

# BASES ESTÁNDAR DE LICITACIÓN PÚBLICA PARA LA CONTRATACIÓN DE BIENES

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



Organismo  
Supervisor de las  
Contrataciones  
del Estado

*[Handwritten signature]*

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

*[Handwritten signature]*

*[Handwritten signature]*

### 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  | <b>Importante</b><br>• Abc                 | Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.   |
| 4  | <b>Advertencia</b><br>• Abc                | Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.  |
| 5  | <b>Importante para la Entidad</b><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:

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

Elaboradas en enero de 2019

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

## **BASES ESTÁNDAR DE LICITACIÓN PÚBLICA PARA LA CONTRATACIÓN DE BIENES**

**LICITACIÓN PÚBLICA N°  
014-2023-MML-OGA-OL**

### **CONTRATACIÓN DE BIENES**

**“ADQUISICIÓN DE LICENCIAS DE PLATAFORMA DE PROTECCIÓN  
DE ENDPOINTS PARA LA MUNICIPALIDAD METROPOLITANA DE  
LIMA “**



## 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.

PA  
Haro  
my



## **SECCIÓN GENERAL**

### **DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN**

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

*P-4*  
*H. M. C.*  
*Q. P.*

## CAPÍTULO I ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

### 1.1. REFERENCIAS

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

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

### 1.2. CONVOCATORIA

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

### 1.3. REGISTRO DE PARTICIPANTES

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

#### Importante

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

### 1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

#### Importante

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

PR  
H  
AM

### 1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

#### Importante

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

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

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

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

#### Advertencia

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

#### Importante

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

### 1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales<sup>1</sup>). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

#### Importante

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



- *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 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 funcionales y condiciones de las Especificaciones Técnicas, detalladas 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.

*[Handwritten signatures and initials in blue ink]*



#### 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.

Handwritten signatures and initials in blue ink.

### CAPÍTULO III DEL CONTRATO

#### 3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

#### 3.2. GARANTÍAS

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

##### 3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

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

En las contrataciones que conllevan la ejecución de prestaciones accesorias, tales como mantenimiento, reparación o actividades afines, se otorga una garantía adicional por una suma equivalente al diez por ciento (10%) del monto del contrato de la prestación accesorio, la misma que debe ser renovada periódicamente hasta el cumplimiento total de las obligaciones garantizadas.

##### Importante

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

##### 3.2.3. GARANTÍA POR ADELANTO

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

#### 3.3. REQUISITOS DE LAS GARANTÍAS

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



#### Importante

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

#### Advertencia

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

1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (<http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo>).
2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.
3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.
4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.

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

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

Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.

#### 3.4. EJECUCIÓN DE GARANTÍAS

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

#### 3.5. ADELANTOS

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

#### 3.6. PENALIDADES

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

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



### 3.6.2. OTRAS PENALIDADES

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

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

### 3.7. INCUMPLIMIENTO DEL CONTRATO

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

### 3.8. PAGOS

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

La Entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los bienes, 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.

P-4  
H. C.  
C. P.

## **SECCIÓN ESPECÍFICA**

### **CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN**

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

*[Handwritten signatures in blue ink]*

## CAPÍTULO I GENERALIDADES

### 1.1. ENTIDAD CONVOCANTE

Nombre : Municipalidad Metropolitana de Lima  
RUC N° : 20131380951  
Domicilio legal : Jr. Conde de Superunda 141 – Cercado de Lima  
Teléfono: : 016321300 – Anexo 1874  
Correo electrónico: : cesar.manyari\_0@munlima.gob.pe

### 1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación de la ADQUISICIÓN DE LICENCIAS DE PLATAFORMA DE PROTECCIÓN ENDPOINTS PARA LA MUNICIPALIDAD METROPOLITANA DE LIMA

| N° | DESCRIPCIÓN   | UNIDAD DE MEDIDA | CANTIDAD |
|----|---|------------------|----------|
| 1  | ADQUISICIÓN DE LICENCIAS DE PLATAFORMA DE PROTECCIÓN ENDPOINTS PARA LA MUNICIPALIDAD METROPOLITANA DE LIMA. | Unidad           | 3,200    |

#### PRESTACIÓN ACCESORIA

El plazo de la prestación accesoria consiste en el mantenimiento y soporte técnico, y será de la siguiente manera:

- **EL MANTENIMIENTO Y SOPORTE:** Deberá ser por un periodo de 1095 días calendarios (36 meses), a partir del día siguiente de la suscripción del acta de finalización de la implementación y puesta en funcionamiento.

### 1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante formato S/N el 08 de noviembre del 2023.

### 1.4. FUENTE DE FINANCIAMIENTO

Recursos Determinados.

#### **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. MODALIDAD DE EJECUCIÓN

Llave en mano.

#### 1.7. DISTRIBUCIÓN DE LA BUENA PRO

No aplica.

#### 1.8. ALCANCES DEL REQUERIMIENTO

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

#### 1.9. PLAZO DE ENTREGA

Los bienes materia de la presente convocatoria se entregarán en el plazo de TREINTA Y SIETE (37) días calendario, de acuerdo a lo siguiente:

**ENTREGA:** La entrega de las 3,200 licencias se realizará en el plazo de siete (07) días calendario, contados a partir del día siguiente de suscrito el contrato y será en el Área de Almacenamiento y Distribución.

**IMPLEMENTACIÓN, PUESTA EN FUNCIONAMIENTO Y CAPACITACIÓN:** Será dentro de los Treinta (30) días calendario contados a partir del día siguiente de la entrega de las licencias.

##### PRESTACIÓN ACCESORIA

El plazo de la prestación accesoria consiste en el mantenimiento y soporte técnico, y será de la siguiente manera:

**EL MANTENIMIENTO Y SOPORTE:** Deberá ser por un periodo de 1095 días calendarios (36 meses), a partir del día siguiente de la suscripción del acta de finalización de la implementación y puesta en funcionamiento.

En concordancia con lo establecido en el expediente de contratación.

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

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/ 5.00 (Cinco con 00/100 SOLES) en la Caja de la Entidad, sito en el Área de Tramite Documentario en el Hospicio Manrique pasaje Acisclo Villarán N° 288-294, Cercado de Lima, altura de la Plaza Francia, (CODIGO 636). El ejemplar de las Bases se entregará en la Oficina de Logística de la Municipalidad Metropolitana de Lima, sito en Jr. Conde Superunda N° 141, Cercado de Lima, en el horario de 08:30 a 1:00 horas y de 14:00 a 16:30 horas.

##### Importante

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

#### 1.11. BASE LEGAL

- Decreto Legislativo N° 1440 – Decreto Legislativo del Sistema Nacional de Presupuesto Público
- Ley N° 31638 Ley de Presupuesto del Sector Público para el Año Fiscal 2023.
- Ley N° 31639 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2023.
- Ley N° 29783 - Ley de Seguridad y Salud en el Trabajo.
- Decreto Supremo N° 005-2012-TR - Reglamento de la Ley de Seguridad y Salud en el Trabajo.
- Ley N° 26842- Ley General de Salud.
- Decreto de Urgencia N° 044-2019, que establece medidas para fortalecer la protección de salud y vida de los trabajadores.
- TUO de la Ley N° 30225, Ley de Contrataciones del Estado, en adelante la Ley.
- Decreto Supremo N° 308-2022-EF, que modifica el Reglamento de la Ley N° 30225, Ley de



Contrataciones del Estado, aprobado mediante Decreto Supremo N° 344-2018-EF.

- Directivas del OSCE.
- Ley N° 27444, Ley de Procedimiento Administrativo General.
- Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública
- Ley N° 27972, Ley Orgánica de Municipalidades y sus modificaciones.
- Código Civil.
- 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.

### 2.2. CONTENIDO DE LAS OFERTAS

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

#### 2.2.1. Documentación de presentación obligatoria

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

- a) Declaración jurada de datos del postor. **(Anexo N° 1)**
- b) Documento que acredite la representación de quien suscribe la oferta.  
  
En caso de persona jurídica, copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto.  
  
En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda.  
  
En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.
- c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. **(Anexo N° 2)**
- d) Declaración jurada de cumplimiento de las Especificaciones Técnicas contenidas en el numeral 3.1 del Capítulo III de la presente sección. **(Anexo N° 3)**
- e) Carta y/o documentos emitidos por el fabricante o representante local del fabricante, en el que se indique que el postor está autorizado a comercializar, instalar y dar soporte al bien solicitado.
- f) Declaración jurada de plazo de entrega. **(Anexo N° 4)<sup>3</sup>**
- g) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)**
- h) El precio de la oferta en Soles. Adjuntar obligatoriamente el **Anexo N° 6**.  
El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales. Los precios unitarios pueden ser expresados con más de dos (2) decimales.

#### Importante

*El comité de selección verifica la presentación de los documentos requeridos. De no cumplir con lo requerido, la oferta se considera no admitida.*

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

<sup>3</sup> En caso de considerar como factor de evaluación la mejora del plazo de entrega, el plazo ofertado en dicho anexo servirá también para acreditar este factor.

### 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.

#### Advertencia

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

### 2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

- a) Garantía de fiel cumplimiento del contrato.
- b) Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso.
- c) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.
- d) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
- e) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.
- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación<sup>4</sup> (**Anexo N° 11**).
- i) Detalle de los precios unitarios del precio ofertado<sup>5</sup>.
- j) Números de teléfono y correo electrónico de la central de atenciones.
- k) Correo electrónico para efectos de la notificación durante la ejecución del contrato.
- l) Copia del Título profesional que acredite la formación académica solicitada para el Jefe de Proyecto.
- m) Copia del Título técnico que acredite la formación requerida para el personal técnico.
- n) Copia de los certificados de capacitación, donde se acredite el número de horas lectivas, para el personal clave.
- o) Copia del certificado en el uso y administración de la Plataforma de Protección Endpoints propuesto, emitido por el fabricante, del Jefe de Proyecto y Personal Técnico.
- p) Copia de la Póliza de Seguro Complementario de Trabajo de Riesgo (SCTR).

#### Importante

- *En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y en el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva “Participación de Proveedores en Consorcio en las Contrataciones del Estado”.*
- *En los contratos 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.*

<sup>4</sup> En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

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



#### Importante

- *Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.*
- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya<sup>6</sup>.*
- *La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

#### 2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en mesa de partes virtual o mesa de partes física de la Municipalidad Metropolitana de Lima, ubicada en Hospicio Manrique, entrada por el pasaje Acisclo Villarán N° 288-294, Cercado de Lima, altura de la Plaza Francia, en el horario de lunes a viernes de 08:30 a 13:00 horas y de 14:00 a 16:00 horas, dirigida a la Oficina de Logística. En caso corresponda hacer entrega de documentos originales, la documentación solo podrá ser presentada a través de mesa de partes física, en la dirección antes mencionada.

#### 2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista según el siguiente detalle:

##### PRESTACIÓN PRINCIPAL

La Entidad efectuará el pago de la prestación principal en PAGO ÚNICO.

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

- Recepción del Área de Almacenamiento y Distribución, a través de la guía de remisión.
- Conformidad emitida por el responsable de la Oficina de Gobierno Digital, previo informe técnico del responsable del Departamento de Redes, Infraestructura y Seguridad TI.
- Comprobante de Pago.
- Entregable del Contratista.

##### PRESTACIÓN ACCESORIA

##### **Soporte y mantenimiento:**

La Entidad efectuará el pago a favor del contratista en forma mensual.

$$\text{Valor mensual} = \text{Costo total de la prestación accesoria} / 36$$

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

- Conformidad emitida por el responsable de la Oficina de Gobierno Digital, de forma mensual (36 meses) previo informe técnico del responsable del Departamento de Redes, Infraestructura y Seguridad TI.
- Comprobante de Pago.
- Entregable del Contratista.

<sup>6</sup> Según lo previsto en la Opinión N° 009-2016/DTN.



Dicha documentación (Prestación Principal y Accesorio) deberá ser presentada por mesa de partes virtual o mesa de partes física de la Municipalidad Metropolitana de Lima, ubicada en Hospicio Manrique, entrada por el pasaje Acisclo Villarón N° 288-294, Cercado de Lima, altura de la Plaza Francia, en el horario de lunes a viernes de 08:30 a 13:00 horas y de 14:00 a 16:00 horas, dirigida a la Oficina de Logística. En caso corresponda hacer entrega de documentos originales, la documentación solo podrá ser presentada a través de mesa de partes física, en la dirección antes mencionada.

Per  
Hern

Op

## CAPÍTULO III REQUERIMIENTO

### 3.1. ESPECIFICACIONES TÉCNICAS



OFICINA GENERAL DE ADMINISTRACIÓN  
Oficina de Gobierno Digital

#### REQUERIMIENTO

#### I. ESPECIFICACIONES TÉCNICAS

##### 1. DENOMINACIÓN DE LA CONTRATACIÓN

ADQUISICIÓN DE LICENCIAS DE PLATAFORMA DE PROTECCIÓN ENDPOINTS PARA LA MUNICIPALIDAD METROPOLITANA DE LIMA.

##### 2. FINALIDAD PÚBLICA

La adquisición de las "Licencias de Plataforma de Protección Endpoints para la Municipalidad Metropolitana de Lima (MML)" permitirá proporcionar protección integral para Endpoints que incluye protección antivirus y antimalware, firewall y prevención de intrusiones, protección web y de red, y seguridad del correo electrónico a los sistemas de información y mitigar los riesgos de amenazas informáticas de acceso no autorizado a la información de la institución, garantizando la continuidad de los servicios informáticos que se brinda a los usuarios de la MML y a los ciudadanos de Lima Metropolitana.

##### 3. ANTECEDENTES

Actualmente la Municipalidad Metropolitana de Lima, cuenta con licencias de antivirus vigentes las cuales fueron adquiridas con Contrato N° 123-2022-MML-GA-SLC, cuya activación y soporte de las licencias de antivirus vence el 20/12/2023.

La Municipalidad Metropolitana de Lima, actualmente cuenta con 20 sedes conectadas a la red LAN y periféricos que se conectan con acceso VPN para uso de los servicios informáticos que brinda la MML, las cuales cuentan con equipos de cómputo que suman un total de 3200 equipos, por tal razón la Oficina de Gobierno Digital requiere adquirir 3200 licencias de Plataforma de Protección Endpoints para evitar la vulnerabilidad e infección de virus en la red de la entidad.

##### 4. OBJETIVO DE LA CONTRATACIÓN

Adquirir licencias de Plataforma de Protección Endpoints para la Municipalidad Metropolitana de Lima (MML), que permita brindar seguridad a las estaciones de trabajo, servidores físicos y virtuales y dispositivos móviles ante las amenazas de virus informáticos, para minimizar los ataques informáticos, accesos no autorizados y alteración de la información.

##### 5. ALCANCE Y DESCRIPCIÓN DE LOS BIENES A CONTRATAR

La Municipalidad Metropolitana de Lima requiere adquirir un total de tres mil doscientos (3.200) licencias de Plataforma de Protección Endpoints como se detalla a continuación:

| N° | DESCRIPCION   | UNIDAD DE MEDIDA | CANTIDAD |
|----|---|------------------|----------|
| 1  | ADQUISICIÓN DE LICENCIAS DE PLATAFORMA DE PROTECCIÓN ENDPOINTS PARA LA MUNICIPALIDAD METROPOLITANA DE LIMA. | Unidad           | 3.200    |

## 5.1. PRESTACIÓN PRINCIPAL: CARACTERÍSTICAS Y CONDICIONES

### 5.1.1. CARACTERÍSTICAS TÉCNICAS:

#### **CARACTERÍSTICAS DE LA SOLUCIÓN DE ENDPOINT PARA ESTACIONES DE TRABAJO**

- Deberá soportar estaciones de trabajo y portátiles Windows y Mac, cuyos sistemas operativos cuenten con soporte por parte del fabricante.
- Deberá proteger contra virus, troyanos, macrovirus, adware, spyware, gusanos, rootkits y todo tipo de programa malicioso (malware) incluyendo la protección contra ransomware
- Deberá contar con un módulo contra ransomware, que realice el bloqueo de amenazas de día cero y ataques de ransomware como Locky, WannCry, Petya, entre otros, sin requerir la actualización de firmas.
- El módulo contra ransomware deberá monitorear y bloquear cambios no autorizados en el Endpoint como cifrados masivos, cambios en el sistema, modificación de llaves en el registro o creación de archivos y carpetas en áreas no autorizadas del sistema operativo.
- La solución deberá contar con tecnologías de detección proactiva de amenazas conocidas y basadas en la nube (in the cloud) del mismo fabricante. Vigilia proactiva ante amenazas del día cero, exploits y entre otros.
- Deberá integrar dos motores antimalware para una mejor protección y como doble capa de protección antimalware. El motor principal deberá ser del fabricante de la solución propuesta y el secundario de un tercero. Ambos motores deberán funcionar al mismo tiempo para una óptima protección.
- Deberá incorporar un módulo de protección basado en la nube el cual deberá tener acceso rápido a las amenazas nuevas directamente desde el laboratorio del fabricante.
- Deberá permitir bloquear amenazas en base a indicadores de compromiso (IoCs) como máximo luego de 5 minutos de ser aplicadas en la consola.
- Deberá analizar el tráfico web y eliminar el malware detectado, así mismo, en caso el análisis tome más de 1 minuto deberá poder mostrar un indicador de progreso de análisis.
- Deberá detectar la presencia de Botnets en la LAN analizando el tráfico generado por consultas DNS en el host, así como ransomware y ATP.
- Deberá analizar las unidades de red.
- Deberá analizar archivos comprimidos (zip, arj, lzh, tar, gz, entre otros).
- Deberá permitir realizar exclusiones de archivos, extensiones, carpetas y unidades tanto para el modo de escaneado en tiempo real como manual.
- Deberá permitir realizar exclusiones de procesos tanto para el modo de escaneado en tiempo real como manual.
- Deberá permitir el bloqueo de cookies de seguimiento de la navegación de los usuarios creado por los navegadores.
- Deberá incluir un módulo que revise la reputación de los archivos en tiempo real con la finalidad de detectar en tiempo real malware sospechoso o desconocido.
- Deberá evaluar amenazas usando técnicas de monitoreo de los procesos sospechosos inyectando ya sea una DLL de monitoreo o integrando una mini máquina virtual que rastree y monitoree el comportamiento de los procesos.
- Deberá contar con opciones para incluir o excluir programas que puedan ser detectados como comportamiento sospechoso como los instaladores de aplicaciones internas, actualizadores de programas u otras aplicaciones. La exclusión deberá



poder realizarse usando el hash SHA-1 de la aplicación el cual podrá ser marcado como confiable o No confiable.

- Deberá permitir realizar el análisis manual de los archivos pudiendo configurarse ya sea para todos los archivos o para determinadas extensiones de archivos.
- Deberá permitir realizar acciones sobre el malware detectado ya sea para informar, desinfectar, eliminar, renombrar, preguntar por la acción al usuario o enviar a la cuarentena tanto para el escaneado en tiempo real como para el escaneado manual.
- Deberá poder realizar el análisis manual ya sea en prioridad normal o en segundo plano con la finalidad de no interrumpir las labores de los usuarios.
- Deberá incluir un módulo para el control de aplicaciones que permita controlar la ejecución de ciertas aplicaciones en el equipo del usuario.
- Deberá permitir crear reglas en base al origen y destino del archivo en base a su ubicación, SHA1, SHA256, prevalencia, reputación, nombre del archivo, versión del archivo, descripción del archivo, nombre del producto, fabricante, por derechos de autor, nombre del signatario, si contiene una firma verdadera, por tipos de nombre y extensión y por la línea de comandos que ejecuta la aplicación.
- Deberá permitir crear notas de las reglas de detección creadas con el fin de contar con una bitácora de consultas.
- Deberá contar con una opción para habilitar o desactivar una regla de control de aplicaciones.
- Deberá permitir reglas comparando si los datos de la aplicación "inicia con", "es igual a", "no es igual a", "contiene", "inicia con", "finaliza con", pudiendo además usar una combinación de estas en una sola regla.
- Deberá permitir crear reglas en base a indicadores de compromiso (IoCs) de terceros.
- Deberá permitir crear una regla global para el monitoreo del uso de aplicaciones.
- Deberá permitir crear una regla global para bloquear aplicaciones no confiables que sean detectadas por el sistema de reputación de archivos del fabricante.
- Deberá incluir reglas predefinidas por el fabricante o por el proveedor que permitan:
  - Bloquear archivos maliciosos que se alojen en la carpeta temp.
  - Bloquear archivos raros y desconocidos que se alojen en la carpeta temp.
  - Bloquear DLLs maliciosas que se alojen en la carpeta temp.
  - Bloquear DLLs con reputación desconocida que se alojen en la carpeta temp.
  - Bloquear archivos maliciosos que se alojen en la carpeta descargas.
  - Bloquear archivos raros y desconocidos que se alojen en la carpeta descargas.
  - Bloquear DLLs maliciosas que se alojen en la carpeta descargas.
  - Bloquear DLLs con reputación desconocida que se alojen en la carpeta descargas.
  - Bloquear el inicio de archivos de batch y/o scripts por parte de aplicaciones de Ofimática de Microsoft como Word, Excel, Power Point, entre otros.
  - Bloquear el inicio de archivos de Powershell por parte de aplicaciones de Ofimática de Microsoft como Word, Excel, Power Point, entre otros.
- Las reglas que se creen deben basarse en eventos como:
  - Inicio de una aplicación.
  - Carga de un módulo DLL.
  - Inicio de instalación.
  - Acceso al archivo exe.
  - Inicio de una aplicación y carga de un módulo DLL.
- Las acciones que debe incluir como mínimo son "Permitir", "Bloquear", "Permitir y Monitorear".
- Cada regla creada deberá tener una descripción para el adecuado seguimiento de la creación y/o ejecución del mismo.
- Deberá integrarse con AMSI de Microsoft y/o Mac.
- Deberá preguntar al usuario si desea escanear una unidad extraíble (USB, Disco Externo) cuando conecta al equipo.

PA  
Hincio  
Am

- Deberá permitir configurar en los perfiles la posibilidad de acceder a las versiones de la solución próximas a lanzarse con el fin de evaluar su funcionamiento y operatividad con las aplicaciones internas de la institución.
- Deberá permitir configurar las actualizaciones en modo HTTP y HTTPS según lo requiera el administrador de la solución.
- Deberá permitir configurar una contraseña de acceso a la cuarentena de los puntos finales.
- Deberá permitir configurar la cantidad de tiempo en la que los archivos en cuarentena serán automáticamente eliminados.
- Deberá incluir un módulo de protección en la navegación web el cual deberá permitir asegurar la navegación realizando las siguientes acciones:
  - Navegación basada en la reputación de los sitios web, permitiendo bloquear el acceso a un sitio web clasificado como inseguro.
  - La reputación de sitios deberá realizarse mediante consultas a la nube de seguridad del fabricante.
  - Reforzamiento de las búsquedas o modo SafeSearch.
  - Deberá mostrar las reputaciones de los sitios web en los resultados de búsqueda en sitios como Google, Yahoo, Bing, entre otros.
  - Permitir al usuario continuar la navegación en páginas bloqueadas la misma que debe poder ser desactivada centralmente.
  - Deberá permitir crear sitios de confianza a los cuales podrán navegar los usuarios sin necesidad de consultar la reputación de estos. La creación deberá admitir dominios completos (p.e. ejemplo.com) y sub-dominios (p.e. www.ejemplo.com).
  - Deberá permitir crear sitios no permitidos a los cuales los usuarios no podrán navegar sin necesidad de consultar la reputación de estos. La creación deberá admitir dominios completos (p.e. ejemplo.com) y sub-dominios (p.e. www.ejemplo.com).
  - Deberá tener una opción para bloquear todos los sitios excepto los indicados por el administrador.
- Deberá incluir un módulo para el control de contenido web pudiendo realizar las siguientes acciones:
  - Bloqueo de la navegación en sitios de categorías específicas.
  - Incluir al menos 32 categorías de sitios web predefinidas como aborto, publicidad, adulto, alcohol, anonimizadores, subastas, banca, blogs, chat, citas, drogas, entretenimiento, apuesta juegos, piratería, odio, búsqueda de trabajo, servicios de pago, estafa, compras en línea, redes sociales, descargas de software, spam, medios de transmisión, violencia, warez, armas, correo web, P2P, entre otros.
  - Filtrar el tipo de contenido que los usuarios pueden descargar desde el internet pudiendo realizar reglas de bloqueo por tipo de archivo (p.e. application/x-executable) y por extensión (p.e \*.exe).
- Deberá incluir un módulo para el control de conexiones o protector de navegación el cual deberá permitir proteger la navegación de los usuarios a sitios de banco, sitios de comercio electrónico y sitios confiables que se definan mediante el protocolo HTTPS con la finalidad de evitar el phishing o robo de datos a los usuarios.
- Deberá controlar las conexiones o protector de navegación deberá también permitir activar o desactivar las siguientes acciones:
  - No interrumpir las conexiones activas.
  - Borrar el portapapeles al cerrar la conexión.
  - Bloquear la ejecución de herramientas de línea de comandos y herramientas de scripting.
  - Bloquear el acceso remoto cuando esté activo esta protección con el fin de evitar el acceso no autorizado y la pérdida de datos.



- Deberá permitir gestionar los cortafuegos de Windows que permita bloquear el tráfico malicioso en la LAN. Este módulo deberá:
  - Incluir un IPS a nivel de host o HIPS.
  - Bloquear fragmentos de IP basados en el tamaño definido en la consola de gestión.
  - Permitir el filtrado de tráfico IPV6.
  - Permitir configurar tarjetas de red confiables.
  - Desactivar el firewall de Windows automáticamente.
  - Aplicar política de firewall del propio fabricante para evitar y parar ataques laterales.
  - Incluir al menos 5 tipos de perfiles predefinidos por el fabricante con las mejores prácticas de seguridad informática, así como con una opción para seleccionar el perfil automáticamente en base a reglas como:
    - IP del Servidor DNS
    - IP del Servidor DHCP
    - IP del Gateway del equipo
    - Segmento LAN y la combinación de todas ellas.
  - Deberá permitir la creación de nuevos perfiles.
  - Incluir reglas de cortafuegos predefinidas para bloquear el tráfico de malware usado para ataques laterales en una red LAN. Estas reglas deberán ser actualizadas y mantenidas por el fabricante.
  - Permitir añadir reglas personalizadas en los diferentes perfiles predefinidos.
  - Permitir activar o desactivar una regla definida.
  - Deberá permitir crear reglas para la cuarentena o aislamiento de equipos basado en un editor de reglas incorporado en la solución. Además, deberá permitir definir la lista de dominios de internet que serán accesibles durante este proceso.
- Deberá incluir un módulo para la protección contra vulnerabilidades y actualizaciones de software (parches) multifabricante centralizada que deberá permitir:
  - Detectar automáticamente, mediante programación y al inicio del equipo la lista de aplicaciones vulnerables y con actualizaciones pendientes.
  - Deberá permitir mostrar y ocultar la interfaz en el punto final donde el usuario final y/o administrador pueda ver la lista de aplicaciones vulnerables y con actualizaciones pendientes.
  - Configurar la prioridad del análisis (Normal y en segundo plano).
  - Configurar tareas automáticas para la instalación de las correcciones a las vulnerabilidades o parches según su tipo (Críticas, Importantes y Todos). Así mismo, deberá contener un programador de tareas completo que permita la gestión de la programación por día, día de la semana, horario, fecha específica y otros).
  - Permitir excluir aplicaciones.
  - Deberá contar con opciones para obligar y/o permitir el reinicio del equipo en caso de ser necesario para aplicar una corrección de una vulnerabilidad y/o parche.
  - Deberá permitir la integración con el WSUS para actualizaciones de Microsoft.
  - Deberá permitir activar o desactivar las opciones de notificación al usuario.
- Deberá incluir un módulo para la protección de dispositivos de almacenamiento extraíble el cual deberá:
  - Crear políticas para permitir, bloquear la escritura y bloquear el acceso a los dispositivos.
  - Permitir o bloquear la ejecución de binarios almacenados en el dispositivo (.exe, .bat, .com, etc) con la finalidad de evitar la entrada de malware desde dispositivos desconocidos a la red.
  - Detectar dispositivos de tipo:



- USB Mass Storage
- Wireless
- DVD/CD-ROM
- Windows CE ActiveSync
- Floppy Drives
- Modems
- COM & LTP
- Impresoras
- Lectores de Smart Cards
- Cámaras y Scanners
- IrDA
- Bluetooth
- Controladores de Bus IEEE 1394

#### **CARACTERÍSTICAS DE LA SOLUCIÓN DE ENDPOINT PARA SERVIDORES FÍSICOS Y VIRTUALES.**

- Deberá soportar los sistemas operativos de servidor Microsoft Windows, 2012, 2016, 2019, 2022, Citrix, Terminal Server, VMware y Hyper-V, AlmaLinux 8+, Amazon Linux 2+, CentOS 7.3+, 8+, CentOS Stream 8, Debian 9+, Oracle Linux 7.3+, Suse Linux Enterprise 12, 15 y Ubuntu 16.04, 18.04 y 20.04.
- Deberá proteger contra virus, troyanos, macrovirus, adware, spyware, gusanos, rootkits y todo tipo de programa malicioso (malware) incluyendo la protección contra ransomware.
- Deberá contar con un módulo contra ransomware que realice el bloqueo de amenazas de día cero y ataques de ransomware como Locky, WannCry, Petya, entre otros, sin requerir la actualización de firmas.
- El módulo contra ransomware deberá monitorear y bloquear cambios no autorizados en el endpoint como cifrados masivos, cambios en el sistema, modificación de llaves en el registro o creación de archivos y carpetas en áreas no autorizadas del sistema operativo.
- La solución deberá contar con tecnologías de detección proactiva de amenazas conocidas y basadas en la nube (in the cloud) del mismo fabricante. Vigilia proactiva ante amenazas del día cero, exploits.
- Deberá integrar dos motores antimalware para una mejor protección y como doble capa de protección antimalware. El motor principal deberá ser del fabricante de la solución propuesta y el secundario de un tercero. Ambos motores deberán funcionar al mismo tiempo para una óptima protección.
- Deberá incorporar un módulo de protección basado en la nube el cual deberá tener acceso rápido a las amenazas nuevas directamente desde el laboratorio del fabricante.
- Deberá analizar el tráfico web y eliminar el malware detectado, así mismo, en caso el análisis tome más de 1 minuto deberá poder mostrar un indicador de progreso de análisis.
- Deberá detectar la presencia de Botnets en la LAN analizando el tráfico generado por consultas DNS en el host, así como ransomware y ATP.
- Deberá analizar las unidades de red.
- Deberá analizar archivos comprimidos (zip, arj, lzh, tar, gz, entre otros)
- Deberá permitir realizar exclusiones de archivos, extensiones, carpetas y unidades tanto para el modo de escaneado en tiempo real como manual.
- Deberá permitir realizar exclusiones de procesos tanto para el modo de escaneado en tiempo real como manual.
- Deberá permitir el bloqueo de cookies de seguimiento de la navegación de los usuarios creado por los navegadores.

- Deberá integrarse con AMSI de Microsoft.
- Deberá preguntar al usuario si desea escanear una unidad extraíble cuando conecta al equipo.
- Deberá incluir un módulo que revise la reputación de los archivos en tiempo real con la finalidad de detectar en tiempo real malware sospechoso o desconocido.
- Deberá evaluar amenazas usando técnicas de monitoreo de los procesos sospechosos inyectando ya sea una DLL de monitoreo o integrando una máquina virtual que rastree y monitoree el comportamiento de los procesos.
- Deberá contar con opciones para incluir o excluir programas que puedan ser detectados como comportamiento sospechoso como los instaladores de aplicaciones internas, actualizadores de programas u otras aplicaciones. La exclusión deberá poder realizarse usando el hash SHA-1 de la aplicación el cual podrá ser marcado como confiable o No confiable.
- Deberá permitir realizar el análisis manual de los archivos pudiendo configurarse ya sea para todos los archivos o para determinadas extensiones de archivos.
- Deberá permitir realizar acciones sobre el malware detectado ya sea para informar, desinfectar, eliminar, renombrar, preguntar por la acción al usuario o enviar a la cuarentena tanto para el escaneado en tiempo real como para el escaneado manual.
- Deberá poder realizar el análisis manual ya sea en prioridad normal o en segundo plano con la finalidad de no interrumpir las labores de los usuarios.
- Deberá permitir la integración con Microsoft AMSI para el escaneado de malware desde aplicaciones de terceros en forma integrada.
- Deberá permitir configurar el escaneado en baja prioridad con la finalidad de minimizar el uso de recursos en los equipos.
- Deberá incluir un módulo para el control de aplicaciones que permita controlar la ejecución de ciertas aplicaciones en el equipo del usuario.
- Deberá permitir crear reglas en base al origen y destino del archivo en base a su ubicación, sha1, prevalencia, reputación, nombre del archivo, versión del archivo, descripción del archivo, nombre del producto, fabricante, por derechos de autor, nombre del signalario, si contiene una firma verdadera, por tipos de nombre y extensión y por la línea de comandos que ejecuta la aplicación.
- Deberá permitir crear notas de las reglas de detección creadas con el fin de contar con una bitácora de consultas.
- Deberá contar con una opción para habilitar o desactivar una regla de control de aplicaciones.
- Deberá incluir un módulo de protección en la navegación web el cual deberá permitir asegurar la navegación realizando las siguientes acciones:
  - Navegación basada en la reputación de los sitios web permitiendo bloquear el acceso a un sitio web clasificado como inseguro. La reputación de sitios deberá realizarse mediante consultas a la nube de seguridad del fabricante.
  - Deberá mostrar las reputaciones de los sitios web en los resultados de búsqueda en sitios como Google, Yahoo, Bing, entre otros.
  - Permitir al usuario continuar la navegación en páginas bloqueadas.
  - Deberá permitir crear sitios de confianza a los cuales podrán navegar los usuarios sin necesidad de consultar la reputación de los mismos. La creación deberá admitir dominios completos (p.e. ejemplo.com) y sub-dominios (p.e. www.ejemplo.com).
  - Deberá permitir crear sitios no permitidos a los cuales los usuarios no podrán navegar sin necesidad de consultar la reputación de los mismos. La creación deberá admitir dominios completos (p.e. ejemplo.com) y sub-dominios (p.e. www.ejemplo.com).
- Deberá incluir un módulo para el control de contenido web pudiendo realizar las siguientes acciones:



- Bloqueo de la navegación en sitios de categorías específicas.
- Incluir al menos 32 categorías de sitios web predefinidas como aborto, publicidad, adulto, alcohol, anonimizadores, subastas, banca, blogs, chat, citas, drogas, entretenimiento, apuesta juegos, piratería, odio, búsqueda de trabajo, servicios de pago, estafa, compras en línea, redes sociales, descargas de software, spam, medios de transmisión, violencia, warez, armas, correo web, P2P, entre otros.
- Filtrar el tipo de contenido que los usuarios pueden descargar desde el internet pudiendo realizar reglas de bloqueo por tipo de archivo (p.e. application/x-executable) y por extensión (p.e \*.exe).
- Deberá incluir un módulo para el control de conexiones el cual deberá permitir proteger la navegación de los usuarios a sitios de banco y sitios confiables que se definan mediante el protocolo HTTPS con la finalidad de evitar el phishing o robo de datos a los usuarios.
- Deberá incluir un módulo para la protección contra vulnerabilidades y actualizaciones de software (parches) multifabricante centralizada que deberá permitir:
  - Detectar automáticamente, mediante programación y al inicio del equipo la lista de aplicaciones vulnerables y con actualizaciones pendientes.
  - Deberá permitir mostrar y ocultar la interface en el punto final donde el usuario final y/o administrador pueda ver la lista de aplicaciones vulnerables y con actualizaciones pendientes.
  - Configurar la prioridad del análisis (Normal y en segundo plano).
  - Configurar tareas automáticas para la instalación de las correcciones a las vulnerabilidades o parches según su tipo (Críticas, Importantes y Todos). Así mismo, deberá contener un programador de tareas completo que permita la gestión de la programación por día, día de la semana, horario, fecha específica y otros).
  - Permitir excluir aplicaciones.
  - Deberá contar con opciones para obligar y/o permitir el reinicio del equipo en caso de ser necesario para aplicar una corrección de una vulnerabilidad y/o parche.
  - Deberá permitir la integración con el WSUS para actualizaciones de Microsoft.
  - Deberá permitir activar o desactivar las opciones de notificación al administrador.
- Deberá incluir un agente liviano independiente y/o agnóstico del Hypervisor para entornos virtuales permitiendo asegurar los servidores en la nube pública o privada de VMware, Citrix, Hyper-V y KVM. Además, deberá:
  - Reducir el uso de recursos como memoria, CPU, y espacio en disco en máquinas virtuales.
  - Contar con un agente de escaneo liviano
  - Contar con un sistema de protección antimalware basado en la reputación de archivos.

#### **CARACTERÍSTICAS DE LA SOLUCIÓN DE ENDPOINT PARA DISPOSITIVOS MOVILES**

- Deberá soportar la protección proactiva en dispositivos inteligentes y tablets Android, Apple iOS con sistemas operativos vigentes y con soporte de los fabricantes.
- La solución deberá detectar y bloquear malware y detectar posibles vulnerabilidades y mantener el tráfico de la red privada.
- La solución deberá detectar ataques de phishing y sitios web maliciosos.
- La solución deberá tener un módulo anti-seguimiento (anti-tracking) para evitar el seguimiento online por cibercriminales y/o aplicaciones online.



- La solución deberá poder integrarse con productos MDM como AirWatch, IBM MaaS360, Google, Microsoft Intune y MobileIron.

#### CARACTERÍSTICAS DE LA CONSOLA DE ADMINISTRACIÓN CENTRALIZADA

- La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas/reutilizadas en caso que un equipo sea dado de baja o cambiada por obsolescencia tecnológica.
- Deberá soportar la instalación de una Consola Central en Windows 2012, Windows 2012 R2, Windows 2016, 2019, 2022 y Servidores Linux RedHat ES 5,6,7, CentOS 6,7, openSUSE 13.2, Suse LES 10,11, Debian 7,8 y Ubuntu 12.04 o mayor.
- La solución deberá permitir la instalación de diversas Consolas adicionales las cuales podrán instalarse en 8.1, 10 (32/64bits). O en las versiones de servidor Windows 2012, Windows 2012 R2, Windows 2016 y Servidores Linux RedHat ES 5,6,7, CentOS 6,7, openSUSE 13.2, Suse LES 10,11, Debian 7,8 y Ubuntu 12.04 o mayor.
- El instalador de la Consola Central deberá incluir su propio manejador de base de datos y no deberá sobrepasar de 500Mb de tamaño incluyendo todos los componentes necesarios para su instalación y despliegue (Pre-requisitos, Base de datos, Instalador de la Consola) para la óptima distribución en la red.
- Deberá soportar base de datos de terceros como Microsoft SQL Server o MySQL.
- La consola podrá ser también Cloud la misma que deberá cumplir con todas las características técnicas solicitadas.
- La consola deberá mostrar la cantidad de licencias que se usan x día.
- La consola deberá permitir administrar la eliminación automática de equipos que no se conectan a la consola según la cantidad de días indicada.
- La consola deberá permitir realizar la comparación de dos políticas de diferentes perfiles con el fin de realizar una adecuada gestión de las políticas de seguridad corporativas.
- La consola deberá permitir realizar el análisis en la red, en búsqueda de los equipos que no tengan instalada la solución de Plataforma de Protección Endpoints propuesta, usando para ello la conexión automática con las unidades organizativas del directorio activo de la Entidad y equipos con el cliente de la solución de Plataforma de Protección Endpoints propuesta con el fin de llegar a todos los puntos de la red sin necesidad de instalar algún programa o agente adicional. Además, deberá mostrar:
  - Nombre del equipo
  - Fecha de creación en el AD
  - Fecha de último inicio de sesión.
  - Sistema Operativo
  - Ruta en el AD
  - GUID del AD
- La comunicación entre la Consola y los Clientes deberá realizarse mediante un canal seguro como HTTPS o vía Certificados Digitales.
- La Consola Central deberá poder realizar:
  - La gestión centralizada de estaciones y servidores en la red.
  - La configuración de actualizaciones automáticas.
  - La configuración del escaneado en tiempo real.
  - La configuración del escaneado manual.
  - La configuración de la detección de malware y spyware.
  - La gestión de la cuarentena central.
  - La configuración de los niveles de seguridad del firewall personal.
  - La configuración de las reglas de firewall.
  - La configuración de los servicios de firewall.
  - La configuración del control de aplicaciones.
  - La configuración del control de dispositivos
  - La configuración del escaneado de tráfico web.

Pr  
H  
M

- La configuración de la protección de navegación.
- La configuración de políticas de filtrado de contenido por categorías.
- La configuración del envío de alertas por correo o syslog.
- Deberá permitir la gestión centralizada de actualizaciones, siendo la Consola Central el único equipo en poder descargar actualizaciones desde el fabricante y como herramienta de backup se deberá poder configurar políticas para la descarga de actualizaciones en los Endpoint desde el fabricante en caso la Consola Central tenga una falla o se encuentre en mantenimiento.
- Deberá permitir la instalación y desinstalación remota del software en el Endpoint centralizadamente.
- Deberá contar con una Cuarentena de Malware centralizada.
- Deberá permitir la desinstalación de software de terceros al momento de realizarse el despliegue o instalación centralizada de los Endpoints.
- La consola deberá reportar el estado de la red en tiempo real como:
  - Promedio de protección.
  - Estado de las actualizaciones.
  - Estado de la protección de malware
  - Estado de la instalación del endpoint.
  - Propiedad de los equipos como (Hostname, IP, Dominio/Grupo)
- La consola deberá permitir configurar los Endpoint como servidores de actualizaciones usando para ello la tecnología P2P o Neigborcast via el protocolo UDP.
- La consola deberá gestionar el módulo de protección contra vulnerabilidades y parches de software multi-fabricante para estaciones y servidores que deberá:
  - Reportar las actualizaciones faltantes del sistema operativo y aplicaciones de terceros en los equipos de la red.
  - Comparar periódicamente el software instalado en el endpoint e identificar las actualizaciones faltantes y las vulnerabilidades encontradas.
  - Descargar a la Consola Central los paquetes y/o programas necesarios para corregir las vulnerabilidades y parches encontrados con el fin de optimizar el uso de ancho de banda en la red.
  - Contar con una opción para visualizar las vulnerabilidades y actualizaciones pendientes encontradas en la red y que endpoints se encuentran afectadas por cada una de ellas.
  - Contar con una opción para visualizar las vulnerabilidades y actualizaciones pendientes encontradas en la red y por cada endpoint.
  - Permitir enviar mediante una política la actualización centralizada de programas y vulnerabilidades en programas de Microsoft y Sistemas Operativos, Java, Mozilla, Google, Adobe, Services Pack, Winzip, Apple, Sun y otras aplicaciones usadas en entornos corporativos.
  - Permitir la instalación automática y centralizada de actualizaciones, parches y/o correcciones de vulnerabilidades en el sistema operativo y aplicaciones existentes en el endpoint de acuerdo a las políticas definidas por el administrador de la consola.
  - Permitir programar la instalación de actualizaciones según su importancia (Crítico, Crítico y Vulnerable y Todas) en forma centralizada.
  - Permitir programar la instalación automática basado en un día y hora.
  - Analizar el endpoint en búsqueda de aplicaciones vulnerables al inicio del equipo o en según una programación establecida en la consola central.
  - Permitir excluir la instalación de actualizaciones según el tipo de software el cual deberá poder definirse por diversos criterios como:
    - Nombre del producto
    - ID del Bulletin de seguridad del fabricante
    - Service Pack



- Nombre del parche
- Severidad o Gravedad de la actualización
- Descargar las actualizaciones desde la consola central o desde el repositorio más cercano con la finalidad de no consumir el ancho de banda de la institución.
- La consola deberá permitir crear repositorios o consolas distribuidas que gestionen las actualizaciones tanto del producto, firmas de malware y gestionar centralizadamente en cada punto las descargas del módulo del control de vulnerabilidades y parches con la finalidad de minimizar el uso del ancho de banda.
  - Los repositorios de actualizaciones deberán soportar como mínimo los mismos sistemas operativos Windows y Linux que la Consola Central.
- La solución deberá integrarse con el Directorio Activo ya sea para el despliegue como para la configuración de políticas.
- La consola deberá permitir crear tareas automatizadas al menos para:
  - Análisis rápido de malware
  - Análisis programado de malware
  - Permitir la actualización del producto antimalware
  - Realizar análisis de vulnerabilidades y parches multi-fabricante faltantes en el equipo
  - Instalar actualizaciones y corregir vulnerabilidades según tipo: Críticos, críticos e Importantes, de Seguridad y Todos.
  - Enviar a reiniciar, apagar y/o hibernar los equipos.
  - Así mismo el sistema de programación de tareas deberá contar con un programador de tareas para ejecutar por día, días de semana, finales de semana, horas, una vez, en cada reinicio, cuando un software se instale, actualice o elimine, a la media noche y mensual. Asimismo, deberá soportar la creación de múltiples tareas que pueden activarse o desactivar en el perfil creado.
- Permitir configurar mediante una política para evitar desinstalación de los Endpoints aun cuando el usuario en el endpoint tenga privilegios de administrador.
- Deberá contar con un sistema para configurar el producto según la ubicación del equipo ya sea esté en la red, por dirección DNS, por servidor DHCP, por Gateway, por IP Wins, por URL disponible o la combinación de ellas.
- Permitir bloquear y/o desactivar mediante políticas el acceso a las opciones de configuración del Endpoint.
- Deberá tener opciones para realizar acciones rápidas para la contención de malware y ataques de intrusiones como: Aislar equipos de la red, reiniciar equipos, recoger archivos forenses, enviar mensajes a los usuarios y recoger las claves de BitLocker.
- Para la protección contra ataques de ransomware deberá contar con opciones para proteger carpetas y permitir configurar para que únicamente los programas autorizados puedan escribir, modificar y borrar archivos de las mismas.
- Deberá contar con una opción para crear instaladores fuera de línea, es decir, instaladores del tipo click-and-run para la instalación del endpoint en estaciones y servidores con un solo click.
- La consola deberá poder recolectar información de seguridad de los equipos como:
  - Estado del cifrado del disco
  - Fortaleza de la contraseña en los equipos
  - Cuenta invitado, si se encuentra activado o desactivado.
  - Cuenta de administrador, si ha iniciado sesión en el equipo o no.
  - Rastreo de la actividad de la tienda en línea de Microsoft.
- La consola deberá contar con un sistema de visualización de eventos de seguridad generado en los endpoints (estaciones y servidores), el mismo que deberá contener las siguientes opciones:
  - Hora del evento

Por  
Harcio  
an



- Gravedad
- Origen
- Dispositivo afectado
- Descripción del evento
- Detalles como Tipo de alerta, perfil utilizado, ruta del archivo comprometido, SHA-1
- La consola deberá visualizar eventos de seguridad por origen y gravedad para:
  - Control de Aplicaciones
  - Control de Dispositivos
  - Módulo de protección antiransomware, IA y Heurística.
  - Control Web, Tráfico y Contenido Web
  - Módulo antivirus
  - Módulo de verificación de integridad
  - Protección contra manipulaciones
  - Cortafuegos y
  - AMSI de Microsoft
- Deberá incluir protección contra manipulaciones, esta opción permitirá proteger los equipos para evitar que sus procesos, archivos y servicios sean apagados y manipulados.
- La consola deberá agrupar automáticamente los equipos basados en la Ruta del Directorio Activo de los equipos, es decir, no deberá requerir instalar ningún agente en el servidor del AD para que se ejecute este agrupamiento.
- La consola deberá tener una opción permita detectar los equipos en la red que se encuentran sin protección. Esta opción podrá usar el Directorio activo y deberá mostrar la siguiente información:
  - Como nodos de escaneado cualquier equipo con un agente instalado.
  - Nombre del host o equipo detectado
  - Fecha de alta del equipo en el AD.
  - Último inicio de sesión
  - Sistema Operativo
  - OU y GUID del Directorio Activo
- La consola deberá permitir visualizar y exportar en formato CSV el inventario de hardware de todos los equipos administrados, en caso de ser en la nube, pudiendo mostrar al menos:
  - Número de serie del equipo
  - Modelo del equipo
  - Fabricante de la BIOS
  - Versión de la BIOS
  - Fecha de la BIOS
  - Cantidad de procesadores
  - Tamaño de la Unidad del sistema C:\
  - Espacio Libre en el disco del sistema
  - Tamaño de memoria RAM
  - Memoria RAM libre
  - Nombre del SO
  - Versión del SO
  - Dirección IP, MAC, WINS, DNSs.
  - Reportar si un Administrador ha iniciado sesión.
  - Si se necesita reiniciar,
  - Versión del cliente instalado
  - Si tiene unidades protegidas con el cifrado de discos,
  - Y añadir otros datos
- La consola deberá permitir visualizar la lista de vulnerabilidades y parches multifabricante con los siguiente datos:

- o Proveedor
- o Aplicación detectada
- o Versión Actual y Pendiente de Actualizar
- o Categoría según tipo (Paquete de servicio, Seguridad Crítica, Seguridad Importante, Solo Seguridad y Distinto a Seguridad)
- o ID del o los CVEs detectados con los enlaces respectivos a mitre.org
- o Clasificación de CSSV3 para la priorización de actualizaciones.
- o Identificación del boletín de seguridad del fabricante
- o Cantidad de equipos y servidores afectados.
- o Deberá contar con un sistema de filtros para mostrar por Categoría, Proveedor, Software y Tipo de Plataforma afectada.
- o Así mismo deberá contar con opciones para visualizar el resumen y el historial de instalaciones y exportar en formato CSV para su análisis posterior.
- o Deberá contar con opciones para enviar comandos para actualizar todos los equipos y/o seleccionar los equipos donde se quiere ejecutar una tarea de corrección de vulnerabilidades o aplicación de los parches detectados.
- La consola deberá permitir registrar los equipos que se conectan vía VPN y que son equipos que no pertenecen a la institución, utilizados por servidores y colaboradores que realizan trabajo remoto, pero que se requieren proteger con el fin de salvaguardar la información contenida en los servidores y equipos de la entidad.
- La consola deberá contar con consideraciones de Alertas y Reportes:
  - o Deberá incluir un sistema de generación de reportes ejecutivos y basados en gráficos. Este sistema deberá ser accesible vía Web desde cualquier punto de la red.
  - o Las alertas deberán ser enviadas a servidores de análisis de datos como los SYSLOG.
  - o La solución deberá ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alertas de registros, entre otros)
  - o La solución deberá generar reportes gráficos, imprimibles y exportables de la cobertura de versiones, actualizaciones e infecciones.
  - o La solución deberá contener un mecanismo de reportes que permite ver el estado de la protección de la red en línea.
  - o La solución deberá permitir acceder a reportes basados en el usuario que permita conocer rápidamente el cumplimiento de políticas por cada usuario
  - o La solución deberá incorporar un mecanismo de reportes que permita programar la creación y envío de reportes en formato PDF y HTML vía correo.
  - o La solución deberá incorporar un mecanismo de conexión con la base de datos para la creación de reportes personalizados.
  - o La solución deberá reportar la información de vulnerabilidades y actualizaciones de parches faltantes y aplicados en los diferentes equipos de la red.
  - o La solución deberá mostrar al menos los siguientes reportes:
    - o Equipos con más infecciones bloqueadas.
    - o Principales malwares detectados
    - o Cantidad de infecciones procesadas por día en el último mes.
    - o Versiones de clientes instalados
    - o Cantidad de equipos por longitud de contraseñas de los usuarios.
    - o Actualizaciones de Vulnerabilidades y Parches instaladas x día en los últimos 30 días.
  - o La solución deberá permitir ver las infecciones detectadas en todos los equipos y mostrar:
    - o Fecha y hora de detección

Car  
H  
A



- Equipo
- Usuario logueado
- Tipo de infección y nombre
- Acción realizada
- Objeto detectado y/o infectado. Así mismo deberá permitir crear rangos de fecha a visualizar.

## 5.2. PRESTACIÓN PRINCIPAL: CONDICIONES COMPLEMENTARIAS

### 5.2.1. IMPLEMENTACIÓN Y PUESTA EN FUNCIONAMIENTO

La implementación y puesta en funcionamiento de la solución de Plataforma de Protección Endpoints adquirido deberá cumplir las siguientes condiciones:

- Comprende la desinstalación de la totalidad de los anteriores antivirus clientes, y el despliegue, instalación y configuración de la solución de Plataforma de Protección Endpoints ofertada.
- Los trabajos programados serán supervisados por el personal de la Oficina de Gobierno Digital.
- Instalación de la consola de administración centralizada, además de subconsolas de ser el caso, las cuales serán determinadas por la Oficina de Gobierno Digital
- Instalación y configuración de las licencias de Plataforma de Protección Endpoints, se realizará en las estaciones de trabajo de la MML (equipos de cómputo y servidores que figuren en la consola de antivirus actual), los cuales deberán ser visualizadas en la consola de administración centralizada. Asimismo, deberán contar con las respectivas pruebas de actualización de firmas, versión del cliente, cambio de configuración entre otros.
- La solución de Plataforma de Protección Endpoints debe estar basada únicamente en software, no deberá incluir la adquisición de ningún tipo de equipamiento adicional como complemento del mismo.
- El software no debe afectar lentitud en los equipos de cómputo conectados a la Red de la MML.

### 5.2.2. CAPACITACIÓN

- El contratista deberá brindar una capacitación en modo presencial o virtual para el uso de las bondades y herramientas que brinda el la licencia de una Plataforma de Protección Endpoints para estaciones de trabajo y Servidores para la MML para cinco (05) personas, que designe el Departamento de Redes, Infraestructura y Seguridad TI, de la Oficina de Gobierno Digital.

Las horas de capacitación serán por un total de 6 horas (2 horas por día), deberá ser realizada en un plazo de siete (07) días, los mismos que deben ser considerados dentro de los treinta (30) días de la implementación de la solución.

- Para el desarrollo de la capacitación el contratista deberá incluir archivos digitales (separatas, manuales y videos para el dictado del curso).
- El contratista deberá considerar dentro de los temas a capacitar lo siguiente:
  - ✓ Ataques de phishing.
  - ✓ Cibersecurity.
  - ✓ Medios extraíbles.
  - ✓ Contraseñas y autenticación.
  - ✓ Configuración y administración de consola central.
  - ✓ Seguridad de los dispositivos móviles.
  - ✓ Trabajar a distancia.
  - ✓ Wi-Fi público.
  - ✓ Seguridad y configuración de estaciones de trabajo.



- ✓ Configuración, uso y despliegue de reglas y políticas de seguridad.
  - ✓ Uso de internet y del correo electrónico.
  - ✓ Ingeniería social.
  - ✓ Configuración y puesta en marcha de doble autenticación.
  - ✓ Durante el curso de capacitación se deberán realizar pruebas de ataques reales, infectando una máquina de prueba.
- o La capacitación se realizará, previa coordinación de horario y lugar con el Departamento de Redes, Infraestructura y Seguridad TI, de la Oficina de Gobierno Digital, a través de correo electrónico y/o coordinaciones telefónicas.
  - o Al finalizar la capacitación, el contratista deberá otorgar a los participantes los certificados de Operador y Administrador de Consola (versión física o digital) de la Plataforma de Protección Endpoints adquirida.

Al término de la implementación y puesta en funcionamiento, se suscribirá un **ACTA DE FINALIZACIÓN DE LA IMPLEMENTACIÓN Y PUESTA EN FUNCIONAMIENTO** (\*).

(\*) Para el inicio de la vigencia de la Plataforma de Protección Endpoints para las estaciones de trabajo y servidores, el contratista y la entidad deberán considerar la culminación de las licencias vigentes, debiendo establecer en el acta, en caso corresponda, la fecha de inicio de la activación de las nuevas licencias.

### 5.3. PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL

La prestación accesoria, comprende los siguientes:

- Mantenimiento
- Soporte Técnico

#### 5.3.1. MANTENIMIENTO

- a) Se debe incluir mantenimiento a todo la Plataforma de Protección Endpoints propuesto para la verificación, administración de consola y prevención de ataques de virus en la red de la MML, por un mínimo de cuatro (04) visitas al mes (un 1 día por semana), a partir del día siguiente de firmada el **Acta de finalización de la implementación y puesta en funcionamiento**.

Este mantenimiento deberá comprender como mínimo:

- La revisión de la consola de gestión
- La revisión de los logs del sistema de Plataforma de Protección Endpoints.
- La revisión de los eventos o alertas generadas
- La revisión y validación de la copia del respaldo de la configuración.

Asimismo, este mantenimiento podrá realizarse de manera remota o en sitio, previa coordinación con el personal del Departamento de Redes, Infraestructura Seguridad TI, de la Oficina de Gobierno Digital.

- b) El Contratista a la culminación de cada mantenimiento deberá remitir en un plazo de dos (02) día calendarios después de realizada cada visita un informe técnico sobre el mantenimiento, siendo un total de 04 informes mensuales y estos deberán ser remitidos debidamente firmados.

Dicha documentación deberá ser presentada por mesa de partes virtual o mesa de partes física de la Municipalidad Metropolitana de Lima, ubicada en Hospicio Manrique, entrada por el pasaje Acisclo Villarán N° 288-294, Cercado de Lima, altura de la Plaza Francia, en el horario de lunes a viernes de 08:30 a 13:00 horas y de 14:00 a 16:00 horas, dirigida a la Oficina de Gobierno Digital. En caso corresponda hacer entrega de

documentos originales, la documentación solo podrá ser presentada a través de mesa de partes física, en la dirección antes mencionada.

### 5.3.2. SOPORTE TÉCNICO

- a) El servicio debe ser 24x7x365 incluyendo sábados, domingos y feriados y estar disponible sin límite de horas por intervención, ni cantidad de intervenciones mensuales del personal del contratista; dándose por atendido un problema cuando es solucionado en su totalidad.
- b) Las llamadas de servicio comprenden también las consultas formuladas por el personal técnico de la Oficina de Gobierno Digital.
- c) El contratista ingresará el requerimiento en su sistema de atención de servicios, generándole un número único o código de boleta de atención, con lo cual hará seguimiento al servicio hasta su ejecución.
- d) El personal técnico del contratista, para la solución de un problema o incidente reportado, deberá coordinar y definir con el personal del Departamento de Redes, Infraestructura Seguridad TI, de la Oficina de Gobierno Digital, si la atención será de manera remota o en sitio.
- e) El contratista, como parte del soporte técnico deberá incluir la actualización de nuevos parches, actualizaciones y liberaciones de nuevas versiones del software de parte del fabricante.

El tiempo de respuesta para atención y solución de incidentes será de acuerdo al siguiente detalle:

**CUADRO N°01**

| TIPO DE INCIDENTE   | TIEMPO DE RESPUESTA                   | TIEMPO DE SOLUCIÓN                 |
|---|---------------------------------------|------------------------------------|
| <b>Crítico:</b> Afecta la disponibilidad de la red y el servicio de equipos informáticos en general, además ataques de nuevo Malware. | 30 minutos de reportado el incidente. | 3 horas de reportado el incidente. |
| <b>No Crítico:</b> errores, Problemas de Configuración de la solución de Plataforma de Protección Endpoints.                          | 45 minutos de reportado el incidente. | 4 horas de reportado el incidente. |

- f) Debe ser ON LINE (por línea telefónica o acceso remoto a los equipos), y ON SITE según se acuerde con el personal del Departamento de Redes, Infraestructura Seguridad TI, de la Oficina de Gobierno Digital.
- g) El contratista deberá proveer información del estado del problema reportado en un enlace web u otro mecanismo equivalente.
- h) Soporte correctivo cada vez que se presente una falla o mal funcionamiento propio de la solución.
- i) El contratista deberá contar con un Call Center (Centro de Atención de Servicios) o Mesa de ayuda con un soporte de 24x7, a través del cual se harán los requerimientos del servicio vía llamada telefónica y/o correo electrónico con la respectiva confirmación de recepción de la solicitud. El contratista deberá ofrecer como parte del soporte, la capacidad de atender y escalar problemas o consultas para ser absueltas por personal de fábrica.
- j) La Entidad a través de la Oficina de Gobierno Digital podrá solicitar al contratista la actualización de reléase del software de la solución ofertada, a la última versión estable sin que esto represente costo adicional para la Entidad, para lo cual el contratista efectuará la instalación, configuración, despliegue y dará el soporte correspondiente.
- k) Soporte (in situ o remoto) para reinstalaciones por problemas de la solución.



l) Apoyo y asesoría técnica en la administración y configuración de la solución durante el periodo de la prestación accesoria.

m) El Contratista deberá remitir un informe técnico mensual sobre las ocurrencias suscitadas durante el soporte técnico, la misma que deberá contener la solución de incidencias en caso ocurra.

Estos informes deberán contener como mínimo:

- o Las atenciones realizadas en el periodo del informe, indicando el número de ticket o atención, fecha y hora del reporte de la avería, la fecha y hora de la atención, modalidad de atención (remoto o en sitio), así como la fecha y hora de solucionado el problema.
- o Listado de los virus detectados, malware, intentos de amenazas, host afectados y políticas implementadas donde se pueda visualizar que usuario la implemento.

## 6. CLAUSULAS ESPECIALES

### 6.1. OTRAS OBLIGACIONES DEL CONTRATISTA

✓ El proveedor se obliga durante el desarrollo de los actos preparatorios, procedimiento de selección y ejecución contractual, a lo siguiente:

- Conducirse en todo momento, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción.
- No haber incurrido y no incurrir en actos de corrupción, así como a respetar el principio de integridad
- No tener impedimento para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.
- Comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento
- Ser responsable de la veracidad de los documentos e información presentada.

### 6.2. SEGUROS APLICABLES

El personal que participará en la ejecución de la prestación, deberá cumplir con los estándares de la Ley N° 29783 "Seguridad y Salud en el Trabajo", de manera obligatoria.

El contratista deberá contratar y/o mantener vigente durante el plazo de la prestación la Póliza de seguro complementario de trabajo de riesgo (SCTR), para todo el personal que participe en la ejecución de la prestación.

### 6.3. CONFIDENCIALIDAD

El contratista asume la obligación, tanto durante la vigencia del contrato, como después de su culminación, de guardar el secreto y la confidencialidad de cualquier información de la MML a la que tenga acceso, datos técnicos y organizativos de la MML. Por lo antes expuesto, el contratista no podrá:

- a. Difundir, transmitir y/o revelar información a terceros.
- b. Usar la información recopilada para ofrecer, proclamar o brindar información sobre productos o servicios.
- c. Arrendar ni vender a terceros ningún dato de identificación personal que les haya sido proporcionado por la MML o como consecuencia de la ejecución de las prestaciones a su cargo.
- d. Invitar al usuario a tomar parte en encuestas sobre productos, servicios, noticias y/o eventos.

## 7. DOCUMENTOS DE PRESENTACIÓN CONJUNTAMENTE CON LAS OFERTAS

- Carta y/o documentos emitidos por el fabricante o representante local del fabricante, en el que se indique que el postor está autorizado a comercializar, instalar y dar soporte al bien solicitado.

## 8. DOCUMENTOS DE PRESENTACIÓN PARA LA SUSCRIPCIÓN DE CONTRATO

Además de los documentos señalados en las bases administrativas del procedimiento de selección



el postor adjudicado deberá presentar los siguientes documentos para la firma del contrato:

- Números de teléfono y correo electrónico de la central de atenciones.
- Correo electrónico para efectos de la notificación durante la ejecución del contrato.
- Copia del Título profesional que acredite la formación académica solicitada para el Jefe de Proyecto.
- Copia del Título técnico que acredite la formación requerida para el personal técnico.
- Copia de los certificados de capacitación, donde se acredite el número de horas lectivas, para el personal clave.
- Copia del certificado en el uso y administración de la Plataforma de Protección Endpoints propuesto, emitido por el fabricante, del Jefe de Proyecto y Personal Técnico.
- Copia de la Póliza de Seguro Complementario de Trabajo de Riesgo (SCTR).

Dicha documentación deberá ser presentada por mesa de partes virtual o mesa de partes física de la Municipalidad Metropolitana de Lima, ubicada en Hospicio Manrique, entrada por el pasaje Acisclo Villarán N° 288-294, Cercado de Lima, altura de la Plaza Francia, en el horario de lunes a viernes de 08:30 a 13:00 horas y de 14:00 a 16:00 horas, dirigida a la Oficina de Logística. En caso corresponda hacer entrega de documentos originales, la documentación solo podrá ser presentada a través de mesa de partes física, en la dirección antes mencionada.

## 9. RECURSOS DEL PROVEEDOR

### 9.1. REQUISITOS DEL PROVEEDOR Y DE SU PERSONAL

#### 9.1.1. PERFIL DEL PROVEEDOR

Debe ser un representante comercial local ó empresa subsidiaria local o empresa especializada certificada o socio de negocios certificado por los fabricantes o los representantes locales del fabricante de la marca, lo cual se deberá acreditar mediante una carta o documento de los fabricantes o representantes locales del fabricante, en la que se indique que la empresa está autorizada a comercializar, instalar y dar soporte al bien solicitado. Dicho documento deberá presentarlo en la etapa de la presentación de la oferta.

#### 9.1.2. PERFIL DEL PERSONAL

##### 9.1.2.1. PERSONAL CLAVE

##### UN (01) JEFE DE PROYECTO

- **FUNCIONES:** Encargado de la planificación, coordinación, seguimiento, capacitación y control de las actividades del proyecto.
- **FORMACIÓN ACADÉMICA:** Profesional con título universitario de las carreras Ingeniería de Sistemas, Computación, Computación y Sistemas, Electrónica, Ingeniería Industrial o Informática.
- **EXPERIENCIA:** Experiencia mínima de 05 años como jefe de proyectos y/o coordinador de proyectos y/o gerente de proyectos, todas en implementación y gestión de soluciones de seguridad informática.
- **CAPACITACIÓN:**
  - ✓ En PMP (profesional en Dirección de Proyectos) con una duración de por lo menos 30 horas lectivas.
  - ✓ En ITIL oficial (Information Technology Infrastructure Library) Con una duración de por lo menos 30 horas lectivas.
  - ✓ En SCRUM oficial (Information Technology Infrastructure Library) Con una duración de por lo menos 30 horas lectivas.

- ✓ En Gestión de la Seguridad de la Información basada en ISO/IEC 27001 con una duración de por lo menos 30 horas lectivas.

#### **DOS (02) TÉCNICOS**

##### **• FUNCIONES:**

- Instalar y configurar la consola de administración centralizada.
- Configurar las políticas y otros requisitos según se ha establecido en el numeral 5.1.1.
- Desinstalar los anteriores antivirus clientes e instalar, desplegar y configurar la Plataforma de Protección Endpoints ofertada.
- Realizar el mantenimiento y soporte técnico de la Plataforma de Protección Endpoints propuesta.
- Coordinar con el fabricante, el uso de la garantía comercial, en caso los incidentes o los eventos lo requieran.

- **FORMACIÓN ACADÉMICA:** Técnico titulado en Computación y/o Sistemas y/o Electrónica y/o Informática y/o profesional bachiller Y/o titulado en las carreras de Ingeniería Electrónica y/o telecomunicaciones Y/o ingeniería de sistemas.

- **EXPERIENCIA:** No menor a tres (03) años como técnico en instalación de sistemas antivirus y/o servicios de doble factor de autenticación y/o gestión de soluciones de seguridad informática.

##### **• CAPACITACIÓN:**

- ✓ En la solución de Plataforma de Protección Endpoints ofertada la cual deberá ser emitida por el mismo fabricante del producto ofertado con una duración de por lo menos 20 horas lectivas.
- ✓ En ITIL oficial (Information Technology Infrastructure Library) Con una duración de por lo menos 40 horas lectivas.
- ✓ En Gestión de la Seguridad de la Información basada en ISO/IEC 20000 IT Service con una duración de por lo menos 20 horas lectivas.
- ✓ En Gestión de la Seguridad de la Información basada en ISO/IEC 27001 con una duración de por lo menos 30 horas lectivas.
- ✓ En ciberseguridad mediante el curso CEHv11 (Certified Ethical Hacker v11) con una duración de por lo menos 20 horas lectivas.

#### **OTRAS CONSIDERACIONES DEL PERSONAL CLAVE**

En caso de cambio y/o rotación de personal clave, el contratista deberá comunicarlo al área usuaria al correo [infraestructura@munlima.gob.pe](mailto:infraestructura@munlima.gob.pe) con copia al correo: [sti\\_servicios@munlima.gob.pe](mailto:sti_servicios@munlima.gob.pe), por lo menos con 48 horas de anticipación, presentando la documentación del nuevo personal clave, en la cual acredite el cumplimiento de los requisitos solicitados en el requerimiento, a fin de evaluarlo y ser aprobada por la Oficina de Gobierno Digital, en un plazo máximo de tres (3) días calendario siguientes a la comunicación realizada.

#### **10. ENTREGABLES DOCUMENTARIOS**

##### **PRESTACIÓN PRINCIPAL**

El entregable consta de:

- a) El contratista deberá entregar el documento de **licenciamiento** firmado por el fabricante de la solución ofertada (si la entrega es virtual, documentó que acredite la entrega), por la adquisición de 3200 licencias de Plataforma de Protección Endpoints con su soporte respectivo, con una



vigencia de licenciamiento por tres (3) años, al momento de la entrega de los bienes en el Área de Almacenamiento y Distribución.

- b) Informe de término de la implementación y puesta en funcionamiento de la Plataforma de Protección Endpoints.
- c) Copia de los Certificados de Capacitación (versión física o digital) otorgados por el Contratista, incluyendo separatas y manuales de usuario.

El documento será presentado dentro de los dos (02) días calendarios de haber suscrito el Acta de finalización de la implementación y puesta en funcionamiento.

#### **PRESTACIÓN ACCESORIA**

- a) Cuatro (04) Informes técnicos mensuales sobre el mantenimiento (un 1 día por semana), el cual deberá ser firmado por el especialista designado para tal fin y remitido por el Contratista.
- b) Un Informe técnico sobre el soporte, deberá ser firmado y remitido por el Contratista.

Dicha documentación (Prestación Principal y Accesorio) deberá ser presentada por mesa de partes virtual o mesa de partes física de la Municipalidad Metropolitana de Lima, ubicada en Hospicio Manrique, entrada por el pasaje Acisclo Villarán N° 288-294, Cercado de Lima, altura de la Plaza Francia, en el horario de lunes a viernes de 08:30 a 13:00 horas y de 14:00 a 16:00 horas, dirigida a la Oficina de Logística. En caso corresponda hacer entrega de documentos originales, la documentación solo podrá ser presentada a través de mesa de partes física, en la dirección antes mencionada.

#### **10.1. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN**

- a) A fin de poder elaborar su propuesta económica, durante el procedimiento de selección los participantes, podrán realizar una visita a la Oficina de Gobierno Digital y solicitar la información pertinente, durante los horarios de oficina (8:30 am – 4:30 pm), a fin de obtener un mejor conocimiento de la implementación, equipamiento técnico, necesidades de configuración de los equipos u otros componentes, que tengan que incluir en la implementación y ejecución del requerimiento.
- b) El contratista deberá garantizar la operatividad de los servicios informáticos que brinda la Entidad.
- c) Cualquier solicitud posterior de reconfiguración del servidor donde se instalará la consola de administración centralizada de Plataforma de Protección Endpoints, deberá realizarse sin costo adicional para la MML.
- d) El software de Plataforma de Protección Endpoints provisto por el contratista debe cumplir con las características técnicas propuestas.
- e) En la implementación, el contratista deberá trabajar de manera conjunta con el personal técnico del Departamento de Redes, Infraestructura y Seguridad TI asignado a supervisar la implementación y puesta en operación de este.
- f) Las pruebas que se requieran no deberán afectar las labores y la red de la MML.
- g) El Contratista junto con el personal del Departamento de Redes, Infraestructura y Seguridad TI, deberán realizar las pruebas o ensayos que serán de uso para la conformidad de los entregables, con el fin de dar cumplimiento a las especificaciones técnicas.
- h) El Contratista deberá cumplir con las políticas de seguridad y con los procedimientos y políticas para el manejo de los recursos tecnológicos definidos por la MML.

#### **11. LUGAR, PLAZO DE EJECUCIÓN DE LA PRESTACIÓN**

##### **11.1. LUGAR DE EJECUCIÓN**

##### **PRESTACIÓN PRINCIPAL**

La implementación, puesta en funcionamiento y capacitación se realizará en la Oficina de Gobierno Digital, sito en Jirón Conde de Superunda N° 141, Cercado de Lima.

**PRESTACIÓN ACCESORIA**

El Mantenimiento y Soporte Técnico se realizarán en las instalaciones de la Oficina de Gobierno Digital, ubicada en el tercer piso del Palacio Municipal, sito en Jirón Conde de Superunda N° 141, Cercado de Lima y vía telefónica en caso se requiera.

**11.2. PLAZO DE EJECUCIÓN**

**PRESTACIÓN PRINCIPAL**

Se ejecutará en un plazo total de Treinta y Siete (37) días calendario, de acuerdo a lo siguiente:

- **ENTREGA:** La entrega de las 3,200 licencias se realizará en el plazo de siete (07) días calendario, contados a partir del día siguiente de suscrito el contrato y será en el Área de Almacenamiento y Distribución.
- **IMPLEMENTACIÓN, PUESTA EN FUNCIONAMIENTO Y CAPACITACIÓN:** Será dentro de los Treinta (30) días calendario contados a partir del día siguiente de la entrega de las licencias.

**PRESTACIÓN ACCESORIA**

El plazo de la prestación accesoria consiste en el mantenimiento y soporte técnico, y será de la siguiente manera:

- **EL MANTENIMIENTO Y SOPORTE:** Deberá ser por un periodo de 1095 días calendarios (36 meses), a partir del día siguiente de la suscripción del acta de finalización de la implementación y puesta en funcionamiento.

**12. PENALIDADES**

**12.1. PENALIDAD POR MORA**

En caso de retraso injustificado del contratista en la ejecución de la prestación objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, en virtud del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

**12.2. OTRAS PENALIDADES**

En concordancia con el artículo 163° del Reglamento de la Ley de Contrataciones del Estado, La Entidad puede establecer penalidades distintas a la mencionada en el artículo 162° del Reglamento de la Ley de Contrataciones del Estado.

**OTRAS PENALIDADES - PRESTACIÓN PRINCIPAL**

| N° | Supuestos de aplicación de penalidad   | Forma de cálculo                | Procedimiento   |
|----|--|---------------------------------|---|
| 1  | Quando el contratista durante la ejecución de la prestación principal, realice el cambio y/o rotación del personal clave, sin la aprobación de la Oficina de Gobierno Digital. | 20 % de UIT por cada ocurrencia | a) El personal designado por la Oficina de Gobierno Digital al advertir el incumplimiento por parte del Contratista, informará de manera sustentada dicho hecho a la Oficina de Logística detallando los incumplimientos para la aplicación de la penalidad respectiva.<br>b) La Oficina de Logística remitirá al contratista carta y/o correo electrónico institucional comunicando la penalidad impuesta, indicando que debe subsanar la falta en la que ha incurrido, en caso corresponda. |



Oficina de Gobierno Digital

| N° | Supuestos de aplicación de penalidad  | Forma de cálculo                     | Procedimiento   |
|----|---|--------------------------------------|---|
| 2  | Cuando el contratista incumpla con el plazo de presentación de los Entregables. | 10 % de UIT por cada día de retraso. | <p>c) En caso de existir reclamos por la(s) penalidad(es) aplicada(s), el contratista presentará el descargo correspondiente mediante una carta debidamente sustentada dirigido a la Oficina de Logística, vía mesa de partes virtual o física, en un plazo máximo de tres (03) días calendario de notificada la penalidad. De no corresponder subsanación o no contar con reclamos, se aplicará la penalidad y se descontará del pago mensual.</p> <p>d) La Oficina de Logística, previo informe del área usuaria, resolverá el mismo en el plazo máximo de 7 días calendario, y lo comunicará al contratista mediante carta y/o correo electrónico institucional.</p> |

**OTRAS PENALIDADES - PRESTACIÓN ACCESORIA**

| N° | Supuestos de aplicación de penalidad   | Forma de cálculo                                 | Procedimiento  |
|----|--|--|--|
| 1  | Cuando el contratista incumpla con el número de visitas al mes en el servicio de Mantenimiento sin justificación comprobada por el área usuaria.                               | 20% de la UIT por visita no realizada.           | a) El personal designado por la Oficina de Gobierno Digital al advertir el incumplimiento por parte del Contratista, informará de manera sustentada dicho hecho a la Oficina de Logística detallando los incumplimientos para la aplicación de la penalidad respectiva.  |
| 2  | Cuando el contratista incumpla con los plazos de presentación de los Entregables   | 10 % de UIT por cada día de retraso.             |  |
| 3  | Cuando el contratista no cumpla con el tiempo de respuesta señalados en el Cuadro N° 01, con respecto a las incidencias críticas y no críticas.                                | 10 % de la UIT por cada hora retraso o fracción. | b) La Oficina de Logística remitirá al contratista carta y/o correo electrónico institucional, comunicando la penalidad impuesta, indicando que debe subsanar la falta en la que ha incurrido, en caso corresponda.  |
| 4  | Cuando el contratista no cumpla con el tiempo de solución señalados en el Cuadro N° 01, con respecto a las incidencias críticas y no críticas.                                 | 10 % de la UIT por cada hora retraso o fracción. | c) En caso de existir reclamos por la(s) penalidad(es) aplicada(s), el contratista presentará el descargo correspondiente mediante una carta debidamente sustentada dirigido a la Oficina de Logística, vía mesa de partes virtual o física, en un plazo máximo de tres (03) días calendario de notificada la penalidad. De no corresponder subsanación o no contar con reclamos, se aplicará la penalidad y se descontará del pago mensual. |
| 5  | Cuando el contratista durante la ejecución de la prestación accesoria, realice el cambio y/o rotación del personal clave, sin la aprobación de la Oficina de Gobierno Digital. | 20 % de UIT por cada ocurrencia                  | d) La Oficina de Logística, previo informe del área usuaria, resolverá el mismo en el plazo máximo de 7 días calendario, y lo comunicará al contratista mediante carta y/o correo electrónico institucional.   |



Oficina de Gobierno Digital

**13. CONFORMIDAD**

La conformidad será otorgada en un plazo máximo de siete (7) días, en concordancia con el artículo 168 del Reglamento de la Ley de Contrataciones del Estado y de acuerdo con lo siguiente:

**PRESTACIÓN PRINCIPAL**

La conformidad de la prestación principal será otorgada por el responsable de la Oficina de Gobierno Digital, previo informe técnico del responsable Departamento de Redes, Infraestructura y Seguridad TI.

**PRESTACIÓN ACCESORIA**

La conformidad de la prestación accesoria será otorgada por el responsable de la Oficina de Gobierno Digital, previo informe técnico del responsable del Departamento de Redes, Infraestructura y Seguridad TI.

**14. PAGO**

**PRESTACIÓN PRINCIPAL**

La Entidad efectuará el pago de la prestación principal en un solo pago.

Para efectos del pago la Entidad debe contar con la siguiente documentación:

- Recepción del Área de Almacenamiento y Distribución, a través de la guía de remisión.
- Conformidad emitida por el responsable de la Oficina de Gobierno Digital, previo informe técnico del responsable del Departamento de Redes, Infraestructura y Seguridad TI.
- Comprobante de Pago.
- Entregable del Contratista.

**PRESTACIÓN ACCESORIA**

**Soporte y mantenimiento:**

La Entidad efectuará el pago a favor del contratista en forma mensual.

$$\text{Valor mensual} = \text{Costo total de la prestación accesoria} / 36$$

Para efectos del pago, la Entidad debe contar con la siguiente documentación:

- Conformidad emitida por el responsable de la Oficina de Gobierno Digital, de forma mensual (36 meses) previo informe técnico del responsable del Departamento de Redes, Infraestructura y Seguridad TI.
- Comprobante de Pago.
- Entregable del Contratista.

Dicha documentación (Prestación Principal y Accesoria) deberá ser presentada por mesa de partes virtual o mesa de partes física de la Municipalidad Metropolitana de Lima, ubicada en Hospicio Manrique, entrada por el pasaje Acisclo Villarán N° 288-294, Cercado de Lima, altura de la Plaza Francia, en el horario de lunes a viernes de 08:30 a 13:00 horas y de 14:00 a 16:00 horas, dirigida a la Oficina de Logística. En caso corresponda hacer entrega de documentos originales, la documentación solo podrá ser presentada a través de mesa de partes física, en la dirección antes mencionada.

**15. ADELANTOS**

La entidad no ha previsto adelantos.

**16. RESPONSABILIDAD POR VICIOS OCULTOS**

La recepción conforme de la prestación por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto en el numeral 40.2 del artículo 40 la Ley de Contrataciones del Estado y 173 de su Reglamento. El plazo máximo de





MUNICIPALIDAD METROPOLITANA DE LIMA  
OFICINA GENERAL DE ADMINISTRACIÓN  
Oficina de Gobierno Digital

responsabilidad del contratista es de dos (02) años contado a partir de la conformidad otorgada por LA ENTIDAD.

17. **SISTEMA DE CONTRATACIÓN**  
SUMA ALZADA

18. **MODALIDAD DE CONTRATACIÓN**  
LLAVE EN MANO

19. **SUBCONTRATACIÓN**  
En la presente contratación la Entidad no aceptará la subcontratación. El contratista mantiene la responsabilidad por la ejecución total de su contrato frente a la Entidad.

20. **VERIFICACIÓN SOBRE EL LBSC, ACUERDO MARCO Y FICHAS DE HOMOLOGACIÓN**  
Los bienes comprendidos en el presente requerimiento no se encuentran definidos en una Ficha de Homologación, en el Catálogo Electrónico de Acuerdos Marco o en el Listado de Bienes y Servicios Comunes.

Cup  
Hacienda

Cup

### 3.2. REQUISITOS DE CALIFICACIÓN

| B | EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD   |
|---|---|
|   | <p><b>Requisitos:</b><br/>El postor debe acreditar un monto facturado acumulado equivalente a S/ 300,000.00 (Trescientos Mil con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran bienes similares a los siguientes Venta de licencias de software de seguridad de Red y/o licencias antimalware y/o licencia de escaneo de Red.</p> <p><b>Acreditación:</b><br/>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago<sup>7</sup>, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el <b>Anexo N° 8</b> referido a la Experiencia del Postor en la Especialidad.</p> <p>En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p> <p>Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.</p> <p>Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el <b>Anexo N° 9</b>.</p> <p>Cuando en los contratos, órdenes de compra 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 compra o de cancelación del comprobante de pago, según corresponda.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el <b>Anexo N° 8</b> referido a la Experiencia del Postor en la Especialidad.</p> <p><b>Importante</b></p> <p><i>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".</i></p> |

<sup>7</sup> Cabe precisar que, de acuerdo con la Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado:

*"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"*

*(...)*

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



|   |  |                   |   |
|---|--|-------------------|---|
| C   | CAPACIDAD TÉCNICA Y PROFESIONAL  |                   |   |
| C.1   | EXPERIENCIA DEL PERSONAL CLAVE   |                   |   |
|   | <p><u>Requisitos:</u></p> <p><b><u>UN (01) JEFE DE PROYECTO</u></b><br/>Experiencia mínima de 05 años como jefe de proyectos y/o coordinador de proyectos y/o gerente de proyectos, todas en implementación y gestión de soluciones de seguridad informática.</p> <p><b><u>DOS (02) TÉCNICOS</u></b><br/>No menor a tres (03) años como técnico en instalación de sistemas antivirus y/o servicios de doble factor de autenticación y/o gestión de soluciones de seguridad informática.</p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <table><tr><td><b>Importante</b></td></tr><tr><td><ul style="list-style-type: none"><li>• <i>El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores.</i></li><li>• <i>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.</i></li><li>• <i>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.</i></li><li>• <i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i></li></ul></td></tr></table> | <b>Importante</b> | <ul style="list-style-type: none"><li>• <i>El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores.</i></li><li>• <i>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.</i></li><li>• <i>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.</i></li><li>• <i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i></li></ul> |
| <b>Importante</b>   |  |                   |   |
| <ul style="list-style-type: none"><li>• <i>El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores.</i></li><li>• <i>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.</i></li><li>• <i>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.</i></li><li>• <i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i></li></ul> |  |                   |   |

**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 las Especificaciones Técnicas 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 las características y/o requisitos funcionales. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.
- Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.

**CAPÍTULO IV**  
**FACTORES DE EVALUACIÓN**

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

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

| FACTOR DE EVALUACIÓN   | PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN  |
|--|---|
| <b>A. PRECIO</b>   |   |
| <p><u>Evaluación:</u></p> <p>Se evaluará considerando el precio ofertado por el postor.</p> <p><u>Acreditación:</u></p> <p>Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).</p> | <p>La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula:</p> $P_i = \frac{O_m \times PMP}{O_i}$ <p>i = Oferta<br/>P<sub>i</sub> = Puntaje de la oferta a evaluar<br/>O<sub>i</sub> = Precio i<br/>O<sub>m</sub> = Precio de la oferta más baja<br/>PMP = Puntaje máximo del precio</p> <p>100 puntos</p> |

P. J.

H. J.

L. J.



## CAPÍTULO V PROFORMA DEL CONTRATO

Conste por el presente documento, la contratación de Adquisición de Licencias de Plataforma de Protección Endpoints para la Municipalidad Metropolitana de Lima, que celebra de una parte la Municipalidad Metropolitana de Lima, en adelante LA ENTIDAD, con RUC N° 20131380951 con domicilio legal en Jirón de la Unión N.º 300 y Jirón Conde de Superunda N.º 141, Cercado de Lima, representada por [...], identificado con DNI N° [...], y de otra parte [...], con RUC N° [...], con domicilio legal en [...], inscrita en la Ficha N° [...] Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], debidamente representado por su Representante Legal, [...], con DNI N° [...], según poder inscrito en la Ficha N° [...], Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

### **CLÁUSULA PRIMERA: ANTECEDENTES**

Con fecha [...], el comité de selección adjudicó la buena pro de la **LICITACIÓN PÚBLICA N° 014-2023-MML-OGA-OL** para la contratación de Adquisición de Licencias de Plataforma de Protección Endpoints para la Municipalidad Metropolitana de Lima, 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 Adquisición de Licencias de Plataforma de Protección Endpoints para la Municipalidad Metropolitana de Lima

### **CLÁUSULA TERCERA: MONTO CONTRACTUAL**

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

Este monto comprende el costo del bien, 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 de la prestación materia del presente contrato.

### **CLÁUSULA CUARTA: DEL PAGO<sup>8</sup>**

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en Soles, en pago único (Prestación Principal) y en forma mensual (Prestación Accesorio), luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

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

LA ENTIDAD debe efectuar el pago dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los bienes, 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.

<sup>8</sup> En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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

El plazo de ejecución del presente contrato es:

##### **PRESTACIÓN PRINCIPAL**

Se ejecutará en un plazo total de Treinta y Siete (37) días calendario, de acuerdo a lo siguiente:

**ENTREGA:** La entrega de las 3,200 licencias se realizará en el plazo de siete (07) días calendario, contados a partir del día siguiente de suscrito el contrato y será en el Área de Almacenamiento y Distribución.

**IMPLEMENTACIÓN, PUESTA EN FUNCIONAMIENTO Y CAPACITACIÓN:** Será dentro de los Treinta (30) días calendario contados a partir del día siguiente de la entrega de las licencias.

#### **CLÁUSULA SEXTA: PRESTACIONES ACCESORIAS<sup>9</sup>**

Las prestaciones accesorias tienen por objeto el Mantenimiento Y Soporte Técnico, y será de la siguiente manera:

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

El plazo de ejecución de las prestaciones accesorias es de 1095 días calendarios (36 meses), a partir del día siguiente de la suscripción del acta de finalización de la implementación y puesta en funcionamiento.

#### **CLÁUSULA SÉTIMA: 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 OCTAVA: 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.

En el caso que corresponda, consignar lo siguiente:

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

##### **Importante**

*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.*

<sup>9</sup> De conformidad con la Directiva sobre prestaciones accesorias, los contratos relativos al cumplimiento de la(s) prestación(es) principal(es) y de la(s) prestación(es) accesorias, pueden estar contenidos en uno o dos documentos. En el supuesto que ambas prestaciones estén contenidas en un mismo documento, estas deben estar claramente diferenciadas, debiendo indicarse entre otros aspectos, el precio y plazo de cada prestación.



**CLÁUSULA NOVENA: 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 en el literal a) del numeral 155.1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

**CLÁUSULA DÉCIMA: RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN**

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La recepción será otorgada por el Área de Almacenamiento y Distribución y la conformidad será otorgada por Oficina de Gobierno Digital, previo informe técnico del responsable del Departamento de Redes, Infraestructura y Seguridad TI en el plazo máximo de siete (07) días de producida la recepción.

De existir observaciones, LA ENTIDAD las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (8) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no cumpliera a cabalidad con la subsanación, LA ENTIDAD puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

Este procedimiento no resulta aplicable cuando los bienes manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

**CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA**

EL CONTRATISTA declara bajo juramento que se compromete a cumplir las obligaciones derivadas del presente contrato, bajo sanción de quedar inhabilitado para contratar con el Estado en caso de incumplimiento.

**CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS**

La recepción conforme de la prestación 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 dos (02) año(s) contado a partir de la conformidad otorgada por LA ENTIDAD.

**CLÁUSULA DÉCIMA TERCERA: PENALIDADES**

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA ENTIDAD le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo a la siguiente fórmula:

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

Donde:

**F = 0.25 para plazos mayores a sesenta (60) días o;**

**F = 0.40 para plazos menores o iguales a sesenta (60) días.**

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de LA ENTIDAD no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme el numeral 162.5 del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

**OTRAS PENALIDADES - PRESTACIÓN PRINCIPAL**

| N° | Supuestos de aplicación de penalidad   | Forma de cálculo                     | Procedimiento  |
|----|--|--------------------------------------|--|
| 1  | Quando el contratista durante la ejecución de la prestación principal, realice el cambio y/o rotación del personal clave, sin la aprobación de la Oficina de Gobierno Digital. | 20 % de UIT por cada ocurrencia      | a) El personal designado por la Oficina de Gobierno Digital al advertir el incumplimiento por parte del Contratista, informará de manera sustentada dicho hecho a la Oficina de Logística detallando los incumplimientos para la aplicación de la penalidad respectiva.<br>b) La Oficina de Logística remitirá al contratista carta y/o correo electrónico institucional, comunicando la penalidad impuesta, indicando que debe subsanar la falta en la que ha incurrido, en caso corresponda.   |
| 2  | Quando el contratista incumpla con el plazo de presentación de los Entregables.  | 10 % de UIT por cada día de retraso. | c) En caso de existir reclamos por la(s) penalidad(es) aplicada(s), el contratista presentará el descargo correspondiente mediante una carta debidamente sustentada dirigido a la Oficina de Logística, vía mesa de partes virtual o física, en un plazo máximo de tres (03) días calendario de notificada la penalidad. De no corresponder subsanación o no contar con reclamos, se aplicará la penalidad y se descontará del pago mensual.<br>d) La Oficina de Logística, previo informe del área usuaria, resolverá el mismo en el plazo máximo de 7 días calendario, y lo comunicará al contratista mediante carta y/o correo electrónico institucional. |

**OTRAS PENALIDADES - PRESTACIÓN ACCESORIA**

| N° | Supuestos de aplicación de penalidad   | Forma de cálculo                                 | Procedimiento   |
|----|--|--|---|
| 1  | Quando el contratista incumpla con el número de visitas al mes en el servicio de Mantenimiento sin justificación comprobada por el área usuaria. | 20% de la UIT por visita no realizada.           | a) El personal designado por la Oficina de Gobierno Digital al advertir el incumplimiento por parte del Contratista, informará de manera sustentada dicho hecho a la Oficina de Logística detallando los incumplimientos para la aplicación de la penalidad respectiva. |
| 2  | Quando el contratista incumpla con los plazos de presentación de los Entregables   | 10 % de UIT por cada día de retraso.             | b) La Oficina de Logística remitirá al contratista carta y/o correo electrónico institucional, comunicando la penalidad impuesta, indicando que debe subsanar la falta en la que ha incurrido, en caso corresponda.   |
| 3  | Quando el contratista no cumpla con el tiempo de respuesta señalados en el Cuadro N° 01, con respecto a las incidencias críticas y no críticas.  | 10 % de la UIT por cada hora retraso o fracción. | c) En caso de existir reclamos por la(s) penalidad(es) aplicada(s), el contratista presentará el descargo correspondiente mediante una carta debidamente sustentada dirigido a la Oficina de Logística, vía mesa de partes virtual o                                    |
| 4  | Quando el contratista no cumpla con el tiempo de solución señalados en el Cuadro N° 01, con respecto a las incidencias críticas y no críticas.   | 10 % de la UIT por cada hora retraso o fracción. |   |

PA  
H  
M



| N° | Supuestos de aplicación de penalidad   | Forma de cálculo                | Procedimiento   |
|----|--|---------------------------------|---|
| 5  | Cuando el contratista durante la ejecución de la prestación accesoria, realice el cambio y/o rotación del personal clave, sin la aprobación de la Oficina de Gobierno Digital. | 20 % de UIT por cada ocurrencia | física, en un plazo máximo de tres (03) días calendario de notificada la penalidad. De no corresponder subsanación o no contar con reclamos, se aplicará la penalidad y se descontará del pago mensual.<br>d) La Oficina de Logística, previo informe del área usuaria, resolverá el mismo en el plazo máximo de 7 días calendario, y lo comunicará al contratista mediante carta y/o correo electrónico institucional. |

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

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

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

#### **CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO**

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 32.3 del artículo 32 y artículo 36 de la Ley de Contrataciones del Estado, y el artículo 164 de su Reglamento. De darse el caso, LA ENTIDAD procederá de acuerdo a lo establecido en el artículo 165 del Reglamento de la Ley de Contrataciones del Estado.

#### **CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES**

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

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

#### **CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN**

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

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

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

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

**CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO**

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

**CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS<sup>10</sup>**

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

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

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

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

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

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

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

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

DOMICILIO DE LA ENTIDAD: Jirón de la Unión N° 300 y Jirón Conde de Superunda N° 141

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

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

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

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

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

**Importante**

*Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales<sup>11</sup>.*

<sup>10</sup> De acuerdo con el numeral 225.3 del artículo 225 del Reglamento, las partes pueden recurrir al arbitraje ad hoc cuando las controversias deriven de procedimientos de selección cuyo valor estimado sea menor o igual a cinco millones con 00/100 soles (S/ 5 000 000,00).

<sup>11</sup> Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>



## ANEXOS

*[Handwritten signature]*

*[Handwritten signature]*

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 014-2023-MML-OGA-OL**  
Presente.-

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

|                                       |               |  |  |
|---------------------------------------|---------------|--|--|
| Nombre, Denominación o Razón Social : |               |  |  |
| Domicilio Legal :                     |               |  |  |
| RUC :                                 | Teléfono(s) : |  |  |
| 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 compra<sup>12</sup>

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

<sup>12</sup> Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de compra.



ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

**COMITÉ DE SELECCIÓN**

**LICITACIÓN PÚBLICA N° 014-2023-MML-OGA-OL**

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) : |  |  |
| Correo electrónico :                  |               |  |  |

|                                       |               |  |  |
|---------------------------------------|---------------|--|--|
| Datos del consorciado 2               |               |  |  |
| Nombre, Denominación o Razón Social : |               |  |  |
| Domicilio Legal :                     |               |  |  |
| RUC :                                 | Teléfono(s) : |  |  |
| Correo electrónico :                  |               |  |  |

|                                       |               |  |  |
|---------------------------------------|---------------|--|--|
| Datos del consorciado ...             |               |  |  |
| Nombre, Denominación o Razón Social : |               |  |  |
| Domicilio Legal :                     |               |  |  |
| RUC :                                 | Teléfono(s) : |  |  |
| 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.
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 compra<sup>13</sup>

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.  
[CONSIGNAR CIUDAD Y FECHA]

<sup>13</sup> Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de compra.

.....  
**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.*

P. J.  
H. J.  
L. J.





**ANEXO N° 2**

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

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 014-2023-MML-OGA-OL**  
Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

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

**ANEXO N° 3**

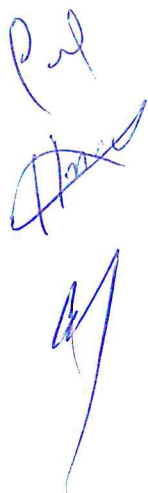
**DECLARACIÓN JURADA DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS**

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 014-2023-MML-OGA-OL**  
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 la ADQUISICIÓN DE LICENCIAS DE PLATAFORMA DE PROTECCIÓN ENDPOINTS PARA LA MUNICIPALIDAD METROPOLITANA DE LIMA, de conformidad con las Especificaciones Técnicas 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 las especificaciones técnicas, conforme a lo indicado en el acápite relacionado al contenido de las ofertas de la presente sección de las bases.*



**ANEXO N° 4**

**DECLARACIÓN JURADA DE PLAZO DE ENTREGA**

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 014-2023-MML-OGA-OL**  
Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a entregar los bienes objeto del presente procedimiento de selección en el plazo de TREINTA Y SIETE (37) días calendario, de acuerdo a lo siguiente:

ENTREGA: Se realizará en el plazo de siete (07) días calendario, contados a partir del día siguiente de suscrito el contrato.

IMPLEMENTACIÓN, PUESTA EN FUNCIONAMIENTO: Será dentro de los Treinta (30) días calendario contados a partir del día siguiente de la entrega de las licencias.

[CONSIGNAR CIUDAD Y FECHA]

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

P.p  
Hnac  
Qyp

**ANEXO N° 5**

**PROMESA DE CONSORCIO**

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

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 014-2023-MML-OGA-OL**  
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 a la **LICITACIÓN PÚBLICA N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]**.

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

- a) Integrantes del consorcio
  - 1. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1].
  - 2. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2].
- b) Designamos a [CONSIGNAR NOMBRES Y APELLIDOS DEL REPRESENTANTE COMÚN], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], como representante común del consorcio para efectos de participar en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato correspondiente con [CONSIGNAR NOMBRE DE LA ENTIDAD].

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

- c) Fijamos nuestro domicilio legal común en [.....].
- d) Las obligaciones que corresponden a cada uno de los integrantes del consorcio son las siguientes:

- 1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [ % ]<sup>14</sup>

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

- 2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [ % ]<sup>15</sup>

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%<sup>16</sup>

[CONSIGNAR CIUDAD Y FECHA]

<sup>14</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>15</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>16</sup> Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.



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

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

**Importante**

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

Pup  
Hacienda  
Cul

**ANEXO N° 6**

**PRECIO DE LA OFERTA**

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 014-2023-MML-OGA-OL**  
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 |
|---|--------------|
| PRESTACIÓN PRINCIPAL: ADQUISICIÓN DE LICENCIAS DE PLATAFORMA DE PROTECCIÓN ENDPOINTS PARA LA MUNICIPALIDAD METROPOLITANA DE LIMA. |              |
| PRESTACIÓN ACCESORIA:   |              |
| <b>TOTAL</b>  |              |

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

**El postor debe detallar en el precio de su oferta, el monto correspondiente a la prestación principal y las prestaciones accesorias.**

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

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

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



**ANEXO N° 7**

**DECLARACIÓN JURADA DE CUMPLIMIENTO DE CONDICIONES PARA LA APLICACIÓN DE LA  
EXONERACIÓN DEL IGV  
(NO APLICA PARA LA PRESENTE CONTRATACIÓN)**

*Puj*

*Haci*

*Asp*

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores  
COMITÉ DE SELECCIÓN  
LICITACIÓN PÚBLICA N° 014-2023-MML-OGA-OL  
Presente.-

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

| N° | CLIENTE | OBJETO DEL CONTRATO | N° CONTRATO / O/C / COMPROBANTE DE PAGO | FECHA DEL CONTRATO O CP <sup>17</sup> | FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>18</sup> | EXPERIENCIA PROVENIENTE <sup>19</sup> DE: | MONEDA | IMPORTE <sup>20</sup> | TIPO DE CAMBIO VENTA <sup>21</sup> | MONTO FACTURADO ACUMULADO <sup>22</sup> |
|----|---------|---------------------|---|---------------------------------------|--|---|--------|-----------------------|------------------------------------|---|
| 1  |         |                     |   |                                       |  |   |        |                       |                                    |   |
| 2  |         |                     |   |                                       |  |   |        |                       |                                    |   |
| 3  |         |                     |   |                                       |  |   |        |                       |                                    |   |
| 4  |         |                     |   |                                       |  |   |        |                       |                                    |   |

<sup>17</sup> Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

<sup>18</sup> Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho periodo.

<sup>19</sup> Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Al respecto, según la Opinión N° 216-2017/DTN "Considerando que la sociedad matriz y la sucursal constituyen la misma persona jurídica, la sucursal puede acreditar como suya la experiencia de su matriz". Del mismo modo, según lo previsto en la Opinión N° 010-2013/DTN, "... en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad incorporada o absorbida, que se extingue producto de la fusión; asimismo, si en virtud de la escisión se transfiere un bloque patrimonial consistente en una línea de negocio completa, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante podrá emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe".

<sup>20</sup> Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

<sup>21</sup> El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.



<sup>22</sup> Consignar en la moneda establecida en las bases.





| N°    | CLIENTE | OBJETO DEL CONTRATO | N° CONTRATO / O/C / COMPROBANTE DE PAGO | FECHA DEL CONTRATO O CP <sup>17</sup> | FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>18</sup> | EXPERIENCIA PROVENIENTE <sup>19</sup> DE: | MONEDA | IMPORTE <sup>20</sup> | TIPO DE CAMBIO VENTA <sup>21</sup> | MONTO FACTURADO ACUMULADO <sup>22</sup> |
|-------|---------|---------------------|---|---------------------------------------|--|---|--------|-----------------------|------------------------------------|---|
| 5     |         |                     |   |                                       |  |   |        |                       |                                    |   |
| 6     |         |                     |   |                                       |  |   |        |                       |                                    |   |
| 7     |         |                     |   |                                       |  |   |        |                       |                                    |   |
| 8     |         |                     |   |                                       |  |   |        |                       |                                    |   |
| 9     |         |                     |   |                                       |  |   |        |                       |                                    |   |
| 10    |         |                     |   |                                       |  |   |        |                       |                                    |   |
| ...   |         |                     |   |                                       |  |   |        |                       |                                    |   |
| 20    |         |                     |   |                                       |  |   |        |                       |                                    |   |
| TOTAL |         |                     |   |                                       |  |   |        |                       |                                    |   |

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 9

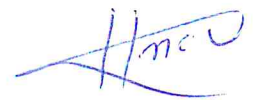
DECLARACIÓN JURADA  
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores  
COMITÉ DE SELECCIÓN  
LICITACIÓN PÚBLICA N° 014-2023-MML-OGA-OL  
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° 11**

**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**  
**LICITACIÓN PÚBLICA N° 014-2023-MML-OGA-OL**  
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.*



