

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

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



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

47
9

SIMBOLOGÍA UTILIZADA:

Nº	Símbolo	Descripción
1	[ABC] / [.....]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / [.....]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	<div>Importante</div> <ul style="list-style-type: none"> • Abc 	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	<div>Advertencia</div> <ul style="list-style-type: none"> • Abc 	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	<div>Importante para la Entidad</div> <ul style="list-style-type: none"> • Xyz 	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

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

Nº	Características	Parámetros
1	Márgenes	Superior : 2.5 cm Inferior: 2.5 cm Izquierda: 2.5 cm Derecha: 2.5 cm
2	Fuente	Arial
3	Estilo de Fuente	Normal: Para el contenido en general Cursiva: Para el encabezado y pie de página Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
4	Color de Fuente	Automático: Para el contenido en general Azul : Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
5	Tamaño de Letra	16 : Para las dos primeras hojas de las Secciones General y Específica 11 : Para el nombre de los Capítulos. 10 : Para el cuerpo del documento en general 9 : Para el encabezado y pie de página Para el contenido de los cuadros, pudiendo variar, según la necesidad 8 : Para las Notas al pie
6	Alineación	Justificada: Para el contenido en general y notas al pie. Centrada : Para la primera página, los títulos de las Secciones y nombres de los Capítulos)
7	Interlineado	Sencillo
8	Espaciado	Anterior : 0 Posterior : 0
9	Subrayado	Para los nombres de las Secciones y para resaltar o hacer hincapié en algún concepto

INSTRUCCIONES DE USO:

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

Elaboradas en enero de 2019

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



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

BASES INTEGRADAS

CONCURSO PÚBLICO N° 007-2024-ATU-1

**CONTRATACIÓN DE SERVICIO DE SUSCRIPCIÓN DE
LICENCIAS DE SOFTWARE ANTIVIRUS PARA LOS
EQUIPOS DE CÓMPUTO DE LA AUTORIDAD DE
TRANSPORTE URBANO PARA LIMA Y CALLAO – ATU**

97
9
xp

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.

47
7 4

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

Importante

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

Importante

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

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

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

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

Advertencia

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

Importante

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

Importante

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

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

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

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

Importante

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

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

1.9. EVALUACIÓN DE LAS OFERTAS

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

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

1.10. CALIFICACIÓN DE OFERTAS

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

1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.12. RECHAZO DE LAS OFERTAS

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

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

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

1.13. OTORGAMIENTO DE LA BUENA PRO

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

1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

Importante

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

CAPÍTULO II

SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

- *Una vez otorgada la buena pro, el comité de selección, está en la obligación de permitir el acceso de los participantes y postores al expediente de contratación, salvo la información calificada como secreta, confidencial o reservada por la normativa de la materia, a más tardar dentro del día siguiente de haberse solicitado por escrito.*

Luego de otorgada la buena pro no se da a conocer las ofertas cuyos requisitos de calificación no fueron analizados y revisados por el comité de selección.

- *A efectos de recoger la información de su interés, los postores pueden valerse de distintos medios, tales como: (i) la lectura y/o toma de apuntes, (ii) la captura y almacenamiento de imágenes, e incluso (iii) pueden solicitar copia de la documentación obrante en el expediente, siendo que, en este último caso, la Entidad deberá entregar dicha documentación en el menor tiempo posible, previo pago por tal concepto.*
- *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

CAPÍTULO III DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

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

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

Importante

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

Advertencia

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

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

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

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

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

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

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

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

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

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

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

Advertencia

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

3.9. DISPOSICIONES FINALES

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

Handwritten signature in blue ink and a circular stamp with the number 17.

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

4/9

CAPÍTULO I GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre : AUTORIDAD DE TRANSPORTE URBANO PARA LIMA Y CALLAO - ATU
RUC N° : 20604932964
Domicilio legal : Calle José Gálvez N° 550 – Miraflores
Teléfono: : (01) 224-4444
Correo electrónico: : abastecimiento278@atu.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del SERVICIO DE SUSCRIPCIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS PARA LOS EQUIPOS DE CÓMPUTO DE LA AUTORIDAD DE TRANSPORTE URBANO PARA LIMA Y CALLAO – ATU.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Formato N° 02 el 11 de julio de 2024.

1.4. FUENTE DE FINANCIAMIENTO

RECURSOS ORDINARIOS

Importante

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

1.5. SISTEMA DE CONTRATACIÓN

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

1.6. DISTRIBUCIÓN DE LA BUENA PRO

No corresponde.

1.7. ALCANCES DEL REQUERIMIENTO

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

1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

Los servicios materia de la presente convocatoria se prestarán en el plazo de HASTA CIENTO CINCO (105) DÍAS CALENDARIO y se contabilizará a partir de la aprobación del plan de trabajo

del servicio contratado, en concordancia con lo establecido en el expediente de contratación.

De acuerdo al siguiente detalle:

10. PLAZO DE PRESTACIÓN DEL SERVICIO

10.1. Prestación Principal

El plazo de ejecución de la prestación principal es de hasta ciento cinco (105) días calendario y se contabilizará a partir de la aprobación del plan de trabajo del servicio contratado, conforme al siguiente detalle:

N°	CONCEPTO	PLAZOS
01	Implementación de la primera fase	Hasta los cuarenta y cinco (45) días calendario contados a partir de la aprobación del plan de trabajo.
02	Implementación de la segunda fase	Hasta los sesenta (60) días calendario contados a partir de la culminación de la implementación de la primera fase.

10.2. Prestación accesoria

N°	CONCEPTO	PLAZOS
01	Informe trimestral de la ejecución del servicio de soporte.	Trimestral Hasta los cinco (5) días calendario culminado el periodo trimestral del servicio. El cual se contabilizará desde la activación de la suscripción de la solución de seguridad avanzada antimalware.

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases de manera **gratuita**, para cuyo efecto deben remitir solicitud al correo electrónico abastecimiento278@atu.gob.pe y será remitido de manera digital al correo del solicitante.

Importante

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

1.10. BASE LEGAL

- Ley N° 31953, Ley de Presupuesto del Sector Público para el Año Fiscal 2024.
- Ley N° 31954, Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2024.
- Ley 30225, Ley de Contrataciones del Estado, en adelante la Ley.
- Reglamento de la Ley de Contrataciones del Estado, en adelante el Reglamento.
- Decreto Supremo N° 082-2019-EF que aprueba el TUO de la Ley N° 30225 – Ley de Contrataciones del Estado.
- Ley N° 27444, Ley del Procedimiento Administrativo General.
- Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
- Comunicados y Directivas del OSCE.
- Código Civil en forma supletoria.
- Directivas y opiniones del OSCE.
- Otras normas de derecho común.

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

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos², la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

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

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

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

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

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE³ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.

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

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

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

- e) Hoja de datos y/o guía de administración y/o ficha técnica y/o manuales y/o folletería, con el fin de acreditar el cumplimiento de las funcionalidades requeridas del producto ofertado. Así también, el Anexo 01 en el que indique el cumplimiento de las características mínimas de la solución ofertada.⁴
- f) Declaración jurada de plazo de prestación del servicio. **(Anexo N° 4)**⁵
- g) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio, así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)**
- h) El precio de la oferta en SOLES. Adjuntar obligatoriamente el **Anexo N° 6**.

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

Importante

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

2.2.1.2. Documentos para acreditar los requisitos de calificación

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

2.2.2. Documentación de presentación facultativa:

No corresponde.

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.

⁴ En atención a la Observación N° 02, formulado por el participante Anapolitica Consulting Group S.A.C. Ver Pliego.

⁵ En caso de considerar como factor de evaluación la mejora del plazo de prestación del servicio, el plazo ofertado en dicho anexo servirá también para acreditar este factor.

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

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁶ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación ⁷ (**Anexo N° 12**).
i) Detalle de los precios unitarios del precio ofertado⁸.

Importante

- En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*
- En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2> opción consulta de empresas acreditadas en el REMYPE.*
- En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

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.*

⁶ Para mayor información de las Entidades usuarias de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

⁷ En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

⁸ Incluir solo en caso de la contratación bajo el sistema a suma alzada.

- 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 Haya⁹.
- 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 de la ATU sito en Avenida José Gálvez N° 550 Miraflores o en la mesa de partes virtual en www.atu.gob.pe

Cabe precisar que la presentación de la documentación referente a las garantías de fiel cumplimiento del contrato y/o garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso deberán presentarse en mesa de partes física sito en sito en Calle José Gálvez N° 550 – Miraflores.

Importante

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

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en SOLES por la contraprestación pactada a favor del contratista dentro de los diez días calendario siguientes de otorgada la conformidad correspondiente emitida por la Unidad de Tecnologías de la Información – UTI, según el siguiente detalle:

Prestación Principal

N°	ENTREGABLE	VALOR DEL MONTO ADJUDICADO	FECHA DE PAGO
01	Informe de implementación de la primera fase	70%	Se efectuará a la entrega y conformidad del entregable
02	Informe de implementación de la segunda fase	30%	Se efectuará a la entrega y conformidad del entregable
TOTAL		100%	

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

- Informe del funcionario responsable de la UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Acta de conformidad emitida por la Unidad de Tecnologías de la Información.
- Informe de implementación por cada etapa.

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

. Prestación accesoria

N°	ENTREGABLE	VALOR DEL MONTO ADJUDICADO	FECHA DE PAGO
01	Informe trimestral I de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
02	Informe trimestral II de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
03	Informe trimestral III de soporte, actualizaciones reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
04	Informe trimestral IV de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
05	Informe trimestral V de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
06	Informe trimestral VI de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
07	Informe trimestral VII de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
08	Informe trimestral VIII de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
TOTAL		100%	

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

- Informe de Conformidad emitida por la Unidad de Tecnologías de la Información.
- Comprobante de pago.
- Informes trimestrales de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas.

Dicha documentación se debe presentar en mesa de partes de la ATU sito en Avenida José Gálvez N° 550 Miraflores o en la mesa de partes virtual en www.atu.gob.pe

CAPÍTULO III REQUERIMIENTO

Importante

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

3.1. TERMINOS DE REFERENCIA

REQUERIMIENTO

I. TÉRMINOS DE REFERENCIA

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de suscripción de licencias de software antivirus para los equipos de cómputo de la Autoridad de Transporte Urbano para Lima y Callao – ATU.

2. DEPENDENCIA SOLICITANTE

La Unidad de Tecnologías de la Información de la Autoridad de Transporte Urbano – ATU para Lima y Callao.

3. FINALIDAD PÚBLICA

Contar con una tecnología que permita la protección y continuidad de los servicios brindados por la entidad, minimizando el riesgo de daño, secuestro, pérdida, eliminación y robo de información almacenados en los equipos de cómputo, de tal manera que se cuente con el resguardo de toda la información crítica para el desarrollo continuo de las labores y con ello, garantizar la prestación eficiente de los servicios brindados a los ciudadanos.

4. OBJETO DE LA CONTRATACIÓN

Contar con un servicio para la protección de la información que se elabora, se gestiona y se transfiere en la infraestructura tecnológica a través de la red de datos institucional, permitiendo garantizar la confidencialidad, integridad y disponibilidad de la misma, mediante la protección contra la infiltración de software malicioso o cualquiera de sus variantes, y alineándose a la protección de información en las plataformas tecnológicas de servicio y de usuario final, en base al análisis, investigación y respuesta ante posibles amenazas maliciosas identificadas garantizando la continuidad de las operaciones de la Autoridad de Transporte Urbano para Lima y Callao – ATU.

5. ANTECEDENTES

- La Autoridad de Transporte Urbano para Lima y Callao - ATU viene trabajando con 1409 estaciones de trabajo y con 210 servidores (virtuales y físicos), administrados por la Unidad de Tecnología de la Información, en el caso que la norma lo requiera, se incluye las computadoras personales que se encuentren trabajando de forma remota (teletrabajo).
- Con fecha 21 de mayo del 2024, se elaboró el Informe Técnico Previo de Evaluación de Software N° 008-2024, para la suscripción de licencias de una solución de protección avanzada antimalware.
- Actualmente, se dispone de dos (02) segmentos de red, en los cuales se encuentran los servidores (DMZ) y red interna, que requieren ser implementados con la solución de antimalware avanzado.
- Esta infraestructura informática requiere de la implementación de un servicio de protección de antimalware avanzado para detección y respuesta extendida, que preserve satisfactoriamente el equipamiento informático de los usuarios y la infraestructura de servidores frente al software malicioso, malware o cualquiera de sus variantes, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información que se gestiona.
- Y, con Orden de Servicio N° 20366 de fecha 31/08/2022, se cuenta con el servicio de suscripción de licencias de software antivirus (ESET Endpoint Antivirus + ESET Server Security, con 1168 agentes para servidores y estaciones de trabajo) para los equipos de cómputo y Servidores (físicos y virtuales), teniendo fecha de finalización de la suscripción el 18/09/2024.

6. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

6.1. ALCANCE

El alcance de la presente contratación incluye la suscripción, implementación, pruebas, capacitación y soporte de una solución avanzada antimalware, el mismo que alcanzará a toda la infraestructura

tecnológica estaciones de trabajo de usuario final y servidores de los centros de datos de la Autoridad de Transporte Urbano de Lima y Callao - ATU.

6.2. DESCRIPCIÓN DEL SERVICIO

6.2.1. Prestación principal

6.2.1.1. Características de la Suscripción

Cantidad end-point	1460 unidades
Cantidad servidores	240 unidades
FUNCIONALIDADES MÍNIMAS REQUERIDAS PARA EL SERVICIO	
Consideraciones generales del servicio	<p>a. El servicio de protección de seguridad antimalware debe ser basada en gestión y despliegue a través de servicios de nube (SaaS) del propio fabricante.</p> <p>b. El servicio de protección debe permitir realizar el despliegue masivo mediante el directorio activo.</p> <p>c. La cantidad de activos debe ser de 1700 productos antimalware dividido de la siguiente manera: 1460 productos antimalware para usuarios finales y 240 para equipos de tipo servidor.</p> <p>d. La solución debe soportar los siguientes sistemas operativos:</p> <ul style="list-style-type: none"> ▪ Estaciones de trabajo: Desde Windows 7 o superior ▪ Windows Server: Desde Windows server 2008 o superior. ▪ Servidores Linux: Desde <ul style="list-style-type: none"> ✓ Ubuntu Linux 14 o superior. ✓ Centos 5 o superior. ✓ Oracle Linux 5 o superior. ✓ Red Hat Enterprise 5. ✓ Alma Linux 8. <p>e. El servicio debe incluir como mínimo las siguientes funcionalidades:</p> <ul style="list-style-type: none"> ▪ Firewall (Endpoint Firewall). ▪ Control de Aplicaciones (Application Control). ▪ Cumplimiento (Endpoint Compliance) ▪ Anti-Virus. ▪ Anti-Ransomware. ▪ Anti-Bot (Protección contra máquinas infectadas de malware). ▪ Anti-Exploit. ▪ Protección de Puertos (Port Protection). ▪ Protección contra Phishing de Día-Cero. ▪ Protección de contraseñas corporativas (opcional)¹. ▪ Mapa de Captura de Amenazas (Threat Hunting). ▪ Análisis Forense. ▪ Mapa de amenazas basado en MITRE ATT&CK. ▪ Emulación de Amenazas de Día-Cero (Sandboxing). ▪ Extracción de Amenazas ▪ Captura de Amenazas (Threat Hunting). ▪ Inteligencia de Amenazas y Gestión de IoC (Indicadores de Compromiso). ▪ Capacidades de Respuesta y Remediación Extendida (XDR). <p>f. La solución de seguridad deberá notificar y mandar alertas mediante correo electrónico y/o SMS sobre la desatención/desinstalación/desactivación y/o amenazas del equipamiento protegido con dicha solución.</p> <p>g. La consola de administración deberá estar en idioma español y/o inglés.</p>
Firewall (endpoint firewall)	<p>a. Debe proporcionar la capacidad de implementar políticas de firewall sobre el Endpoint y gestionarlo de forma centralizada, controlando tráfico entrante, saliente y los servicios asociados, y registrando los eventos sobre cada regla implementada.</p>

¹ En atención a la consulta N° 29

	<ul style="list-style-type: none"> b. Debe permitir la creación de zonas de seguridad (redes confiables) a través de diferentes objetos como: hosts, rango de direcciones IP, redes, grupos de redes y dominio, con diferentes permisos controlado accesos no autorizados. c. Capacidad de permitir o no en los equipos de usuario final, conectarse a redes Wireless cuando se encuentra conectado a redes LAN.
Control de aplicaciones (application control)	<ul style="list-style-type: none"> a. Debe permitir el control de aplicaciones por política (grupos de equipos) o de forma global. b. Debe restringir el acceso a la red de aplicaciones específicas, para lo cual el administrador podrá definir políticas y reglas con acciones de: permitir, bloquear y finalizar las aplicaciones y procesos. También se debe poder configurar, que una aplicación finalice cuando intente acceder a la red, o evitar que una aplicación se inicie al intentar ejecutarla. c. Debe permitir configurar reglas detalladas para programas de software, y tomar acción como permitir o bloquear versiones específicas de un mismo software. Cada versión de aplicación debe ser identificado con un hash único y entidad firma (certificado). d. Debe tener capacidad de realizar un inventario detallado de las aplicaciones preexistentes en los equipos de usuario final y sobre la base de dicho inventario, realizar políticas y reglas de control. e. Los usuarios administradores deben tener la opción de terminar un proceso potencialmente peligroso. f. Debe permitir personalizar listas negras y blancas de aplicaciones.
Cumplimiento (endpoint compliance)	<ul style="list-style-type: none"> a. Debe poder establecer una política de cumplimiento en las estaciones de usuario final, sobre la base de diversos controles de cumplimiento que deben ser verificados en los equipos. b. Las acciones de cumplimiento por cada política infringida (no cumplimiento) deberá ser: observar (solo registra actividad), alertar y restringir (en ambos casos notifica y permite acciones de remediación). c. Las etapas de cumplimiento deberán ser como mínimo: cumplimiento, próximo a ser restringido (opcional) y restringido o no cumplimiento.²⁻³ d. A través de las políticas de cumplimiento se debe poder restringir al equipo, si se encuentra que la política no está siendo cumplida. e. Los controles de cumplimiento deben ser personalizables, se deben poder crear controles basados en: tipo de sistema operativo, un valor específico del registro de Windows, la existencia o no de un archivo en particular, en una ruta específica y con opciones de verificar las propiedades del archivo tales como versión, antigüedad del archivo y hash MD5. f. El control de remediación debe ser personalizables por cada control de cumplimiento, es decir cada control de cumplimiento puede tener asociado una acción de remediación. Las acciones de remediación deben poder ejecutar un programa o script en particular que puede ser descargado de una ruta URL específica, y tener la capacidad de ejecutar la remediación empleando los permisos de cuenta del sistema local o la del usuario. g. Los mensajes de alerta de incumplimiento deben ser personalizables por cada control de cumplimiento, es decir cada control de cumplimiento puede tener asociado un mensaje de alerta. h. Debe validar también controles tales como, service pack en sistema operativo, Anti-Virus/Anti-Malware tanto propias y opcionalmente de terceros instalados y actualizadas⁴⁻⁵.

² En atención a la observación N° 24

³ En atención a la observación N° 41

⁴ En atención a la consulta N° 28

⁵ En atención a la observación N° 43

	i. Debe validar que todos los componentes de seguridad asignados al de usuario y/o equipo final, están instalados y en ejecución en el Endpoint.
Anti-virus (anti-malware)	<ul style="list-style-type: none"> a. Debe trabajar con base de firmas de archivos, bloqueo por basado en comportamiento. b. Anti-Malware debe proteger contra ataques "día cero" y bloquear la instalación de malware a través de sitios web c. Debe proporcionar una manera de informar a los usuarios finales con alertas o informes de análisis locales relacionados con la actividad del Anti malware d. Debe permitir las siguientes opciones de tratamiento de sobre antivirus o antispyware; reparación y/o limpieza, cuarentena y borrado.⁶
Anti-ransomware	<ul style="list-style-type: none"> a. Debe tener protección específica contra malware del tipo ransomware que posea detección automática, bloqueo y eliminación de este tipo de amenazas. b. Debe tener capacidad de monitorear actividad de los archivos y la red, sobre comportamiento sospechosos. Debe detener el ataque inmediatamente cuando detecta que el ransomware modifica los archivos. c. Debe tener la capacidad de restaurar archivos que fueron cifrados por el ransomware, como parte de la recuperación automática (remediación), en su ubicación original o en una ubicación alterna que se defina. d. Debe ser posible definir un límite de espacio y frecuencia para el resguardo de los archivos y/o contar con mecanismos para la recuperación de archivos cifrados por el ransomware⁷. e. Debe proteger contra ataques de Ransomware basado en el uso de herramientas de cifrado de volumen en bloque (tales como BitLocker y herramientas similares). f. Debe tener capacidad de protección de ransomware en carpetas compartidas en la red. Todas las carpetas compartidas están protegidas.
Protección contra máquinas infectadas de malware (anti-bot)	<ul style="list-style-type: none"> a. Debe identificar equipos infectados por Bots y bloquear la comunicación del bot hacia sitios de C&C; para asegurar de que no se robe ni se envíe información confidencial fuera de la organización. b. Debe utilizar una base de datos en nube del propio fabricante para recibir actualizaciones y consultar la clasificación de la: IP, URL y recursos DNS no identificados.
Prevención contra exploits	<ul style="list-style-type: none"> a. Debe proporcionar protección contra ataques basados en exploits que comprometen aplicaciones legítimas como los navegadores y Microsoft Office. b. Identificar manipulaciones sospechosas de memoria en tiempo de ejecución. Al detectarse, el Anti-Exploit deberá terminar todos los procesos de Exploit, corregir la cadena de ataque completamente y desencadenar una Informe forense.
Protección de puertos (port protection)	<ul style="list-style-type: none"> a. Controla en base a políticas, el acceso del dispositivo a todos los puertos disponibles (USB, Firewire, Bluetooth, entre otros) b. Las políticas definen los derechos de acceso para cada tipo de dispositivo de almacenamiento extraíble y los puertos a los que se pueden conectar. La política también evita que los usuarios conecten dispositivos no autorizados a las computadoras. c. Debe controlar (permitir o bloquear) la entrada y salida en todos los puertos de conexión, específicamente: <ul style="list-style-type: none"> ▪ Medios de almacenamiento USB, unidades DVD/CD-ROM; Módems, Impresoras, Controladores USB ▪ Dispositivos de captura de imágenes (Ej.: Cámaras digitales, Web Cams, scanner, etc.), Dispositivos Infrarrojos, Smart Card Readers, Memorias PCMCIA ▪ Adaptadores de red tanto cableados como inalámbricos, adaptador Bluetooth, Bluetooth USB.

⁶ En atención a la consulta N° 44

⁷ En atención a la consulta N° 15

	<ul style="list-style-type: none"> d. Debe poder crear listas blancas (permitido) y listas negras (denegado) para control de medios extraíbles y/o dispositivos de E/S en cualquier puerto (USB, Firewire, Bluetooth). e. Debe poder controlar medios extraíbles por su número de serie, lo que permite la creación de políticas para dispositivos únicos y específicos.
Protección contra phishing de día-cero o Phishing no conocido⁹	<ul style="list-style-type: none"> a. Debe contar con capacidad de prevención de Phishing de día cero o Phishing no conocido, debe tener la capacidad de detectar y prevenir⁹⁻¹⁰. b. La prevención de phishing verifica diferentes características de un sitio web para asegurarse de que un sitio no pretenda ser un sitio diferente y use información personal de manera maliciosa. c. Debe poner analizar phishing de día-cero o phishing no conocido en sitios que son accedidos a través de navegadores basados en: Edge, Chrome y Brave¹¹. d. Debe ser compatible con los navegadores actuales de MS Edge, Firefox y Chrome. e. Los mensajes de alerta o bloqueo al usuario final deben ser configurables.
Protección de contraseñas corporativas (opcional)¹²	<ul style="list-style-type: none"> a. Debe proteger las credenciales (contraseña) corporativas, con la capacidad de prevenir y alertar. b. Opcionalmente, debe alertar y prevenir que los usuarios utilicen las contraseñas corporativas, tanto en aplicaciones web corporativas, como en sitios o dominios externos no-corporativos (Ej. Redes sociales)¹³. c. Se debe poder configurar que dominios internos y/o corporativos debe ser protegidos por esta funcionalidad. d. Debe ser compatible con los navegadores actuales de MS Edge, Firefox y Chrome. e. Los mensajes de alerta o bloqueo al usuario final deben ser configurables.
Análisis forense	<ul style="list-style-type: none"> a. Debe construir automáticamente informes forenses, entregando visibilidad completa del alcance, daño o severidad y vectores del ataque, incluyendo: <ul style="list-style-type: none"> ▪ Actividades sospechosas (conexiones y procesos relacionados al ataque). ▪ Actividades de Remediación (procesos terminados, archivos en cuarentena o eliminados, archivos restaurados en el caso de Ransomware). ▪ Impacto al negocio del incidente, como archivo exfiltrados o cifrados por ransomware. ▪ Detalle de la línea de tiempo del Incidente para determinar si es una infección. b. Debe mostrar un reporte forense detallado, que incluya el mapa o matriz del Framework MITRE ATT&CK, el cual mostrara las tácticas y técnicas de compromiso que fueron ejecutadas por el atacante. c. Debe mostrar los elementos maliciosos que fueron remediados (cuarentena). d. Debe indicar el punto de entrada del ataque (ej. Navegador, puerto USB, red interna, etc.)
Emulación de amenazas de día-cero (sandboxing)	<ul style="list-style-type: none"> a. Debe tener capacidad de detección y prevención de malware no conocido. Para ello, el software deberá realizar la emulación del malware en la nube del propio fabricante, en donde se analiza y detecta amenazas no conocidas o de día cero. b. Debe proteger contra los ataques de múltiples vectores de amenazas que llegan a través de descargas de la web, contenido copiado de medios de almacenamientos extraíbles, enlaces o

⁹ En atención a la consulta N° 35

⁹ En atención a la consulta N° 48

¹⁰ En atención a la observación N° 51

¹¹ En atención a la consulta N° 50

¹² En atención a la consulta N° 29

¹³ En atención a la observación N° 51

	<p>archivos adjuntos en mensajes de correo electrónico, movimiento lateral de datos y malware entre segmentos de red e infecciones a través de contenido cifrado.</p> <p>c. Debe permitir combinación de capacidades avanzadas de machine learning, análisis de comportamiento dinámico de Sistema Operativo, identificación de comportamientos maliciosos y sospechosos, tácticas de hacking y técnicas de ingeniería social, análisis de comunicaciones de C&C durante el análisis de Sandboxing</p> <p>d. El Sandboxing debe soportar al menos 30 tipos de archivos, incluyendo: Adobe PDF, Microsoft Word, Excel, PowerPoint, Ejecutables (EXE, COM, SCR, Flash SWF, RTF, Zip)¹⁴.</p> <p>e. Debe ser posible realizar emulación a nivel sistema operativo y/o a nivel CPU.¹⁵</p> <p>f. Debe ser posible analizar las amenazas evitando las técnicas de evasión como VM Detection, Time Delays, Interacción Humana, etc.</p> <p>g. Debe ser posible analizar Adobe Flash & Javascript.</p> <p>h. Debe ser posible remover el contenido activo de los archivos Office</p> <p>i. Debe utilizar Machine Learning, análisis de Macros y ambientes de emulación Windows XP, Windows 7, Windows 8.1 y/o Windows 10 o superior¹⁶.</p> <p>a. Debe analizar todas las descargas de archivos sobre canal HTTP, HTTPS y ser integrado con los navegadores MS Edge, Firefox, Google Chrome y Brave.</p> <p>b. Debe tener capacidad de prevención de amenazas de internet, a través del filtrado de contenido y acceso a sitios de internet que representan riesgos informáticos.</p> <p>c. Debe prevenir el acceso a los sitios categorizados de riesgo tales como: anonymizer, botnets, phishing, spam, spyware, sitios maliciosos y sitios inactivos.</p> <p>d. Debe tener la capacidad de crear listas negras (denegar) sobre sitios, dominios y direcciones IP específicas de Internet.</p> <p>e. Opcionalmente, debe tener la capacidad de permitir al usuario acceder al sitio restringido (configurable por política)¹⁷.</p>
Extracción de amenazas (Threat extraction)	<p>a. Protege proactivamente a los usuarios del contenido malicioso. Para todas las descargas de internet entrega archivos seguros mientras se inspeccionan los archivos originales en busca de posibles amenazas.</p> <p>b. Para todas las descargas de archivos de internet, se debe tener las siguientes capacidades:</p> <ul style="list-style-type: none"> Extracción y Prevención. - El usuario final recibe una versión limpia del archivo (se retiran los elementos activos de riesgo). El administrador puede seleccionar qué partes maliciosas extraer del archivo basado en nivel de riesgo. Por ejemplo, Macros, Java Scripts, etc. Opcionalmente, debe poder transformar el archivo en PDF y se obtienen una versión benigna del archivo en formato PDF, en tanto el archivo original es emulado. Cuando la emulación termina el usuario recibe el archivo original. También se puede determinar que se suspenda la descarga hasta que termine con la emulación¹⁸. Detección. - Se emula el archivo sin detener la descarga del archivo original.
Captura de Amenazas (Threat Hunting)	<p>a. Debe proveer una herramienta de investigación que permite realizar consultas avanzadas sobre todos los eventos forenses maliciosos y benignos recopilados de los terminales que cuenta con el software de seguridad instalado.</p> <p>b. La información recopilada debe permitir:</p> <ul style="list-style-type: none"> Investigue el alcance completo de un ataque.

¹⁴ En atención a la consulta N° 53

¹⁵ En atención a la consulta N° 32

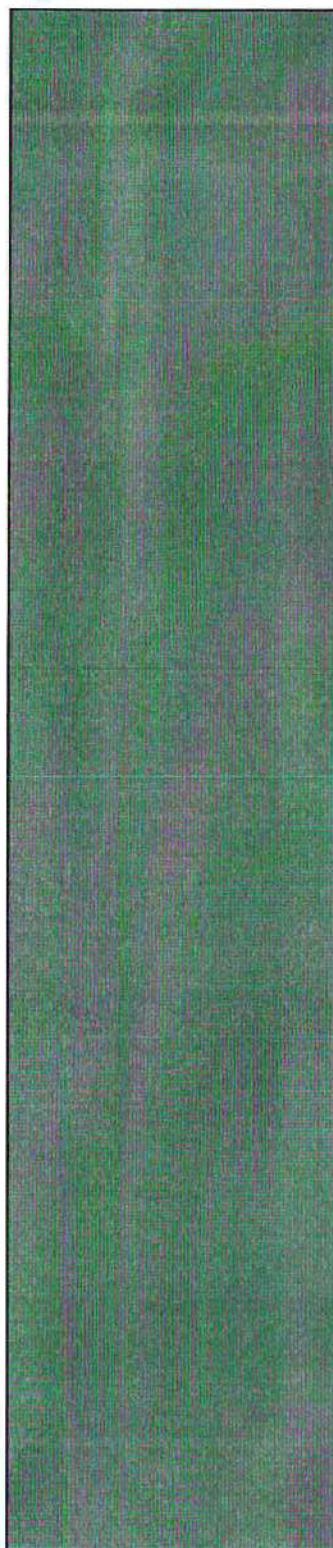
¹⁶ En atención a la consulta N° 56

¹⁷ En atención a la consulta N° 60

¹⁸ En atención a la observación N° 62

	<ul style="list-style-type: none"> ▪ Descubrir un ataque sigiloso mediante la observación de una actividad sospechosa. ▪ Reparar el ataque antes de que cause más daño. ▪ Busque de forma proactiva ataques avanzados mediante la búsqueda de anomalías y el uso de pistas de búsqueda. <p>c. La caza de amenazas debe permitir:</p> <ul style="list-style-type: none"> ▪ Recopilación y enriquecimiento de datos: todos los eventos se recopilan a través de múltiples sensores en el producto antimalware, se envían a un repositorio unificado y se complementan con información de inteligencia de amenazas, mapa de MITRE y alertas de todos los motores de prevención de amenazas. ▪ Consultas predefinidas y un panel de MITRE que mapean toda la actividad y permite el inicio rápido a la búsqueda proactiva de amenazas. ▪ Acciones de remediación por cada resultado o de manera masiva, para tomar acciones como la cuarentena de archivos, terminar procesos, iniciar análisis forense y aislar equipos. <p>d. Los datos del mapa de captura de amenazas se deben almacenar con un periodo mínimo de treinta días.</p>
<p>Capacidades de remediación y respuesta extendida</p>	<p>a. Debe tener capacidades de remediación automáticas y manuales que requieran acción del administrador.</p> <p>b. Debe permitir la detección automática temprana y respuesta a eventos de seguridad en todos los productos antimalware gestionados, para poder eliminar falsos positivos.</p> <p>c. Debe correlacionar varios registros de seguridad notificado por el producto antimalware, en un solo incidente de seguridad.</p> <p>d. Los incidentes de seguridad deben tener los estados de: nuevo, asignado, en proceso y cerrado o similares.</p> <p>e. Debe mostrar una vista general de línea de tiempo de todos los incidentes de seguridad agrupados e identificados por severidad (crítico, alto, medio, bajo) mediante colores.</p> <p>f. Debe brindar una comprensión integral de la postura de seguridad de la organización, para permitir tomar medidas más confiables y efectivas que permitan mitigar y prevenir ataques.</p> <p>g. Debe tener capacidad de detecciones avanzadas de UEBA (User Entity Behavioral Analytics).</p> <p>h. La plataforma debe crear los incidentes de manera manual, y estos deben ser asignados a un analista de seguridad.</p> <p>i. Cada incidente de seguridad asociado a un analista debe tener la siguiente información:</p> <ul style="list-style-type: none"> ▪ Nivel de prioridad. ▪ Fuente Origen. ▪ Tácticas de MITRE ATT&CK involucradas. ▪ Activos involucrados. ▪ Indicadores de compromiso identificados. ▪ Acciones de prevención realizadas y acciones de prevención recomendadas. ▪ Cronología (línea de tiempo) del incidente. <p>j. Las capacidades de análisis de cada incidente deben permitir tener una vista detallada de:</p> <ul style="list-style-type: none"> ▪ Información y análisis forense para ver procesos, archivos, URL, dominios y registros involucrados en la información y relacionados con el incidente. ▪ Indicadores (IoC) y artefactos para ver los indicadores y artefactos relacionados con el incidente. ▪ Árbol de ataque para ver una representación gráfica del informe forense generado por el producto para el Endpoint es para cada detección realiza. ▪ MITRE para conocer las tácticas MITRE ATT&CK utilizadas en el incidente. <p>k. Debe contar con un módulo de Inteligencia de Amenazas, que nos permita tener contexto a través de fuentes del propio fabricante, así como de fuentes terceras, con los siguientes datos:</p> <ul style="list-style-type: none"> ▪ Información del indicador de compromiso y/o peligro (IoC) en una descripción general de alto nivel del indicador analizado.

	<ul style="list-style-type: none"> ○ Para dominios y URL, muestra una captura de pantalla en vivo del sitio web. ○ Para los archivos, muestra el detalle del hash del archivo: MD5, SHA1 y SHA256 ○ Visto por primera vez: fecha en que se vio el archivo por primera vez. ○ Visto por última vez: fecha en que se vio el archivo por última vez. ▪ Información de Research o Búsqueda que muestre para Dominios y URLs: <ul style="list-style-type: none"> ○ Datos del Whois, muestra usuarios registrados de un recurso de Internet, como un nombre de dominio o un bloque de direcciones IP. ○ Datos de reputación resumidos en este dominio. ○ Subdominios asociados para este dominio. ○ URL relacionadas a este dominio. ○ Comunicando archivos que se vieron comunicándose con el dominio buscado. ○ Archivos descargados de este dominio. ○ Producto antimalware de usuario utilizado para ponerse en contacto con este dominio durante un evento malicioso. ▪ Información de Research o Búsqueda que muestre para Archivos: <ul style="list-style-type: none"> ○ Los nombres de archivo observados por el fabricante para este tipo de archivo. ○ El tráfico de red que creó el archivo durante la emulación de amenazas. ○ Solicitudes DNS del archivo creados durante la emulación de amenazas. ○ Proceso principal (parent process) que creó el archivo. ○ El hash del archivo de archivo disponible. ○ URL de origen desde las que se descargó el archivo. ○ Asuntos de correo electrónico que contienen este archivo, como archivo adjunto. ▪ Información de análisis de tráfico global: <ul style="list-style-type: none"> ○ Geolocalización, para el uso del IoC en diferentes ubicaciones geográficas. ○ Muestra los tres principales países que tienen el mayor número de visitas para este IoC. ○ Muestra las tres principales industrias donde se vio este IoC. ○ Tipos de plataformas que accedieron al indicador (Ejemplo, Web, Correo electrónico). ○ Número de eventos en estado salvaje a lo largo del tiempo para el IoC. l. Debe permitir crear indicadores de compromiso sobre la base de cada uno de los incidentes, y sobre la base de estos IoC, tomar las siguientes acciones de prevención manera automática o manual: <ul style="list-style-type: none"> ▪ Crear el IoC en la gestión de IoC (para prevención o detección). ▪ Aislar un Endpoint a través del producto antimalware. ▪ Poner en cuarentena un archivo través del producto antimalware. ▪ Matar un proceso través del producto antimalware. m. Debe permitir crear respuesta automática en base al nivel de confianza y severidad de los indicadores de compromiso (IoC) sobre la base de cada uno de los incidentes, para que estos puedan ser habilitados en el gestor de IoC y su posterior aplicación por el producto antimalware. n. Se debe poder crear notificaciones automáticas ante la prioridad de un incidente (crítica, alta, media) empleando correo electrónico y/o canales de Microsoft Teams (URL).
<p>Consola de administración & eventos</p>	<p>a. La consola de administración deberá estar alojada en nube provista por el fabricante y deberá administrar centralizadamente todos los equipos que cuentan con el producto, a través de internet.</p>

	<ul style="list-style-type: none">b. El acceso a consola de administración en nube, debe soportar doble factor de autenticación (MFA) a través de Google Authenticator y Microsoft Authenticator.c. El acceso a consola de administración en nube, debe soportar integración con proveedores de identidad (IdP) tales como Microsoft ADFS, Microsoft Azure AD, Okta y otros basados en SAML.d. Debe tener capacidad de gestión de equipos finales, integrado con el Directorio Activo Microsoft existente on-premise, a través de los productos antimalware que realicen la función de scanner, para importar el árbol de equipos internos en red LAN.e. Debe ser capaz de crear log de seguridad, de tal forma que se tenga información ante un incidente de seguridad.f. Debe contar con un módulo que permita ver en forma general cual es el estado de los puntos finales, así como las alertas que están activas.g. Debe permitir la configuración de políticas de todos los módulos para los equipos de usuario final.h. Debe tener un módulo que permita hacer seguimiento de cada módulo de seguridad instalado en los puntos finales, de tal forma que podamos tener información relevante de los usuarios y PC por módulo de seguridad instalado en los productos antimalware.i. Debe contar con un módulo que permita configurar todo lo relacionado al modo de implementación o despliegue de los productos antimalware. El despliegue se podrá realizar mediante archivo MSI o paquetes completos pre-configurados.j. Debe contar con un módulo de vista operacional, que permita mostrar la siguiente información:<ul style="list-style-type: none">▪ El tipo de Endpoint sea desktop o laptop u opcional.▪ El tipo del SO en el Endpoint y servidores (Windows, MacOS, Linux).▪ Versión del producto antimalware desplegado.▪ El resumen de estado del despliegue de cada producto antimalware.▪ Versiones del Sistema Operativo empleado.▪ Actualizaciones de las firmas anti-malware y si estas presentan algún desfase en la actualización.k. Debe contar con un módulo de reportes que permite mostrar la siguiente información:<ul style="list-style-type: none">▪ Reporte análisis de amenazas.▪ Cyber Ataques de alto riesgo▪ Opcionalmente, debe poder transformar el archivo en PDF y se obtienen una versión benigna del archivo en formato PDF, en tanto el archivo original es emulado. Cuando la emulación termina el usuario recibe el archivo original. También se puede determinar que se suspenda la descarga hasta que termine con la emulación¹⁹.▪ Reporte de Emulación de Amenazas▪ Reporte de Extracción de Amenazas (opcional)²⁰.▪ Reporte de Cumplimiento▪ Reporte de Despliegue de Productol. Debe contar con un módulo de vista de seguridad que permita mostrar la siguiente información:<ul style="list-style-type: none">▪ Hosts bajo ataque y ataques activos.▪ Ataques limpiados y bloqueados.▪ Hosts infectados.▪ Línea de Tiempo de los ataques.
--	---

6.2.1.2. Plan de Trabajo

- a. El contratista deberá elaborar un plan de trabajo y realizar una presentación del mismo en la reunión del kick-off, hasta los diez (10) días calendario posteriores

¹⁹ En atención a la consulta N° 68

²⁰ En atención a la consulta N° 69



a la firma del contrato.

- b. El contratista, como parte del kick-off deberá exponer el plan de trabajo elaborado, el cual será revisado con el personal de la Unidad de Tecnologías de la Información para su posterior aprobación, en un plazo no mayor a dos (02) días calendario.

6.2.1.3. Implementación

- a. El contratista será responsable de realizar todas las actividades para la implementación del servicio ofertado.
- b. El contratista deberá realizar la instalación de la solución en su integridad procediendo a la desinstalación de la solución de seguridad en las estaciones de trabajo de los usuarios finales, servidores y/o consola de administración ya implementada, a la culminación de la vigencia del servicio de suscripción de antivirus con la cual cuenta la entidad, sin afectación a los sistemas, estaciones de trabajo y equipos de tipo servidor.
- c. La activación de las licencias se realizará de acuerdo a las coordinaciones realizadas con el personal de la Unidad de Tecnologías de la Información.
- d. Para la implementación de la solución de seguridad se debe considerar dos (02) fases:
 - Primera Fase: Se realizará el despliegue de 1529 agentes lo cual incluye estaciones de trabajo y servidores (1409 estaciones de trabajo y 120 servidores).
 - Segunda Fase: Se realizará el despliegue de 90 agentes el cual incluye servidores.
- e. Para la implementación de los agentes restantes y completar el total de licencias adquiridas, estos deberán ser instalados a demanda y a solicitud de la Unidad de Tecnologías de la Información – UTI.
- f. El contratista deberá implementar la solución contratada en coordinación con la UTI sin afectar la operatividad de los servicios y/o sistemas; para los trabajos que requieran de una ventana de corte programado, estos se realizarán en días y/o horarios no laborales y deberá estar autorizado por la Unidad de Tecnología de la Información de la Autoridad de Transporte Urbano para Lima y Callao – ATU, quien a su vez ha de gestionar las autorizaciones correspondientes para que el contratista pueda realizar las labores de instalación dentro de las áreas destinadas para tal fin.
- g. El contratista deberá implementar un mecanismo de seguridad para la protección de los sistemas operativos en los equipos que a la fecha no cuenten con soporte de fabricante por versión y/o compatibilidad.

6.2.1.1 Transferencia de conocimiento

- a. El Contratista deberá brindar un entrenamiento técnico en el producto antimalware ofertado. El curso deberá ser brindado para cuatro (04) profesionales designados por la Unidad de Tecnología de la Información – UTI, y deberá ser dictado de manera virtual por un periodo de ocho (08) horas lectivas. Como mínimo se deberá consignar el siguiente temario:
 - Despliegue y configuración de agentes.
 - Arquitectura y componentes.
 - Reportes, Dashboards.
 - Prevención y Detección de amenazas.
 - Respuesta ante incidentes.
 - Mejores prácticas de implementación y administración.
 - Casos de uso, uso de las características y ejemplo prácticos.
- b. El entrenamiento técnico será programado en coordinación con el personal de la Unidad de Tecnologías de la Información – UTI, el cual no podrá exceder los cuarenta y cinco (45) días calendario posteriores al despliegue de la primera fase.

6.2.2. Prestación accesoria

6.2.2.1 Soporte Técnico

- a. El contratista brindará la asistencia técnica sobre el producto ofertado, asegurando la disponibilidad del mismo teniendo en cuenta lo siguiente:
- La solución deberá notificar los incidentes de seguridad que se identifiquen como potencialmente peligrosos (crítico) para cualquier activo de la entidad, los cuales deberán ser atendidos, aperturando automáticamente el ticket de atención por cada incidente tipificado como crítico, con la siguiente información:
 - ✓ Fecha y hora.
 - ✓ Tipo de incidente.
- b. El contratista deberá atender todo requerimiento de seguridad que el personal de la Unidad de Tecnología de la Información – UTI reporte para revisión y atención mediante los diferentes canales brindados.
- c. El Contratista deberá contar con una Mesa de Ayuda, bajo los siguientes requerimientos de tiempo de respuesta, para atención de incidentes durante la vigencia del periodo del servicio contratado:
- c.1. Tiempo de Respuesta Mesa de Ayuda:** Si el reporte se realizara vía telefónica, la atención será en un plazo de atención no mayor a dos (02) minutos a partir de la primera llamada realizada, asimismo si el reporte de atención fuera vía correo electrónico, debiéndose generar inmediatamente el ticket de atención correspondiente.
- c.2. Tiempo de Solución Temporal:** De acuerdo con lo indicado conforme a lo descrito en el inciso c1., del numeral 6.2.2.1., a partir del momento en que el personal de la Unidad de Tecnologías de la Información de la Autoridad de Transporte Urbano para Lima y Callao – ATU, genere el ticket de atención respectivo para determinar la atención del incidente, las mismas que se encuentran descritas en el cuadro SLA.
- d. El Contratista deberá garantizar el cumplimiento de los siguientes Acuerdos de Niveles de Servicios (SLA) ante los requerimientos de incidentes de seguridad de la solución: El cumplimiento es obligatorio de los procedimientos y se encuentra debidamente detallado y dependerá de las repercusiones que tenga en los requerimientos que el Contratista presta a la Autoridad de Transporte Urbano para Lima y Callao – ATU, a demanda:
- Tiempo de Resolución:** Una vez reportado el incidente de seguridad el Contratista dispondrá del tiempo relacionado en el siguiente cuadro, donde el tiempo de respuesta hace referencia a la cantidad de tiempo que transcurre desde que se reporta el incidente de seguridad hasta que se da respuesta; solución temporal es una acción urgente para salir del incidente pudiendo encontrarse la operación en condiciones inferiores al nivel pactado y el tiempo de resolución es restablecer las condiciones normales del servicio y haber solucionado de manera definitiva el problema. A continuación, se detallan los niveles de servicios para la atención de requerimientos de incidentes de seguridad, y su cumplimiento es obligatorio:

ACUERDOS DE NIVELES DE SERVICIOS (SLA) (Equipos de tipo usuario final / Equipos de tipo servidor)			
Nivel de atención	Tiempo de Respuesta (mesa de ayuda)	Solución temporal	Tiempo de resolución
Nivel 1	02 minutos	30 minutos	02 horas
Nivel 2	02 minutos	40 minutos	02 horas
Nivel 3	02 minutos	50 minutos	03 horas
Nivel 4	02 minutos	01 hora	03 horas

En caso de que la atención deba ser escalada al fabricante el tiempo para la resolución definitiva de los incidentes reportados no deberá excederse en más de cuatro (04) horas de respuesta después del tiempo de resolución establecido en los SLA del cuadro anterior, esta atención deberá ser comunicado y autorizada por la Unidad de Tecnologías de la Información - UTI de la Autoridad de Transporte Urbano para Lima y Callao – ATU, previo informe técnico inmediato elaborado por el Contratista donde se describa el incidente.

DONDE:

- **Nivel de atención 1 (Crítico):** Se considera un incidente de Nivel 1 aquel

- que su impacto paralice totalmente la(s) operación(es) de los servicios que brinda la entidad.
 - **Nivel de atención 2 (Alto):** Se considera un incidente de Nivel 2 aquellos que tengan impacto en la degradación o intermitencia de los servicios de la entidad.
 - **Nivel de atención 3 (Medio):** Se considera un incidente de Nivel 3 aquellos que producto de las capacidades ofertadas en el servicio afecten más de un equipo computo de la entidad.
 - **Nivel de atención 4 (Bajo):** Se considera incidente Nivel 4 aquellos que susciten riesgo para algún activo informático de la entidad.
- e. Por cada reporte de incidencia de seguridad que tenga impacto en la continuidad operativa de los servicios de TI, el Contratista deberá realizar y presentar un informe a la Autoridad de Transporte Urbano para Lima y Callao – ATU, vía mesa de partes virtual (https://soluciones.atu.gob.pe/portal_ciudadano/login) o presencial, el cual contendrá como mínimo la siguiente información:
- Descripción detallada del problema, su causa y solución encontrada.
 - Personal asignado para la resolución del mismo.
 - Problemas presentados durante resolución.
 - Documentación adjunta de los cambios hechos.
 - Recomendaciones.
 - Fecha y hora de resolución.
- f. De presentarse un incidente de seguridad que no pueda resolverse de forma remota, el Contratista deberá desplegar un personal insitu para atención en cualquier sede desconcentrada de la entidad.
- g. El Contratista brindará un soporte técnico remoto por el servicio contratado por un periodo de setecientos treinta (730) días calendario, debiendo presentar un informe trimestral por la prestación brindada (Siendo un total de 8 informes trimestrales).

6.3. CONDICIONES DEL SERVICIO

- a. Es de responsabilidad del contratista contemplar todas las actividades, dispositivos, componentes y accesorios para la instalación y ejecución del servicio requerido en los plazos establecidos.
- b. El contratista es el único responsable del cumplimiento de la implementación y soporte del servicio ante la Autoridad de Transporte Urbano para Lima y Callao – ATU, de cumplir con la prestación contratada, no pudiendo transferir dicha responsabilidad a terceros; es decir, el contratista no podrá subcontratar las actividades generadas por la prestación principal o prestaciones accesorias.
- c. En el caso de que el contratista requiera realizar un corte en el servicio, éste deberá ser programado y deberá contar necesariamente con la aprobación y autorización de la Unidad de Tecnología de la Información – UTI de la Autoridad de Transporte Urbano para Lima y Callao – ATU, debiendo considerar que las actividades se realicen fuera del horario laboral.
- d. La suscripción de la solución de seguridad avanzada antimalware requerido, deberá estar a nombre de la Autoridad de Transporte Urbano para Lima y Callao – ATU, manteniéndose activas por un periodo de setecientos treinta (730) días calendario.

7. ENTREGABLES

A efectos de cumplir con las actividades encomendadas, el contratista deberá presentar a través de la Mesa de Partes de la Autoridad de Transporte Urbano para Lima y Callao – ATU, ubicado en la Calle José Gálvez 550, Miraflores o en su defecto a través de la Mesa de Partes Virtual: https://soluciones.atu.gob.pe/portal_ciudadano/login, los siguientes entregables:

7.1. Prestación Principal

N°	ENTREGABLES	DETALLE
01	Plan de Trabajo	El contratista, deberá presentar un plan de trabajo, el mismo que estará sujeto a la evaluación y aprobación por parte de la Unidad de Tecnologías de la Información de la Autoridad de Transporte Urbano para Lima y Callao – ATU. Debiendo contener como mínimo la siguiente información: <ul style="list-style-type: none">▪ Objetivos y alcance del servicio.▪ Roles y responsabilidades del equipo para la implementación de la solución

		<p>integral y el despliegue correspondiente.</p> <ul style="list-style-type: none"> ▪ Cronograma, que incluya la información necesaria para la implementación del servicio (hitos, actividades, responsables, ventanas de tiempo y riesgos). ▪ Matriz de escalamiento para el soporte y gestión de operaciones, el cual debe incluir cuentas de correo u número telefónicos. ▪ Protocolo de pruebas y validación de la solución ofertada.
02	Informe de la implementación de la Primera Fase	<p>El contratista deberá presentar un informe de la implementación de la primera fase. Debiendo presentar lo siguiente:</p> <ul style="list-style-type: none"> ▪ Detalle de la instalación, como cantidad de estaciones de trabajo y servidores con la solución de seguridad instalada. ▪ Acta de implementación de la solución de protección antimalware de la primera fase, firmada entre el contratista y la Unidad de Tecnología de la Información – UTI.
03	Informe de la implementación de la Segunda Fase	<p>El contratista deberá presentar un informe de la implementación de la segunda fase. Debiendo presentar lo siguiente:</p> <ul style="list-style-type: none"> ▪ Detalle de la instalación, como cantidad de servidores con la solución de seguridad instalada. ▪ Documento de activación que certifique la vigencia de la solución ofertada ante la Autoridad de Transporte Urbano para Lima y Callao – ATU, por el periodo contratado. ▪ Acta de implementación de la solución de protección antimalware de la segunda fase, firmada entre el contratista y la Unidad de Tecnología de la Información – UTI. ▪ El contratista deberá presentar el informe del entrenamiento técnico, debiendo presentar lo siguiente: <ul style="list-style-type: none"> ○ La lista de asistencia del personal capacitado. ○ Material técnico – didáctico utilizado. ○ Certificado del curso de capacitación en el producto ofertado.

7.2. Prestación Accesorio

7.2.1. Soporte Técnico

El contratista deberá presentar un informe trimestral de soporte, actualizaciones y reportes de incidentes de seguridad del servicio de antimalware contratado, hasta los cinco (05) días calendario culminado el periodo. El cual se contabilizará a partir de la activación de la suscripción de la solución avanzada de antimalware. Debiendo presentar lo siguiente:

- Reporte de atenciones y acciones realizadas.
- Mejoras en la herramienta (actualizaciones desplegadas).
- Top 50 de vulnerabilidades de seguridad encontradas.
- Propuesta de mejoras a nivel de seguridad.

8. PERSONAL CLAVE

8.1. Requisitos del Personal clave

8.2.1. Un (01) Gestor de Proyecto:

Tendrá bajo su responsabilidad:

- Liderar el proceso de implementación y el equipo que formará parte de la implementación.
- Coordinará con el personal de la Unidad de Tecnologías de la Información – UTI, las actividades a realizar durante dicha implementación.

8.2.2. Un (01) Implementador/capacitador:

Tendrá bajo su responsabilidad:

- La implementación del servicio de antimalware contratado en su integridad bajo los requerimientos de la solución ofertada.
- La transferencia de conocimientos al personal de la Unidad de Tecnologías de la Información de la Autoridad de Transporte Urbano para Lima y Callao, en el uso de la solución de seguridad ofertada.

9. LUGAR DE LA PRESTACIÓN DEL SERVICIO

El contratista deberá ejecutar el servicio en su integridad de manera presencial en la Av. Domingo Orué #165 - 3er. Piso, distrito de Surquillo, o de manera virtual a solicitud y en coordinación con la Unidad de Tecnologías de la Información – UTI.

10. PLAZO DE PRESTACIÓN DEL SERVICIO

10.1. Prestación Principal

El plazo de ejecución de la prestación principal es de hasta ciento cinco (105) días calendario y se contabilizará a partir de la aprobación del plan de trabajo del servicio contratado, conforme al siguiente detalle:

N°	CONCEPTO	PLAZOS
01	Implementación de la primera fase	Hasta los cuarenta y cinco (45) días calendario contados a partir de la aprobación del plan de trabajo.
02	Implementación de la segunda fase	Hasta los sesenta (60) días calendario contados a partir de la culminación de la implementación de la primera fase.

10.2. Prestación accesoria

N°	CONCEPTO	PLAZOS
01	Informe trimestral de la ejecución del servicio de soporte.	Trimestral Hasta los cinco (5) días calendario culminado el periodo trimestral del servicio. El cual se contabilizará desde la activación de la suscripción de la solución de seguridad avanzada antimalware.

11. FORMA DE PAGO

La Autoridad de Transporte Urbano para Lima y Callao – ATU, realizará el pago en SOLES por la contraprestación pactada a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad correspondiente emitida por la Unidad de Tecnologías de la Información – UTI, según el siguiente detalle:

11.1. Prestación Principal

N°	ENTREGABLE	VALOR DEL MONTO ADJUDICADO	FECHA DE PAGO
01	Informe de implementación de la primera fase	70%	Se efectuará a la entrega y conformidad del entregable
02	Informe de implementación de la segunda fase	30%	Se efectuará a la entrega y conformidad del entregable
TOTAL		100%	

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

- Acta de Conformidad emitida por la Unidad de Tecnologías de la Información.
- Comprobante de pago.
- Informe de implementación por cada etapa.

11.2. Prestación accesoria

N°	ENTREGABLE	VALOR DEL MONTO ADJUDICADO	FECHA DE PAGO
01	Informe trimestral I de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
02	Informe trimestral II de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
03	Informe trimestral III de soporte, actualizaciones reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
04	Informe trimestral IV de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
05	Informe trimestral V de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
06	Informe trimestral VI de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
07	Informe trimestral VII de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
08	Informe trimestral VIII de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
TOTAL		100%	

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

- Informe de Conformidad emitida por la Unidad de Tecnologías de la Información.
- Comprobante de pago.
- Informes trimestrales de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas.

12. PENALIDADES APLICABLES

12.1. Penalidad por mora

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la ATU aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo a la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto del contrato}}{F \times \text{plazo en días}}$$

Donde F tiene los siguientes valores:

- Para plazos menores o iguales a sesenta (60) días: F = 0.40
- Para plazos mayores a sesenta (60) días: F = 0.25

12.2. Otras Penalidades

Cualquier retraso en la presentación de la documentación solicitada en Los Resultados Esperados del Servicio (Entregable), se aplicará la siguiente penalidad:

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD	FORMA DE CALCULO (Del monto contratado)	PROCEDIMIENTO
01	Demora en la presentación del plan de trabajo.	0.05 del total de una (01) UIT por día de atraso.	Informe Técnico de la Unidad de Tecnologías de la Información – UTI
02	Demora en la presentación de los informes de implementación de la primera y segunda fase.	0.05 del total de una (01) UIT por día de atraso.	

03	Con relación al soporte técnico: Demora en la presentación del informe trimestral.	0.05 del total de una (01) UIT por día de atraso.	
04	En caso de no cumplirse el tiempo de respuesta de la Mesa de Ayuda del Contratista, de acuerdo a los SLA establecidos.	0.05 del total de una (01) UIT por incidente reportado.	
05	En caso de no cumplirse el tiempo de respuesta para la resolución del incidente de seguridad reportado, de acuerdo a los SLA establecidos.	50% del total de una (01) UIT por incidente reportado.	
06	En caso de no cumplirse el tiempo de respuesta para la resolución definitiva del incidente de seguridad reportado al fabricante, de acuerdo a los SLA establecidos.	Una (01) UIT por incidente reportado.	

13. RESPONSABILIDADES POR VICIOS OCULTOS

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado por el plazo de un (1) año, contado a partir de la conformidad otorgada por la ATU. La recepción conforme de la ATU no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos.

14. SISTEMA DE CONTRATACIÓN

El sistema de contratación será a SUMA ALZADA.

15. OTROS DOCUMENTOS PARA ACREDITAR EN LA ADMISIÓN DE OFERTAS

Para la admisión de ofertas el proveedor deberá presentar adicionalmente a lo solicitado en las bases estandarizadas lo siguiente:

- Hoja de datos y/o guía de administración y/o ficha técnica y/o manuales y/o folletería, con el fin de acreditar el cumplimiento de las funcionalidades requeridas del producto ofertado. Así también, el Anexo 01 en el que indique el cumplimiento de las características mínimas de la solución ofertada.²¹

16. CLÁUSULA DE CONFIDENCIALIDAD

El contratista debe guardar confidencialidad sobre los aspectos relacionados a la prestación, no encontrándose autorizado por la Autoridad de Transporte Urbano para Lima y Callao – ATU, para divulgar la información.

Las obras, creaciones intelectuales, científicas, entre otros, que se hayan realizado en el cumplimiento de las obligaciones contractuales, son de propiedad de la Autoridad de Transporte Urbano para Lima y Callao – ATU. En cualquier caso, los derechos de autor y demás derechos de cualquier naturaleza sobre cualquier material producido bajo las estipulaciones del presente requerimiento son cedidos a la Autoridad de Transporte Urbano para Lima y Callao – ATU en forma exclusiva.

El contratista no podrá divulgar, revelar, entregar o poner a disposición de terceros, dentro o fuera de la Autoridad de Transporte Urbano para Lima y Callao – ATU, salvo su autorización expresa, la información proporcionada por ésta para la prestación del servicio y, en general, toda información a la que tenga acceso o la que pudiera producir con ocasión del servicio que presta, durante y después de concluida la vigencia del contrato.

17. CLÁUSULA 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.

²¹ En atención a la observación N° 2

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.

18. NORMAS ANTISOBORNO

El proveedor, no debe ofrecer, negociar o efectuar, cualquier pago, objeto de valor o cualquier dádiva en general, o cualquier beneficio o incentivo ilegal en relación al contrato, que pueda constituir un incumplimiento de la ley, tales como robo, fraude, cohecho o tráfico de influencias, directa o indirectamente, o a través de socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas, en concordancia a lo establecido en la Ley de Contratación del Estado, Ley N°30225 y su Reglamento aprobado mediante Decreto Supremo N°344-2018-EF.

Asimismo, el proveedor 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, participaciones, integrantes de los órganos de administración apoderados, representantes legales, funcionarios, asesores y personas vinculadas en virtud a lo establecido en los artículos antes citados de la Ley de Contrataciones del Estado y su Reglamento.

Asimismo, el proveedor se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento, así también en adoptar medidas técnicas, prácticas, a través de los canales dispuestos por la entidad.

De la misma manera, el proveedor es consciente que, de no cumplir con lo anteriormente expuesto, se someterá a la resolución del contrato y a las acciones civiles y/o penales que la entidad pueda accionar.

Handwritten signature and initials in blue ink.

II. REQUISITOS DE CALIFICACIÓN

B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.3	CALIFICACIONES DEL PERSONAL CLAVE
B.3.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>Un (01) Gestor de Proyecto: Profesional titulado, colegiado y habilitado²² en Ingeniería: de Sistemas, y/o de Computación y Sistemas, y/o de Sistemas e Informática, y/o Informática, y/o Electrónica, y/o de Redes y/o Empresarial y de Sistemas.²³</p> <p>Un (01) Implementador/capacitador: Profesional titulado, colegiado y habilitado²⁴ en Ingeniería: de Sistemas, y/o de Computación y Sistemas, y/o de Sistemas e Informática, y/o Informática, y/o Electrónica, y/o de Redes.</p> <p><u>Acreditación:</u> El Título Profesional será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <p>En caso Título Profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p> <p>La habilitación profesional en el Colegio de Ingenieros del Perú será verificada en el siguiente enlace: https://cipvirtual.cip.org.pe/sicecolegiacionweb/externo/consultaCol/, opcionalmente el certificado de habilitación podrá ser presentado en formato físico como copia simple para el inicio efectivo del servicio.²⁵</p>
B.3.2	CAPACITACIÓN
	<p><u>Requisitos:</u></p> <p>Un (01) Gestor de Proyecto:</p> <ul style="list-style-type: none"> Con un mínimo de veinticuatro [24hrs] horas lectivas, en Gestión de Proyectos. <p>Un (01) Implementador/capacitador:</p> <ul style="list-style-type: none"> Con un mínimo de veinticuatro [24hrs] horas lectivas en programa y/o especialización y/o curso y/o taller en gestión de la ciberseguridad. Con un mínimo de veinticuatro [24hrs] horas lectivas en programas y/o especialización y/o cursos y/o talleres en sistemas operativos multi-plataforma (usuarios finales y/o servidores) y/o Red Hat System Administration y/o Microsoft Windows²⁶ y/o administración, soporte en instalación y mantenimiento de sistemas operativos²⁷. Con un mínimo de veinticuatro [24hrs] horas lectivas en programas y/o cursos en operación del producto antimalware ofertado. <p><u>Acreditación:</u> Se acreditará con copia simple de constancias o, certificados.</p>

²² En atención a la observación N° 9

²³ En atención a la consulta N° 4

²⁴ En atención a la observación N° 9

²⁵ En atención a la observación N° 9

²⁶ En atención a la consulta N° 5

²⁷ En atención a la consulta N° 71

B.4	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>Un (01) Gestor de Proyecto: Experiencia profesional no menor a ocho (08) años en gestión de proyectos de Tecnologías de Información y/o proyectos de seguridad informática y/o responsable de proyectos de tecnología de información, implementación y ejecución en proyectos de seguridad de la información y/o seguridad informática.</p> <p>Un (01) Implementador/capacitador: Experiencia no menor de cinco (05) años en implementación de soluciones, tales como: arquitecto de soluciones en tecnologías de la información y/o administración de plataformas de seguridad cloud y on-premise y/o análisis en infraestructura de comunicaciones y/o arquitectura en sistemas de información y/o implementador de mejoras en infraestructura informática y/o supervisión en plataformas de seguridad y/o implementador en soluciones de tipo antimalware.</p> <p><u>Acreditación:</u> 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 de prestaciones de servicios o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p>
C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/. 3,000,000.00 (tres millones con 00/100 soles); por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran servicios similares a los siguientes: Implementación de antimalware para usuario final (Endpoint), y/o soluciones antimalware y/o servicio de soporte de protección por gestión de equipos de seguridad, y/o servicios de seguridad informática con herramientas de seguridad de acceso lógico, y/o análisis de vulnerabilidades, y/o auditoría funcional de plataformas de seguridad para la gestión de tráfico, y/o auditoría por contaminación de software malicioso, y/o verificación o auditoría del cumplimiento de controles de seguridad y/o ventas de suscripciones de software de protección antimalware, y/o servicio de renovación de licencia antivirus, y/o servicio de plataforma de protección y seguridad de endpoint,²⁸ y/o renovación de licencias de Firewalls y/o Equipamientos de seguridad con capacidad de detección de malware²⁹.</p> <p><u>Acreditación:</u></p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con boucher de depósito, nota de abono, reporte de estado de cuenta bancaria, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago³⁰, correspondientes a un máximo de veinte (20) contrataciones.</p>

²⁸ En atención a la consulta N° 6

²⁹ En atención a la consulta N° 72

³⁰ 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"
(...)

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

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

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

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

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

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

ANEXO N° 01

REQUERIMIENTOS MÍNIMOS DE LA SOLUCIÓN OFERTADA

FABRICANTE DE LA LICENCIA ANTIMALWARE	
DENOMINACIÓN DE LA LICENCIA	
VERSIÓN / AÑO DE FABRICACIÓN	
OFERTADO	

CARACTERÍSTICAS	CUMPLIMIENTO		
	SI	NO	FOLIO
La solución de seguridad ofertada debe permitir automatizar respuesta respuestas hacia incidentes de seguridad.			
La solución de seguridad deberá estar alojada en nube (SaaS) provista por el fabricante y deberá administrar centralizadamente todos los equipos que cuentan con el producto, a través de internet.			
El acceso a consola de administración en nube debe soportar doble factor de autenticación (MFA) a través de Google Authenticator y Microsoft Authenticator.			
La solución de seguridad debe contar con un módulo de inteligencia de amenazas, que nos permita tener contexto a través de fuentes del propio fabricante, así como de fuentes terceras.			
La solución de seguridad debe permitir crear indicadores de compromiso sobre la base de cada uno de los incidentes de seguridad, y sobre la base de estos IoC, tomar las siguientes acciones de prevención manera automática o manual. La respuesta automática se debe realizar en base al nivel de confianza y severidad de los indicadores de compromiso (IoC).			
La solución de seguridad debe mostrar un reporte forense detallado, que incluya el mapa o matriz del Framework MITRE ATT&CK, el cual mostrara las tácticas y técnicas de compromiso que fueron ejecutadas por el atacante			
La solución ofertada debe tener la capacidad de restaurar archivos que fueron cifrados por el Ransomware, como parte de la recuperación automática (remediación), en su ubicación original o en una ubicación alterna que se defina.			
La solución ofertada debe contar con capacidad de prevención de Phishing de día cero o phishing no conocido, debe tener la capacidad de detectar y prevenir.			
La solución de seguridad debe detener el ataque inmediatamente cuando detecta que el ransomware modifica los archivos; así como, restaurar archivos que fueron cifrados por el ransomware, como parte de la recuperación automática (remediación), en su ubicación original o en una ubicación alterna que se defina.			
La solución de seguridad debe utilizar una base de datos en nube del propio fabricante para recibir actualizaciones y consultar la clasificación de la: IP, URL y recursos DNS no identificados.			
La solución de seguridad debe tener capacidad de detección y prevención de malware no conocido. Para ello, el software deberá realizar la emulación del malware en la nube del propio fabricante (Sandboxing), en donde se analiza y detecta amenazas no conocidas o de día cero.			
La solución de seguridad debe tener capacidad de detecciones avanzadas de UEBA (User Entity Behavioral Analytics).			
La solución de seguridad debe tener la capacidad de proteger proactivamente a los usuarios del contenido malicioso. Para todas las descargas de internet entrega archivos seguros mientras se inspeccionan los archivos originales en busca de posibles amenazas. El usuario final recibe una versión limpia del archivo (se retiran los elementos activos de riesgo).			
La solución de seguridad debe proveer una herramienta de investigación (Captura de Amenazas) que permite realizar consultas avanzadas sobre todos los eventos forenses maliciosos y benignos recopilados de los terminales que cuenta con el software de seguridad instalado. Los datos del mapa de captura de amenazas se deben almacenar con un periodo mínimo de treinta días.			
La solución de seguridad debe permitir crear incidentes de seguridad, con una vista detallada de: Información y análisis forense para ver procesos, archivos, URL, dominios y registros involucrados relacionados con el incidente. Indicadores (IoC) y artefactos relacionados con el incidente y árbol de ataque para ver una representación gráfica del informe forense.			

Importante

Para determinar que los postores cuentan con las capacidades necesarias para ejecutar el contrato, el comité de selección incorpora los requisitos de calificación previstos por el área usuaria en el requerimiento, no pudiendo incluirse requisitos adicionales, ni distintos a los siguientes:

3.2. REQUISITOS DE CALIFICACIÓN

B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.3	CALIFICACIONES DEL PERSONAL CLAVE
B.3.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>Un (01) Gestor de Proyecto: Profesional titulado, colegiado y habilitado¹⁰ en Ingeniería: de Sistemas, y/o de Computación y Sistemas, y/o de Sistemas e Informática, y/o Informática, y/o Electrónica, y/o de Redes y/o Empresarial y de Sistemas.¹¹</p> <p>Un (01) Implementador/capacitador: Profesional titulado, colegiado y habilitado¹² en Ingeniería: de Sistemas, y/o de Computación y Sistemas, y/o de Sistemas e Informática, y/o Informática, y/o Electrónica, y/o de Redes.</p> <p><u>Acreditación:</u></p> <p>El Título Profesional será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <p>En caso el Título Profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p> <p>La habilitación profesional en el Colegio de Ingenieros del Perú será verificada en el siguiente enlace: https://cipvirtual.cip.org.pe/sicecolegiacionweb/externo/consultaCol/, opcionalmente el certificado de habilitación podrá ser presentado en formato físico como copia simple para el inicio efectivo del servicio.¹³</p>
B.3.2	CAPACITACIÓN
	<p><u>Requisitos:</u></p> <p>Un (01) Gestor de Proyecto: Con un mínimo de veinticuatro [24hrs] horas lectivas, en Gestión de Proyectos.</p> <p>Un (01) Implementador/capacitador:</p> <ul style="list-style-type: none"> • Con un mínimo de veinticuatro [24hrs] horas lectivas en programa y/o especialización y/o curso y/o taller en gestión de la ciberseguridad. • Con un mínimo de veinticuatro [24hrs] horas lectivas en programas y/o especialización y/o cursos y/o talleres en sistemas operativos multi-plataforma (usuarios finales y/o servidores) y/o Red Hat System Administration y/o Microsoft Windows¹⁴ y/o administración, soporte en instalación y mantenimiento de sistemas

¹⁰ En atención a la Observación N° 09, formulada por el participante HYNET S.A.C. Ver Pliego.

¹¹ En atención a la Consulta N° 04, formulada por el participante AGGITY PERU S.A.C. Ver Pliego.

¹² En atención a la Observación N° 09, formulada por el participante HYNET S.A.C. Ver Pliego.

¹³ En atención a la Observación N° 09, formulada por el participante HYNET S.A.C. Ver Pliego.

¹⁴ En atención a la Consulta N° 05, formulada por el participante AGGITY PERU S.A.C. Ver Pliego.

	<p>operativos¹⁵.</p> <ul style="list-style-type: none"> • Con un mínimo de veinticuatro [24hrs] horas lectivas en programas y/o cursos en operación del producto antimalware ofertado <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de constancias o certificados.</p> <div> <p>Importante</p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p> </div>
B.4	<p>EXPERIENCIA DEL PERSONAL CLAVE</p> <p><u>Requisitos:</u></p> <p>Un (01) Gestor de Proyecto: Experiencia profesional no menor a ocho (08) años en gestión de proyectos de Tecnologías de Información y/o proyectos de seguridad informática y/o responsable de proyectos de tecnología de información, implementación y ejecución en proyectos de seguridad de la información y/o seguridad informática.</p> <p>Un (01) Implementador/capacitador: Experiencia no menor de cinco (05) años en implementación de soluciones, tales como: arquitecto de soluciones en tecnologías de la información y/o administración de plataformas de seguridad cloud y on-premise y/o análisis en infraestructura de comunicaciones y/o arquitectura en sistemas de información y/o implementador de mejoras en infraestructura informática y/o supervisión en plataformas de seguridad y/o implementador en soluciones de tipo antimalware.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><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> <div> <p>Importante</p> <ul style="list-style-type: none"> • Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento. • En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo. • Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas. • Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases. </div>

¹⁵ En atención a la Consulta N° 71, formulada por el participante THINK NETWORKS PERU S.A.C. Ver Pliego.

C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 3,000,000.00 (Tres millones con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran servicios similares a los siguientes: Implementación de antimalware para usuario final (Endpoint), y/o soluciones antimalware y/o servicio de soporte de protección por gestión de equipos de seguridad, y/o servicios de seguridad informática con herramientas de seguridad de acceso lógico, y/o análisis de vulnerabilidades, y/o auditoría funcional de plataformas de seguridad para la gestión de tráfico, y/o auditoría por contaminación de software malicioso, y/o verificación o auditoría del cumplimiento de controles de seguridad y/o ventas de suscripciones de software de protección antimalware, y/o servicio de renovación de licencia antivirus, y/o servicio de plataforma de protección y seguridad de endpoint¹⁶, y/o renovación de licencias de Firewalls y/o Equipamientos de seguridad con capacidad de detección de malware¹⁷.</p>
	<p><u>Acreditación:</u></p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago ¹⁸, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <p>En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el</p>

¹⁶ En atención a la Observación N° 06, formulada por el participante AGGITY PERU S.A.C. Ver Pliego

¹⁷ En atención a la Consulta N° 72, formulada por el participante THINK NETWORKS PERU S.A.C. Ver Pliego

¹⁸ Cabe precisar que, de acuerdo con la Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado:

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

(...)

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

porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

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

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

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

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

Importante

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

Importante

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

CAPÍTULO IV FACTORES DE EVALUACIÓN

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

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

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

Importante

Los factores de evaluación elaborados por el comité de selección son objetivos y guardan vinculación, razonabilidad y proporcionalidad con el objeto de la contratación. Asimismo, estos no pueden calificar con puntaje el cumplimiento de los Términos de Referencia ni los requisitos de calificación.

CAPÍTULO V PROFORMA DEL CONTRATO

Importante

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

Conste por el presente documento, la contratación del SERVICIO DE SUSCRIPCIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS PARA LOS EQUIPOS DE CÓMPUTO DE LA AUTORIDAD DE TRANSPORTE URBANO PARA LIMA Y CALLAO – ATU, que celebra de una parte la AUTORIDAD DE TRANSPORTE URBANO PARA LIMA Y CALLAO – ATU, en adelante LA ENTIDAD, con RUC N° 20604932964, con domicilio legal en Calle José Gálvez N° 550, distrito de Miraflores, provincia y departamento 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 del **CONCURSO PÚBLICO N° 007-2024-ATU-1** para la contratación de SERVICIO DE SUSCRIPCIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS PARA LOS EQUIPOS DE CÓMPUTO DE LA AUTORIDAD DE TRANSPORTE URBANO PARA LIMA Y CALLAO – ATU, 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 el SERVICIO DE SUSCRIPCIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS PARA LOS EQUIPOS DE CÓMPUTO DE LA AUTORIDAD DE TRANSPORTE URBANO PARA LIMA Y CALLAO – ATU.

CLÁUSULA TERCERA: MONTO CONTRACTUAL

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

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

CLÁUSULA CUARTA: DEL PAGO¹⁹

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

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

LA ENTIDAD debe efectuar el pago de las contraprestaciones pactadas a favor del CONTRATISTA

¹⁹ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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

Prestación Principal

N°	ENTREGABLE	VALOR DEL MONTO ADJUDICADO	FECHA DE PAGO
01	Informe de implementación de la primera fase	70%	Se efectuará a la entrega y conformidad del entregable
02	Informe de implementación de la segunda fase	30%	Se efectuará a la entrega y conformidad del entregable
TOTAL		100%	

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

- Acta de Conformidad emitida por la Unidad de Tecnologías de la Información.
- Comprobante de pago.
- Informe de implementación por cada etapa.

Prestación accesoria

N°	ENTREGABLE	VALOR DEL MONTO ADJUDICADO	FECHA DE PAGO
01	Informe trimestral I de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
02	Informe trimestral II de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
03	Informe trimestral III de soporte, actualizaciones reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
04	Informe trimestral IV de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
05	Informe trimestral V de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
06	Informe trimestral VI de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
07	Informe trimestral VII de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
08	Informe trimestral VIII de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas	12.5 %	Se efectuará a la entrega y conformidad del entregable
TOTAL		100%	

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

- Informe de Conformidad emitida por la Unidad de Tecnologías de la Información.
- Comprobante de pago.
- Informes trimestrales de soporte, actualizaciones y reportes de vulnerabilidades de seguridad resueltas.

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

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de [...], el mismo que se computa desde la aprobación del plan de trabajo del servicio contratado, en concordancia con lo establecido en el expediente de contratación.

De acuerdo al siguiente detalle:

El plazo de ejecución de la prestación principal es de hasta ciento cinco (105) días calendario y se contabilizará a partir de la aprobación del plan de trabajo del servicio contratado, conforme al siguiente detalle:

N°	CONCEPTO	PLAZOS
01	Implementación de la primera fase	Hasta los cuarenta y cinco (45) días calendario contados a partir de la aprobación del plan de trabajo.
02	Implementación de la segunda fase	Hasta los sesenta (60) días calendario contados a partir de la culminación de la implementación de la primera fase.

CLÁUSULA SEXTA: PRESTACIONES ACCESORIAS

Las prestaciones accesorias tienen por objeto el SOPORTE TÉCNICO.

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

El plazo de ejecución de las prestaciones accesorias es de acuerdo al siguiente detalle:

Prestación accesoria

N°	CONCEPTO	PLAZOS
01	Informe trimestral de la ejecución del servicio de soporte.	Trimestral Hasta los cinco (5) días calendario culminado el periodo trimestral del servicio. El cual se contabilizará desde la activación de la suscripción de la solución de seguridad avanzada antimalware.

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 SÉTIMA: GARANTÍAS

EL CONTRATISTA entregó al perfeccionamiento del contrato la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de LA ENTIDAD, por los conceptos, montos y vigencias siguientes:

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

Importante

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

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

Importante

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

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

Importante

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

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

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

CLÁUSULA NOVENA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN en el plazo máximo de SIETE (7) días de producida la recepción.

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

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

CLÁUSULA DÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA UNDÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

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

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

CLÁUSULA DUODÉCIMA: PENALIDADES

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

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

Donde:

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

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

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

Importante

De haberse previsto establecer penalidades distintas a la penalidad por mora, incluir dichas penalidades, los supuestos de aplicación de penalidad, la forma de cálculo de la penalidad para cada supuesto y el procedimiento mediante el cual se verifica el supuesto a penalizar, conforme el artículo 163 del Reglamento de la Ley de Contrataciones del Estado.

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.

Otras Penalidades

Cualquier retraso en la presentación de la documentación solicitada en Los Resultados Esperados del Servicio (Entregable), se aplicará la siguiente penalidad:

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD	FORMA DE CALCULO (Del monto contratado)	PROCEDIMIENTO
01	Demora en la presentación del plan de trabajo.	0.05 del total de una (01) UIT por día de atraso.	Informe Técnico de la Unidad de Tecnologías de la Información – UTI
02	Demora en la presentación de los informes de implementación de la primera y segunda fase.	0.05 del total de una (01) UIT por día de atraso.	
03	Con relación al soporte técnico: Demora en la presentación del informe trimestral.	0.05 del total de una (01) UIT por día de atraso.	
04	En caso de no cumplirse el tiempo de respuesta de la Mesa de Ayuda del Contratista, de acuerdo a los SLA establecidos.	0.05 del total de una (01) UIT por incidente reportado.	
05	En caso de no cumplirse el tiempo de respuesta para la resolución del incidente de seguridad reportado, de acuerdo a los SLA establecidos.	50% del total de una (01) UIT por incidente reportado.	
06	En caso de no cumplirse el tiempo de respuesta para la resolución definitiva del incidente de seguridad reportado al fabricante, de acuerdo a los SLA establecidos.	Una (01) UIT por incidente reportado.	

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

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

CLÁUSULA DÉCIMA TERCERA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA 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 CONTROVERSIAS²⁰

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

²⁰ 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).

la ejecución del presente contrato:

DOMICILIO DE LA ENTIDAD: Calle José Gálvez N° 550, distrito de Miraflores, provincia y departamento de Lima.

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 Digitales²¹.

²¹ 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

7
9 4

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2024-ATU-1
Presente.-

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

Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE ²²	Sí	No	
Correo electrónico :			

Autorización de notificación por correo electrónico:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios²³

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.

²² Esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en consideración, en caso el postor ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, en los contratos periódicos de prestación de servicios, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento.

²³ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

Importante

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

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 007-2024-ATU-1

Presente.-

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

Datos del consorciado 1			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE ²⁴	Sí	No	
Correo electrónico :			

Datos del consorciado 2			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE ²⁵	Sí	No	
Correo electrónico :			

Datos del consorciado ...			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE ²⁶	Sí	No	
Correo electrónico :			

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

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

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

²⁴ En los contratos periódicos de prestación de servicios, esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en consideración, en caso el consorcio ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

²⁵ Ibidem.

²⁶ Ibidem.

4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios²⁷

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

²⁷ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

ANEXO N° 2

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2024-ATU-1
Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2024-ATU-1
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

79

ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2024-ATU-1
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 5

PROMESA DE CONSORCIO

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

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 007-2024-ATU-1

Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO N° 007-2024-ATU-1**

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] [%]²⁸

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²⁹

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%³⁰

[CONSIGNAR CIUDAD Y FECHA]

²⁸ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²⁹ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

³⁰ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

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

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

Importante

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

ANEXO N° 6

PRECIO DE LA OFERTA

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 007-2024-ATU-1

Presente.-

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

CONCEPTO	PRECIO TOTAL
Prestación Principal:	
Prestación accesoria:	
TOTAL	

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

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

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2024-ATU-1
Presente.-

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ³¹	FECHA DE LA CONFORMIDAD DE SER EL CASO ³²	EXPERIENCIA PROVENIENTE ³³ DE:	MONEDA	IMPORTE ³⁴	TIPO DE CAMBIO VENTA ³⁵	MONTO FACTURADO ACUMULADO ³⁶
1										
2										
3										
4										

³¹ Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.

³² 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.

³³ 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".

³⁴ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

³⁵ El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.

³⁶ Consignar en la moneda establecida en las bases.

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ³¹	FECHA DE LA CONFORMIDAD DE SER EL CASO ³²	EXPERIENCIA PROVENIENTE ³³ DE:	MONEDA	IMPORTE ³⁴	TIPO DE CAMBIO VENTA ³⁵	MONTO FACTURADO ACUMULADO ³⁶
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 9

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2024-ATU-1
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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



ANEXO N° 12

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

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 007-2024-ATU-1

Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

4 9 2