender/apagar el sistema de manera remota.
- La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real.

## ANEXO A: PUNTO N° 05

## SERVICIO DE SEGURIDAD DE PROTECCION AVANZADA PARA ENDPOINTS

- Para el caso de la solución de protección avanzanda de Endpoints; dicha solución deberá integrarse de forma nativa con el equipamiento Firewall; siendo dichas soluciones de la misma marca.
- Se debe considerar 250 agentes para la protección EDR (Endpoint Detection and Response) de los servidores.
- Prevención contra exploits
- Detección de técnicas de explotación sin necesidad de utilizar firmas, patrones o heurísticas, enfocadas principalmente en la prevención de exploits lógicos, procesos vulnerables y exploits del sistema operativo, para sistemas Microsoft Windows, MacOS y Linux.
- Mitigación de vulnerabilidades conocidas, desconocidas y prevención de explotación de vulnerabilidades.
- Soporta técnicas de explotación de vulnerabilidades distintas, entre las que se encuentran Return Oriented Programming, Heap Spray, Jit Spray, Shell link, Structured Exception Handler, etc.
- Capacidad de utilizar los módulos de protección contra técnicas de explotación en cualquier aplicación, incluyendo aquellas desarrolladas internamente.
- Capacidad de descargar snapshot desde la memoria o stack Memory d manera parcialmente, para un mayor análisis.
- Es posible configurar perfiles de protección en modo de prevención o monitoreo.
- Terminación del proceso en el cual fue identificado el intento de ejecución de una técnica de explotación.
- la solución de seguridad deberá de proteger equipos Mac OS de técnicas de explotación.
- Prevención de técnicas de explotación que buscan redireccionar los flujos de entrada y salida estándares a sockets de red para sistemas operativos Linux.
- Capacidad de proporcionar la protección contra la explotación de vulnerabilidades sin necesidad de tener una conexión a la consola.
- Identificación y prevención de intentos de escalación de privilegios a nivel de Kernel. Esta protección debe de poder ser utilizada en agentes Windows, Mac y Linux.

**Prevención contra malware**

- Utiliza un modelo matemático generado a partir de aprendizaje de máquina para comparar cientos de características de un archivo ejecutable, de manera estática, para determinar si es malicioso. Esta protección debe estar disponible para sistemas operativos Windows y Mac.
- Capacidad de proteger contra shells reversos (reverse shell) y web shell exploits para sistemas operativos Linux.
- Capacidad de prevenir ataques de Cryptomining a partir del

comportamiento del objeto ejecutado.

- Prevención de ejecución de procesos utilizando su hash, de manera que el administrador puede determinar qué aplicaciones pueden ser ejecutadas.
- Capacidad de identificar si la macro contenida en un documento de Word o Excel es maliciosa, sin necesidad de tener que ejecutar la macro ni observar su comportamiento o ejecución, para determinar si es maliciosa.
- Capacidad de identificación y bloqueo de malware basado en reglas de comportamiento de amenazas. Estas reglas deberán estar de forma predeterminada y se deberán actualizar periódicamente por el fabricante.
- Capacidad de poder colocar los malware en una carpeta de cuarentena o eliminarlo.
- Capacidad de realizar escaneos a demanda y programados
- Capacidad de proporcionar protección contra malware sin necesidad de tener una conexión a la consola.
- Capacidad de proporcionar protección contra malware sin necesidad de una BD de firmas o heurística y sin necesidad de una herramienta de sandboxing.
- Debe permitir configurar las políticas en modo de prevención o monitoreo.
- Capacidad de mostrar en una cadena gráfica de eventos la causa raíz que originó el evento malicioso.
- Creación de hashes de procesos en ejecución y verificación de veredictos en una nube de inteligencia de amenazas.
- Opcionalmente deberá ser posible enviar los archivos a un entorno de Sandbox Cloud para ser explotados y generar un informe de análisis de malware.
- Capacidad de enviar los archivos clasificados como maliciosos a cuarentena o eliminarlo ya sea que hayan sido identificados al momento de intentar ejecutarse o al momento de ser identificados mediante un escaneo.
- Cuenta con un módulo de prevención contra ransomware.

**Tecnología de Sandboxing**

- Capacidad de enviar automáticamente los archivos sospechosos para su análisis en un sandbox ubicado en la nube gestionada por el fabricante, con la finalidad de incrementar la capacidad de detección y reportería forense sobre las acciones potenciales que podría realizar el malware.
- 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 garantiza la privacidad y seguridad del contenido de los archivos analizados, para lo cual se requiere que cuente como mínimo con certificaciones SOC2 Tipo II de AICPA y FedRAMP.
- Deberá contar con una acreditación de una entidad independiente del fabricante, que certifique el alineamiento de los controles de seguridad del servicio nube a los estándares HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation) y PCI

(Payment Card Industry Data Security Standard

- Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP, Windows 7, Windows 10, Mac OS X, Linux y Android.
- Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOSX (mach-o, dmg, pkg), Android APKs entre otros.
- 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.
- El sandbox cloud debe poder realizar el análisis en un ambiente de hardware real (bare metal), deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.

**Escaneo de archivos ejecutables.**

- Permite realizar el escaneo de archivos ejecutables
- Permite programar el escaneo de archivos de manera semanal o mensual.
- El consumo de recursos al momento de realizar el escaneo debe de ser mínimo y no debe impactar en la experiencia del usuario.
- Permite habilitar el escaneo de dispositivos de almacenamiento removible.
- Permite crear listas blancas de carpetas para que sean excluidas del proceso de escaneo.
- Permite poner en cuarentena o eliminarlo los archivos identificados como maliciosos, si es que la política está configurada de esta manera.

**Control de dispositivos**

- Debe de permitir generar perfiles que gestionen las siguientes características de bloqueo de puertos USB cuando se conecten los siguientes tipos de dispositivos: discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles con conexión USB, unidades lectoras de discos floppy externas con conexión USB.
- Debe de permitir generar perfiles de excepciones para poder conectar dispositivos en puertos USB utilizando los siguientes parámetros: tipo de dispositivo, tipo de permiso a asignar (lectura/escritura o sólo lectura), fabricante (debe de contener una lista predeterminada), producto (debe de contener una lista predeterminada), y número de serie. Los parámetros tipo de dispositivo.
- Deber permitir la creación de políticas que utilicen los perfiles de bloqueo y de excepciones generados.
- Las políticas generadas deben de poder asignarse a una computadora en particular o a un grupo de computadoras definido previamente.
- Debe de permitir generar perfiles de excepciones para poder conectar dispositivos en puertos USB utilizando los siguientes parámetros: tipo de

dispositivo.

- Debe permitir añadir ClassGuid personalizados para incrementar la cobertura de control de dispositivos.
- Debe de permitir la creación de excepciones temporales a partir de una violación registrada.
- Debe de mostrar las violaciones a las políticas que se hayan registrado mostrando lo siguiente: horario, computadora, usuario, dirección IP, tipo de dispositivo, producto, fabricante y número de serie del dispositivo que intentó conectarse.

**Protección contra el robo de contraseñas.**

- Proporciona una protección predeterminada en memoria contra el uso de la herramienta de extracción de contraseñas Mimikatz.

**Administración y revisión de eventos.**

- Administración de políticas centralizada, vía una consola web basada en nube.
- La consola de administración identifica claramente los eventos que han sido reportados y/o bloqueados y aquellos que han sido detectados.
- Capacidad para clasificar el estado de los incidentes y alertas en cuatro distintos niveles de severidad: alto, mediano, bajo e informacional.
- Capacidad de poder extraer los elementos importantes o relevantes de las alertas, y mostrarlos a manera de resumen en la pantalla de análisis del incidente.
- La consola deberá de proporcionar información detallada bajo demanda de los eventos identificados como exploits.
- Permite la actualización y desinstalación del agente a partir de la consola.
- Permite utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente.
- La integración con Active Directory será opcional para la gestión de computadoras y configuración de políticas.
- Cuenta con la capacidad de asignar acceso en base a roles.
- Cuenta con la capacidad de crear grupos que pueden alimentarse de forma estática o dinámica.
- La alimentación dinámica o estática de los grupos se podrá configurar en base a un prefijo del nombre de la computadora y dirección IP como mínimo.
- Cada evento de prevención o notificación cuenta con información básica como tipo de evento, módulo de la solución que realizó la prevención, detalles de ese módulo, nombre de la computadora, nombre del usuario, sistema operativo, versión del agente, proceso que generó el evento de prevención, ruta de ejecución del proceso que generó el evento de prevención, horario y fecha del evento, hash del archivo u objeto asociado a la amenaza, nombre de la técnica y ataque según el framework de ciberseguridad MITRE ATT&CK.
- Cuenta con un dashboard donde se muestran los incidentes de seguridad que no han sido atendidos (clasificados de acuerdo con su criticidad: alta, media y baja), un resumen sobre los incidentes de seguridad, la cantidad de endpoints que tienen instalado el agente (clasificados por su

plataforma), la cantidad de licencias disponibles y la versión del agente.

- Integración con una plataforma de ciberseguridad la cual incluya una nube de inteligencia y contextualización de amenazas, a través de un API.
- Debe permitir crear excepciones a reglas, mecanismos de detección y/o mecanismos de protección desde la consola. Estas excepciones deben de poder aplicarse a una computadora en específico, o a un grupo de computadoras.
- Capacidad de personalización del dashboard
- Capacidad de almacenar una auditoría de eventos sobre las acciones realizadas en la consola de gestión.
- Capacidad de tomar control remoto de los equipos Windows donde se encuentre instalado el agente, como mínimo deberá ser capaz de: 1) listar procesos, 2) listar carpetas y archivos, 3) ejecutar instrucciones por la línea de comandos y 4) ejecutar instrucciones basados en scripts de Python

**Características del agente**

- Bajo consumo de recursos del equipo, no debe consumir más de 250 MB de memoria RAM
- Soporte para las siguientes versiones de sistemas operativos:
  - Windows 7 (32-bit, 64-bit, RTM & SP1; excepto Home), Windows 8* (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit; FIPS mode), Windows Embedded 8.1 Pro, Windows 10 Pro, Windows 10 Enterprise LTSB, Windows Server 2003* (32-bit, SP2 o posterior), Windows Server 2003 R2 (32-bit, SP2 o posterior), Windows Server 2008 (32-bit, 64-bit; FIPS mode), Windows Server 2008 R2 (32-bit, 64-bit; FIPS mode), Windows Server 2012 (todas las ediciones; FIPS mode), Windows Server 2012 R2 (todas las ediciones; FIPS mode), Windows Server 2016, Windows Server Core option 2012, 2012 R2 y 2016, Windows Server 2016 Datacenter.
  - OSX 10.11 (El Capitan), macOS 10.12 (Sierra), macOS 10.14, macOS 10.15
  - CentOS 6, CentOS 7, Centos 8, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Suse for Enterprise 12.1, Suse for Enterprise 12.2, Oracle Linux 6, 7 y 8, Ubuntu Server 12, Ubuntu Server 14, Ubuntu Server 16, Ubunto 18.
- Soporte para los siguientes ambientes virtuales: VMware ESX, Citrix XenServer, Oracle Virtualbox, Microsoft Hyper-V
- No debe requerir el reinicio del equipo para que agente se encuentre operativo y ofreciendo protección.
- Capacidad para configurar la captura de datos que serán enviados a la nube para su almacenamiento, procesamiento y análisis en una consola de detección y respuesta a incidentes.
- Gestión de usuarios
  - La consola debe permitir la gestión de usuarios mediante roles.
  - La consola debe contar con roles preconfigurados

**Reportes**

- La solución debe tener la capacidad para generar informes de incidentes a nivel de malware y exploit sin la necesidad utilizar una consola diferente.

- El formato de los reportes generados es PDF.
- La consola mantiene un historial de los reportes que han sido generados para su posterior consulta.
- Los reportes podrán ser enviados de forma automática y programada a una o más direcciones de correos electrónicos.
- Debe mostrar como mínimo los siguientes tipos de reportes:
    - Listado de equipos con incidentes detectados
    - Listado de amenazas con mayor recurrencia
    - Severidad o criticidad de las amenazas detectadas
    - Usuarios asignados a la gestión de los incidentes o Usuario que clasificó el evento
    - Sistemas Operativos más afectados
    - reporte general de acciones tomadas por la solución por cada amenaza
    - Categorización de las amenazas de seguridad
    - Identificación de técnica y táctica de ataque de la amenaza.
    - Estado de los agentes instalados
    - Distribución de agentes instalados según sistema operativo

**MÓDULO DE ANALÍTICA, DETECCIÓN Y RESPUESTA AVANZADA Y ANÁLISIS DE COMPORTAMIENTO DE USUARIOS**

Deberán cumplir los siguientes requerimientos:

**Capacidades de Threat Hunting**

- Deberá de poder utilizar los datos capturados por el agente que se utiliza para realizar las tareas de detección e investigación, sin necesidad de utilizar un segundo agente.
- La solución deberá de tener la capacidad de realizar consultas por:
    - Actividad de los archivos, identificando las siguientes operaciones: creación, lectura, eliminación, escritura y renombrar.
    - Actividad de red, identificando el tráfico saliente, entrante, IP origen e IP destino, Puerto origen y Puerto destino, protocolo de red.
    - Actividad en el registro Windows, identificando la creación, eliminación, renombrado, definición de valores, eliminación de valores de las llaves de registro.
    - Actividad de procesos, identificando si se trata de una ejecución o inyección, ruta desde donde se ejecuta, comando que inicializa el proceso, usuario, hash en SHA256 y MD5.
    - Actividad en el Log de Eventos de Windows, identificando la descripción, ID del evento, nivel, mensaje, nombre del proveedor y usuario.
    - Actividad de autenticación al endpoint
- Deberá ser posible hacer búsquedas correlacionando todos los tipos de actividad indicados.
- Todas las búsquedas mencionadas anteriormente deberán de poder programarse para ser ejecutadas en un día y hora determinados por una ocasión, o de manera recurrente ya sea de forma diaria en un horario determinado o algún día de la semana en particular, en un horario en específico.
- Todas las búsquedas deberán de poder ser ejecutadas observando los resultados en tiempo real o permitiendo trabajar al analista mientras la

búsqueda se ejecuta en segundo plano o se debe permitir al analista continuar con su análisis en una ventana aparte.

- Deberá de contar con un dashboard que permita visualizar alertas generadas de distintas fuentes.
- El dashboard o consola de administración deberá de mostrar los siguientes datos de contar con varias columnas:
  - Timestamp
  - Nombre de la computadora
  - Nombre de usuario
  - Severidad
  - Fuente de la alerta
  - Si la alerta constituye una detección o un bloqueo.
  - Categoría de la detección
  - Nombre de la alerta
  - Descripción
  - Proceso que lo inició
  - Línea de comando del proceso que lo inició
  - Firma del proceso que lo inició
  - Nombre de la entidad que firmó el proceso
  - Nombre del proceso que generó la alerta
  - Comando del proceso que generó la alerta
  - Firma del proceso que generó la alerta
  - Nombre de la entidad que firmó el proceso que generó la alerta
  - Identificador de la alerta
  - IP del host
  - Tipo de evento
  - Ruta del archivo
  - Valor MD5 del archivo
  - Valor SHA256 del archivo
  - Valor del registro
  - Llave completa del registro
  - IP local
  - Puerto local
  - Host remoto
- Deberá de poder mostrar el número total de alertas, incluyendo la cantidad de alertas que resultan de aplicar un filtro, y poder almacenar dicho filtro.
- El producto deberá implementar un menú contextual que permita analizar de manera detallada la alerta, generar una línea de tiempo, editar una regla, eliminar una alerta, copiar el URL de una alerta y copiar la alerta. Se aceptará también que el producto ofrezca una vista detallada de la alerta que incluya una linea de tiempo e información contextual de la alerta.
- El timeline del ataque deberá mostrar el intento de ataque en diferentes fases de explotación acorde al Framework MITRE, tales como Ejecución, Persistencia, Descubrimiento, Desplazamiento Lateral, Command & Control, Exfiltración.
- El producto deberá de mostrar el nombre de la computadora, su dirección IP, el nombre del proceso que generó la alerta y el número de la alerta en la parte superior para que el analista pueda consultarla con facilidad.

**Análisis de alertas e investigación de actividad sospechosa**

- El producto deberá implementar un menú contextual que permita analizar de manera detallada la alerta, generar una línea de tiempo. También se aceptará también que el producto ofrezca una vista detallada de la alerta que incluya una linea de tiempo e información contextual de la alerta.
- El producto deberá genere una advertencia o alarma cuando un ejecutable realice un comportamiento sospechoso o de riesgo, sea parte o no de un ataque ya reconocido
- El producto deberá de mostrar datos generales de la ejecución de un proceso que forme parte de la secuencia gráfica, entre los que se encuentran ruta de ejecución, nombre de usuario que ejecutó el proceso, tiempo de su ejecución, entidad que firmó el proceso, valor MD5 del ejecutable relacionado con el proceso, veredicto del análisis del sandbox, valor SHA256 y línea de comandos de la ejecución.
- El producto deberá de mostrar la actividad de cada proceso identificado, en columnas por categorías. Entre las categorías a incluir debe de estar la actividad de red, actividad de los archivos, actividad del registro, módulos ejecutados e intentos de inyección a procesos.
- El producto deber a de poder identificar, de todas las actividades mencionadas anteriormente, aquellas que sean maliciosas o altamente sospechosas y separarlas en una categoría de fácil acceso para el analista.
- Para cada una de las actividades mencionadas anteriormente el producto deberá de desplegar los siguientes datos en columnas: fecha, nombre de la computadora, IP del host que generó la alerta, nombre de usuario, sistema operativo del host, tipo de actividad identificada, descripción de la actividad identificada, nombre del archivo asociado, nombre previo del archivo, ruta del archivo, ruta anterior del archivo, valor MD5 del archivo, valor SHA256 del archivo, ruta del archivo que fue el ejecutor del archivo, comando que utilizó el ejecutor del archivo, identificador del proceso que fue el ejecutor del archivo, valor MD5 del ejecutor del archivo que fue la causa raíz de la alerta, valor SHA256 del ejecutor del archivo que fue la causa raíz de la alerta, indicador sobre si el ejecutor de la alerta está firmado, ruta del archivo que fue la causa raíz de la alerta, comando del archivo que fue la causa raíz de la alerta, valor SHA 256 del archivo que fue la causa raíz de la alerta.
- Deberá mostrar en un mapa geográfico la actividad de red saliente y entrante, mostrando la información de la IP en investigación en base a un rango de fechas, endpoints afectados y datos enriquecidos con alguna fuente externa de Threat Intelligence.

V°B° Y SELLO
REPRESENTANTE DEL ÁREA
USUARIA